UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

TESIS

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTAN

GUADALUPE DELGADO GUERRERO

JOSÉ GABRIEL PERAL GARCÍA

DIRECTORA DE TESIS

M.C. MA. JAQUELINA LÓPEZ BARRIENTOS

DEDICATORIAS

Dedicatoria a mis Padres

Ma. del Rosario Guerrero Estrada ✝
Juan Delgado Zárate

"Las cosas adquieren su importancia para nosotros en cuanto nos damos cuenta de que existen alas más grandes".

Gracias por darme alas, guía, visión, apoyo, por ampliar mis horizontes, apoyar mis sueños y sobre todo gracias por darme la vida y su inmenso amor.

Guadalupe Delgado Guerrero

Dedicatoria a mi Esposo

José Gabriel Peral García

"La virtud, como el arte, se consagra constantemente a lo que es difícil de hacer, y cuanto más dura es la tarea más brillante es el éxito".

A ti que has compartido los momentos más difíciles y más maravillosos de mi vida, dándome tu constante e incondicional apoyo, amor, cariño, comprensión, motivación, gracias por ser una persona maravillosa y generosa conmigo... ***TE AMO***.

Guadalupe Delgado Guerrero

Dedicatoria a mis Hijos

Juan Antonio Peral Delgado
Horus Peral Delgado

"Entre todas las personas, los niños son los más imaginativos: se abandonan sin reserva a toda ilusión y sueños".

Nunca dejen de soñar ya que es la forma en que seguimos siendo niños y vemos cumplidos nuestros anhelos, vayan más allá y realícenlos, recuerden que la constancia, estudio, trabajo y sacrificio son la base del éxito. Se que ustedes serán personas exitosas… ***ADELANTE***.

Guadalupe Delgado Guerrero

Dedicatoria a mi Familia

Delia Delgado Guerrero
Claudia Isabel Delgado Guerrero
Oscar Flores Rojas
Miguel Antonio Flores Huerta
Carisa Mabel Flores Delgado
Kiara Isabel Flores Delgado

"Sabemos lo que somos, pero no sabemos lo que podemos llegar a ser".

Gracias por compartir mis sueños e ilusiones, recuerden que con tenacidad podemos ver cumplidas nuestras metas.

Guadalupe Delgado Guerrero

Dedicatoria a un gran Amigo

M.C. Ing. Alejandro Jiménez García

"La verdadera amistad es una planta de lento desarrollo y debe experimentar y resistir los embates de la adversidad antes de tener derecho a esa denominación".

Gracias por todos tus consejos, experiencia, cariño, dedicación, comprensión y por transmitir el amor a la profesión, simplemente por estar.

Guadalupe Delgado Guerrero

Dedicatoria a mi Esposa

Guadalupe Delgado Guerrero

Por tu gran amor, paciencia, comprensión, confianza y por creer en mí; el haber terminado esta Tesis ha sido un gran logro que con orgullo te la dedico. Por tu entusiasmo, motivación, por darme guía y por ser mi consuelo en los momentos más difíciles de mi vida; gracias por estar conmigo y por ser parte de esta historia. Eres dueña de mi vida, de mi alma y de mi corazón; simplemente te amo pequeña. Que Dios te ilumine y bendiga.

J. Gabriel Peral García

Dedicatoria a mis Hijos

Juan Antonio Peral Delgado
Horus Peral Delgado

Por su paciencia y sacrificio al permitirme concluir mi Tesis, lo único que tengo que decirles es gracias por todos esos fines de semana de entrega, les dedico la Tesis de mi Carrera Profesional. Quiero pedirles algo muy especial, que siempre sean personitas de bien y que nunca pierdan la magia del niño que llevan dentro. Continúen con entusiasmo y compromiso sus estudios y terminen una carrera profesional, la cual les abrirá las puertas del mundo el día de mañana. Siempre confíen en sí mismos y actúen con base a su buen pensamiento y corazón. Saben que siempre estaré junto a ustedes y que cuentan conmigo. Les amo sobre todas las cosas. Que Dios los bendiga.

J. Gabriel Peral García

Dedicatoria a mis Padres

Esther García Miranda
Guillermo Peral López

A ustedes que siempre estuvieron velando por mí en todo momento y bajo cualquier circunstancia. A su gran esfuerzo y dedicación para que yo estudiara y terminara una Carrera Profesional; hoy soy lo que soy gracias a ustedes. No tengo como agradecerles todo lo que hicieron de mí y por mí. Les dedico este gran logro, la Tesis de mi Carrera Profesional. Les agradezco, respeto y los amo infinitamente. Que Dios los bendiga.

J. Gabriel Peral García

Dedicatoria a Nuestra Directora de Tesis

M.C. Ma. Jaquelina López Barrientos

Por su interés, guía, empeño, ayuda, paciencia y experiencia que siempre mostró durante el desarrollo de nuestra Tesis Profesional, la cual sin usted no hubiera podido haberse hecho realidad; por tal motivo se la dedicamos. No tenemos como agradecerle todo lo que ha hecho por nosotros, simplemente gracias, mil gracias, por creer en nosotros y ayudarnos hacer realidad nuestro sueño. Que Dios la bendiga.

Guadalupe Delgado Guerrero
José Gabriel Peral García

ÍNDICE TEMÁTICO

PRÓLOGO

Hasta finales de 1988 muy poca gente tomaba en serio el tema de la Seguridad en redes de computadoras de propósito general. Mientras que por una parte Internet iba creciendo exponencialmente con redes importantes que se adherían a ella; por otro lado el auge de la informática de consumo (hasta la década de los ochenta, muy poca gente contaba con una computadora y un módem en casa) unido a factores menos técnicos (como la película Juegos de Guerra, de 1983) iba produciendo un aumento espectacular en el número de piratas informáticos.

Sin embargo, el 22 de Noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de la Seguridad Informática: uno de sus programas se convirtió en el famoso worm o gusano de Internet. Miles de computadoras conectadas a la red se vieron inutilizadas durante días y las pérdidas se estiman en millones de dólares. Desde ese momento el tema de la Seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos. Poco después de este incidente, y a la vista de los potenciales peligros que podía entrañar un fallo o un ataque a los sistemas informáticos estadounidenses (en general, a los sistemas de cualquier país) la agencia DARPA (Defense Advanced Research Projects Agency) creó el CERT (Computer Emergency Response Team), un grupo formado en su mayor parte por voluntarios calificados de la comunidad informática, cuyo objetivo principal es facilitar una respuesta rápida a los problemas de Seguridad que afecten a hosts de Internet[1].

Han pasado más de diez años desde la creación del primer CERT, y cada día se hace patente la preocupación por los temas relativos a la Seguridad en la red y sus equipos, y también se hace patente la necesidad de esta Seguridad. Los piratas de antaño casi han desaparecido, dando paso a nuevas generaciones de intrusos que forman grupos como Chaos Computer Club o Legion of Doom, organizan encuentros como el español Iberhack, y editan revistas o c*ines* electrónicos (The Hacker's Quartely o Phrack son quizás las más conocidas, pero no las únicas). Todo esto con un objetivo principal: compartir conocimientos. Hace unos años cualquiera que quisiera adentrarse en el bajo mundo no tenía más remedio que conectarse a alguna BBS donde se tratara el tema, generalmente con una cantidad de información muy limitada; hoy en día tiene a su disposición gigabytes de información electrónica publicada en Internet; cualquier aprendiz de pirata puede conectarse a un servidor web, descargar un par de

[1] Consultar Bibliografía Libro (1)

programas y ejecutarlos contra un servidor desprotegido con un poco de suerte, esa misma persona puede conseguir un control total sobre un servidor de varios miles de dólares, probablemente desde su PC con Windows 98 o 2000 y sin saber nada. De la misma forma que en su día la película Juegos de Guerra creó una nueva generación de piratas, en la segunda mitad de los noventa películas como The Net, Hackers o Los Corsarios del Chip han creado otra generación, en general mucho menos peligrosa que la anterior, pero cuanto menos, preocupante: aunque sin grandes conocimientos técnicos, tienen a su disposición multitud de programas y documentos sobre Seguridad (algo que los piratas de los ochenta apenas podían imaginar), además de computadoras potentes y conexiones a Internet baratas. Por si esto fuera poco, se ven envalentonados a través de sistemas de conversación como el IRC (Internet Relay Chat), donde en canales como #hack o #hackers presumen de sus logros ante sus colegas.

La Seguridad de un equipo ha de ser algo a considerar en cualquier red. Diariamente por cualquiera de ellas circulan todo tipo de datos, entre ellos muchos que se podrían catalogar como confidenciales (nóminas, expedientes, presupuestos, etc.), o al menos como privados (correo electrónico, proyectos de investigación, artículos a punto de ser publicados, etc.). Independientemente de la etiqueta que cada usuario de la red quiera colgarle a sus datos, parece claro que un fallo de Seguridad de un equipo o de la propia red no beneficia a nadie, y mucho menos a la imagen de una organización. Y no se trata simplemente de una cuestión de imagen: según el Computer Security Institute, en su encuesta de 1998, las pérdidas económicas ocasionadas por delitos relacionados con nuevas tecnologías (principalmente accesos internos no autorizados) sólo en Estados Unidos ascienden anualmente a más 20,000 millones de dólares, cifra que cada año se incrementa en más del 35%; los delitos informáticos en general aumentan también de forma espectacular año tras año, alcanzando incluso cifras del 800%[2].

Es imposible garantizar una plena seguridad ante cualquier atacante; seguramente un pirata experimentado, con el tiempo suficiente, pagado o simplemente muy interesado en algún equipo de la organización, no tendría muchos problemas en acceder a él.

El objetivo final de este proyecto es identificar los factores que ayuden a conseguir un nivel de seguridad aceptable en los sistemas conectados en cualquier red, entendiendo por "aceptable" un nivel de protección suficiente para que la mayoría de intrusos potenciales

[2] Consultar Bibliografía Libro (2)

interesados en los equipos de una organización fracase ante un ataque contra los mismos.

Por supuesto, este proyecto no pretende ser en ningún momento una ayuda para la gente que esté interesada en atacar sistemas o redes completas, ni tampoco una invitación a hacerlo. Aunque por su naturaleza la información aquí presentada puede ser utilizada para dañar sistemas informáticos (como cualquier información sobre seguridad informática), no es ese su propósito sino, como hemos dicho, incrementar la seguridad de los sistemas y las redes en las que éstos se ubican. Por tanto va a intentar estar escrito de forma que no se pueda utilizar fácilmente como una "receta de cocina" para piratas; si alguien quiere un documento sobre cómo atacar sistemas, puede dejar de leer este trabajo y buscar en Internet información sobre ese tema. Conseguir romper la seguridad de un sistema de forma no autorizada es, en la mayoría de los casos, un símbolo de inmadurez, y por supuesto ni denota inteligencia ni unos excesivos conocimientos: si alguien se considera superior por acceder ilegalmente a un equipo o sistemas utilizando un programa que ni ha hecho ni es capaz de entender, que revise sus principios, y si tras hacerlo aún piensa lo mismo, que dedique su inteligencia y sus conocimientos a tareas que ayuden a incrementar la seguridad, como la construcción de sistemas de autenticación fiables y baratos o el diseño de nuevos criptosistemas seguros. Eso es seguridad informática, y no lo que habitualmente se nos quiere hacer creer: la seguridad informática no consiste en conocerse todos los bugs o fallas de un sistema operativo, con sus correspondientes ventajas, ni en jugar a superhackers (superpiratas) en canales de IRC (Internet Relay Chat). Lamentablemente, este es el panorama de la Seguridad más visible en México en la actualidad; esperemos que algún día cambie.

El presente trabajo presenta una visión de la Seguridad en los Sistemas de Información y cómo evaluar los aspectos de la misma. Esta dirigido a dar un panorama amplio de la situación sin entrar a detalles técnicos profundos.

A lo largo de este trabajo se hace un repaso de los puntos habituales y más importantes referentes a Seguridad en los Sistemas de Información (problemas, ataques, defensas, etc.), aplicando el estudio a entornos con requisitos de seguridad medios (universidades, empresas y proveedores de acceso a internet); de esta forma se ofrecerá una perspectiva general de la Seguridad, el funcionamiento de sus mecanismos, y su correcta utilización. También se hablará, en menor medida, sobre temas menos técnicos pero que también afectan

directamente a la Seguridad informática, como pueden ser el problema del personal o la legislación vigente.

La Seguridad en los Sistemas de Información es un amplio concepto cuyas características ampliaremos en el presente trabajo. La ruptura de la Seguridad en un Sistema de Información puede resultar en un acceso no autorizado de los recursos, penetración de virus, robo de datos o destrucción de la infraestructura de tecnología. La cobertura dada por los medios de comunicación lleva al público a creer que la mayoría de las violaciones de Seguridad son el resultado de ataques de "hackers" (piratas) o foráneos; sin embargo, mucho de los actos no autorizados, pueden ser llevados a cabo por empleados molestos con la empresa o infiltrados. Todo esto ilustra la importancia de proteger los recursos basados en computadoras tanto de los entes externos e internos a la empresa.

Se presenta una serie de recomendaciones que se hacen a los Gerentes de Empresas con la finalidad de que presten atención a los problemas de seguridad, debido a los nuevos riesgos que el internet introduce en las organizaciones.

Se aborda el tema de la seguridad externa e interna de un Sistema de Información, teniendo como propósito el identificar cuáles son los factores que se deben considerar para asegurar la confiabilidad, integridad y disponibilidad de un Sistema de Información.

Finalmente se presenta una de las mejores prácticas para asegurar que un Sistema de Información es seguro o fiable; esta práctica es la auditoría, la cual es un instrumento para asegurar la continuidad de la aplicación de normas, políticas y procedimientos que garanticen la fiabilidad, integridad y disponibilidad de un Sistema de Información para que una organización opere bajo estándares, en un ambiente controlado y de riesgo bajo.

CAPÍTULO I

Importancia de la Seguridad de los Sistemas de Información

La ruptura de la seguridad en un sistema puede resultar en un acceso no autorizado de los recursos, penetración de virus, robo de datos o destrucción de la infraestructura de tecnología. La cobertura dada por los medios de comunicación lleva al público a creer que la mayoría de las violaciones de seguridad son el resultado de ataques de hackers o foráneos; sin embargo, muchos de los actos no autorizados, pueden ser llevados a cabo por empleados molestos con la empresa o infiltrados. Todo esto ilustra la importancia de proteger los recursos basados en computadoras tanto de los entes externos e internos a la empresa. Cabe mencionar que el porcentaje más alto es dado precisamente por personal "enterado" del manejo, control, distribución, etc., de la información y sabe exactamente cómo llegar a ella y cómo robarla o dañarla si se lo propone.

No hace mucho tiempo atrás solo las grandes organizaciones y compañías se preocupaban por los riesgos de seguridad en sus sistemas de información. Sus esfuerzos en mantener la propiedad de la información son el objetivo primordial, hoy en día ya no es únicamente esto, la tecnología se ha convertido tan prevalente que afecta en casi todos los aspectos de la vida cotidiana. Las computadoras son el centro de todos los negocios, que van desde los sistemas de comercialización de acciones hasta páginas de deportes que muestran los resultados de los juegos de la noche anterior. Las computadoras son responsables por mantener cosas tales como: cuentas de bancos, registros médicos, reportes bancarios e historiales de crédito. Claramente, todo individuo que posea una tarjeta de crédito y/o débito y usa un cajero electrónico debe estar preocupado por la exactitud y privacidad de su información personal, en consecuencia, ellos también se encuentran preocupados por los riesgos de seguridad en los sistemas de información.

¿Por qué es una causa de preocupación?

Muchos factores han causado que se incremente la preocupación de los asuntos de seguridad en los sistemas. Las computadoras personales no son exclusivamente usadas en la oficina. El uso de las computadoras para recreación y en el hogar ha crecido dramáticamente. De hecho muchos de los propietarios de computadoras están optando por adquirir acceso a Internet lo cual les permite acceder a los recursos de la red mundial (www: world wide web) y correo electrónico. Estos usuarios han encontrado el comercio electrónico el cual representa una gran conveniencia, simplicidad y robustez que los usuarios necesitan.

Adicionalmente, como los precios de las computadoras siguen bajando y la gente encuentra mayor comodidad con el uso de la

tecnología, la confianza en los recursos basados en computadoras continúa creciendo. Igualmente crece la dependencia y de igual manera aumentan los riesgos de seguridad que pueden llevar a resultados desastrosos con posibles ramificaciones financieras y legales. Lo mínimo que puede suceder con una brecha de seguridad es la pérdida de tiempo y disminución de la productividad mientras se vuelve a la normalidad, aunque los resultados en la realidad sean peores con efectos tales como: pérdidas financieras, disminución de la confiabilidad y no ser capaces de capturar más clientes.

1.1 ¿Qué es Seguridad?

Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas de información, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo: en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de backup) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados. En cambio, en un servidor de un departamento se premiará la disponibilidad frente a la confidencialidad: importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados va a suponer una pérdida de tiempo y dinero. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

1.1.1 Objetivos de la Seguridad

Existen tres objetivos principales en una efectiva práctica de seguridad en sistemas de información: confidencialidad, integridad y disponibilidad. A continuación una explicación sobre cada uno de ellos:

1.1.1.1 Confidencialidad

Es el concepto que define que la información no está disponible a aquellos que no están autorizados a ella. Controles estrictos deben ser implantados a únicamente aquellas personas que necesitan acceso a cierta información. En algunas organizaciones con datos confidenciales, las personas deben tener acceso solo a las relacionadas para realizar su función en la misma. La mayoría de los crímenes de computadoras comprenden el comprometer la confidencialidad y el robo de información. El concepto de permitir acceso a la información o recursos a aquellos que lo necesiten es llamado **control de acceso.**

La forma más común del control de acceso es el uso de claves de seguridad y la forma más común de encontrar una brecha de seguridad es el comprometer la privacidad de estas claves de seguridad. El requerir claves de seguridad complicadas, tarjetas de acceso inteligentes, dispositivos de seguridad o biométricos, son el primer paso en prevenir a usuarios no autorizados el acceso de información. El proteger estas claves de seguridad es uno de los principios fundamentales de la seguridad en sistemas de información ya que a través de éstas el personal accede a la información; es por ello importante resaltar que es necesario responsabilizar al usuario de los sistemas de información sobre el uso de estas claves de seguridad.

Como parte de la confidencialidad de la información la encriptación es el proceso que transforma la información en alguna forma secreta para prevenir que individuos no autorizados tengan acceso a la misma.

1.1.1.2 Integridad

Se asegura que la información no pueda ser modificada de manera inesperada. La pérdida de integridad pudiera resultar de un error humano, daño intencional o eventos catastróficos. Si se modifica incorrectamente la información, ésta puede convertirse en inútil, o peor, peligrosa. Todos los esfuerzos deben ser hechos con la finalidad de que los datos estén correctos.

Cuando la validez de la información es crítica, en algunas ocasiones es útil diseñar los controles que permitan asegurar la exactitud. Por ejemplo: sería importante asegurarse que la información se vuelva inútil si es robada.

1.1.1.3 Disponibilidad

Previene que los recursos sean eliminados o que estén inaccesibles. Esto aplica no solo a la información, sino a la infraestructura tecnológica presente en las organizaciones. El ataque intencional en contra de los sistemas de computación está dirigido a eliminar el acceso a los datos y en algunos casos al robo de los mismos.

Garantizar la seguridad física de un sistema de información es una manera de proteger la disponibilidad. El limitar el acceso físico a computadoras críticas o fuentes de datos, la probabilidad de que no estén disponibles se disminuye. Así mismo es importante y necesario identificar los accesos lógicos a los sistemas de información ya que ellos pueden saturar de peticiones al sistema, bloquearlo hasta derribarlo ocasionando con ello la pérdida de su disponibilidad.

1.1.2 Estrategia de Seguridad

Se deben analizar los tres aspectos anteriormente descritos para evaluar y formular una estrategia de seguridad. Dependiendo de la necesidad de su negocio varios niveles deben ser aplicados a cada objetivo.

Cuando se desarrolla una política de seguridad, se debe tener cuidado al identificar y comprender los asuntos relevantes. Cuando se evalúa la efectividad de una política en particular los recursos protegidos deben ser analizados. El objetivo es proteger la información en relación con su valor e importancia en los procesos de negocio.

Una política de seguridad bien preparada debe garantizar el acceso de la información necesaria para el desarrollo normal de las labores de los empleados y los accesos deben ser según el tipo de acceso requerido, por ejemplo: solo lectura, lectura y modificación, etc.

Otro factor a considerar en la formulación de una estrategia de seguridad es el costo monetario de la misma. Adicionalmente al costo de la estrategia se debe contemplar el tiempo y el esfuerzo necesario para la aplicación de la misma con base en la importancia de los datos a proteger.

1.2 ¿Qué Queremos Proteger?

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, tales como: CPU's, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROM's, diskettes, etc.), tarjetas de red, entre otros. Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tales como: sistemas operativos, aplicaciones, programas, etc. Por datos entiéndase el conjunto de información lógica que es manejada por el software y el hardware, como por ejemplo: paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorías de seguridad se habla de un cuarto elemento a proteger, los fungibles (elementos que se gastan o desgastan con el uso continuo, como papel para impresora, toner, cartuchos (tintas) para impresora, etc.) Para efectos de esta tesis no consideraremos el trato de la seguridad de estos elementos por ser consumibles.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar. Con toda seguridad un sistema de información está ubicado en un lugar de acceso físico restringido, o al menos controlado y además, en caso de pérdida de una aplicación (un programa, o el propio sistema operativo) este software se puede restaurar sin problema desde su medio original (por ejemplo, el CD-ROM con el sistema operativo que se utilizó para su instalación.) Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio original desde el cual restaurar y hemos de pasar obligatoriamente por un sistema de copias de seguridad y a menos que la política de copias y/o respaldos sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida. Cabe destacar que la información es el elemento a proteger más importante de la seguridad; la cual se puede encontrar en diferentes estados - almacenamiento, procesamiento, generación o en tránsito (transacción) – y en cualquiera de ellos, la información debe estar protegida al igual que los recursos asociados a ella y en sus diferentes facetas.

Contra cualquiera de los tres elementos descritos anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación,

modificación y fabricación. Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema. Una modificación si además de conseguir el acceso consigue modificar el objeto. Algunos autores[3] consideran un caso especial de la modificación a la destrucción; entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el fabricado. En la figura 1.1 se muestran estos tipos de ataque de una forma gráfica.

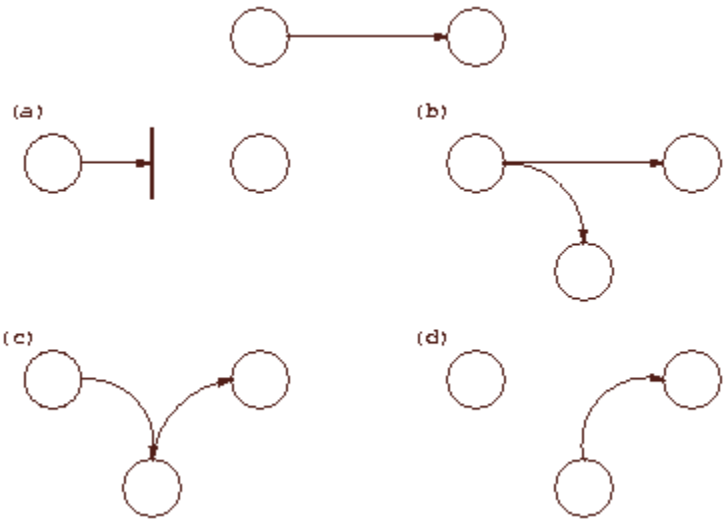

Figura 1.1 Tipos de Ataques
Flujo normal de información entre emisor, receptor y posibles amenazas: (a) interrupción, (b) intercepción, (c) modificación y (d) fabricación

1.3 ¿De qué nos Queremos Proteger?

En la gran mayoría de las publicaciones relativas a la seguridad de los sistemas de información en general se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. Con frecuencia, especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad[4,5] se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático. En el presente trabajo

[3] Consultar Bibliografía Libro (3)
[4] Consultar Bibliografía Libro (4)
[5] Consultar Bibliografía Libro (5)

hablaremos de elementos y no de personas, aunque a veces lo olvidemos, nuestro sistema puede verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo: programas, catástrofes naturales o, por qué no, hackers; si un usuario pierde un trabajo importante a causa de un ataque, poco le importará que haya sido un intruso, un gusano (virus), un simple error del administrador, o un hacker que haya violado su disco duro.

A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a nuestro sistema de información. No pretende ser exhaustiva, ni por supuesto una taxonomía formal (para este tipo de estudios, se recomienda consultar[6,7]), simplemente trata de proporcionar una idea acerca de qué o quién amenaza un sistema de información. A lo largo de este trabajo se ahondará en aspectos de algunos de los elementos presentados aquí.

1.3.1 Personas

No podemos engañarnos, la mayoría de los ataques a un sistema de información van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) de los riesgos lógicos de los que hablaremos a continuación, especialmente agujeros del software. Pero con demasiada frecuencia se suele olvidar que los piratas clásicos no son los únicos que amenazan nuestros equipos. Es especialmente preocupante que mientras que hoy en día cualquier administrador preocupado por la seguridad, va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos, etc.), pocos administradores tienen en cuenta factores como la ingeniería social o el basureo a la hora de diseñar una política de seguridad.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestro sistema de información; generalmente se dividen en dos grandes grupos: **(1) los atacantes pasivos**, aquellos que fisgonean por el sistema pero no lo modifican - o destruyen -, y **(2) los atacantes activos**, aquellos que dañan el objetivo atacado - o lo modifican -, en su favor. Generalmente los curiosos y los hackers realizan ataques pasivos (que se pueden

[6] Consultar Bibliografía Libro (6)
[7] Consultar Bibliografía Libro (7)

convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo y activos en caso contrario. El personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

1.3.1.1 Personal

Las amenazas a la seguridad de un sistema proveniente del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento), puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas y sus debilidades), lo normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad. Un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de ficheros; y en el primer caso, el atacante ni siquiera ha de tener acceso lógico (ni físico) a los equipos, ni conocer nada sobre seguridad de los sistemas de información. Hemos de recordar siempre que decir "No lo hice a propósito" no va a servir para recuperar datos perdidos, ni para restaurar un hardware dañado o robado.

1.3.1.2 Ex-empleados

Otro gran grupo de personas potencialmente interesadas en atacar nuestro sistema son los antiguos empleados del mismo, especialmente los que no abandonaron el entorno por voluntad propia. Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema de información que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo. Amparados en excusas como "No me han pagado lo que me deben" o "Es una gran universidad, se lo pueden permitir" pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema de información como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso

meses después de abandonar la universidad o empresa.) Conseguir el privilegio necesario y dañarlo de la forma que deseen, estas personas utilizan tácticas de hasta incluso, chantajear a sus ex-compañeros o ex-jefes.

1.3.1.3 Curiosos

Junto con los hackers, los curiosos son los atacantes más habituales de los sistemas de información en redes de I+D. Recordemos que los sistemas de información están trabajando en entornos donde se forma a futuros profesionales de la informática y las telecomunicaciones (gente que a priori tiene interés por las nuevas tecnologías), y recordemos también, que las personas suelen ser curiosas por naturaleza; esta combinación produce una avalancha de estudiantes o personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. En la mayoría de las ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema de información concreto. Aunque en la mayoría de las situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema de información. El hecho de que alguien este "enterado" de la información que sólo nos concierne a nosotros y que está clasificada como "confidencial" la pone en riesgo.

1.3.1.4 Hackers

Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otros sistemas de información o simplemente por diversión. Por un lado, las redes generalmente abiertas y la seguridad no es un factor tenido muy en cuenta en ellas; por otro, el gran número y variedad de sistemas de información conectados a éstas redes provoca, casi por simple probabilidad, que al menos algunos de éstos sistemas de información (cuando no la mayoría) sean vulnerables a problemas conocidos de antemano. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple exploit a los sistemas de información que presentan vulnerabilidades; esto convierte a las redes de I+D, a las redes de empresas, o a las redes ISP's en un objetivo fácil y apetecible para piratas o hackers con cualquier nivel de conocimientos, desde los más novatos (y a veces más peligrosos) hasta los expertos, que pueden utilizar toda la red para

probar nuevos ataques o como nodo intermedio en un ataque a otros organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto) que supone para una universidad ser, sin desearlo, un apoyo a los piratas o hackers que atacan sistemas de información teóricamente más protegidos, como los militares.

1.3.1.5 Terroristas

Por terroristas no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca a un sistema de información simplemente por causar algún tipo de daño en él. Por ejemplo: alguien puede intentar borrar las bases de datos de un partido político enemigo, o destruir los sistemas de ficheros de un sistema de información que alberga páginas web de algún grupo religioso, entre otros; en el caso de los sistemas de información ubicados en redes de I+D, los típicos ataques son la destrucción de prácticas o la modificación de páginas web de algún departamento escolar o de ciertos profesores; generalmente por parte de alumnos descontentos.

1.3.1.6 Intrusos Remunerados

Este es el grupo de atacantes de un sistema más peligroso, suele afectar más a las grandes empresas o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte. Generalmente para robar secretos (por ejemplo: el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía, etc.), o simplemente para dañar la imagen de la entidad afectada. Esta tercera parte suele ser una empresa de la competencia o un organismo de inteligencia, es decir; una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad, se suele pagar bien a los mejores piratas y por si esto fuera poco los atacantes van a tener todos los medios necesarios a su alcance.

Aunque como hemos dicho los intrusos remunerados son los menos comunes en la mayoría de situaciones, en ciertas circunstancias pueden aprovechar los sistemas de información como plataforma para atacar otros organismos; una excelente lectura sobre esta situación es[8], en la que el experto en seguridad Cliff Stoll describe cómo piratas pagados por el KGB soviético utilizaron sistemas de información de

[8] Consultar Bibliografía Libro (8)

redes I+D para acceder a organismos de defensa e inteligencia estadounidenses.

1.3.2 Amenazas Lógicas

Bajo la etiqueta de amenazas lógicas encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema de información, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros.)[9,10].

1.3.2.1 Software Incorrecto

Las amenazas más habituales a un sistema de información provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. Una situación no contemplada a la hora de diseñar el kernel del sistema de información o un error al acceder a la memoria, puede comprometer local o remotamente a un sistema de información.

A estos errores de programación se les denomina bugs y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema de información se les llama exploits. Como hemos dicho, representan la amenaza más común contra un sistema de información, ya que cualquiera puede conseguir un exploit y utilizarlo contra nuestro equipo sin saber cómo funciona y sin tener los conocimientos mínimos del sistema; incluso hay exploits que dañan seriamente la integridad de un sistema (negaciones de servicio o incluso acceso remoto) y están preparados para ser utilizados desde el sistema operativo, con lo que cualquier pirata novato (comúnmente, se les denomina Script Kiddies) puede utilizarlos contra un sistema de información y conseguir un control total del equipo de varios millones de dólares desde su PC sin saber nada del sistema atacado; incluso hay situaciones en las que se analizan los logs de estos ataques y se descubre que el pirata incluso intenta ejecutar órdenes de línea de comando.

1.3.2.2 Herramientas de Seguridad

Cualquier herramienta de seguridad representa un arma de doble filo; de la misma forma que un administrador las utiliza para detectar y solucionar fallos en el sistema de información o en la red completa, un

[9] Consultar Bibliografía Libro (9) para estudiar definiciones detalladas de amenazas y sus implicaciones
[10] Consultar Bibliografía Libro (10) para estudiar definiciones generales de amenazas y sus implicaciones

potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Estas herramientas pasan de ser útiles a ser peligrosas cuando las utilizan hackers que buscan información sobre las vulnerabilidades de un sistema de información o de una red completa.

La conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque es un tema difícil; incluso expertos reconocidos como Alec Muffet (autor del adivinador de contraseñas Crack) han recibido enormes críticas por diseñar determinadas herramientas de seguridad. Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema de información en el supuesto desconocimiento de sus problemas por parte de los atacantes; esta política, denominada security through obscurity, se ha demostrado inservible en múltiples ocasiones. Si los administradores de un sistema no utilizan herramientas de seguridad que muestren las debilidades de nuestros sistemas de información (para corregirlas), tenemos que estar seguros que un atacante no va a dudar en utilizar tales herramientas (para explotar las debilidades encontradas); por lo que, hemos de agradecer a los diseñadores de dichos programas el esfuerzo que han realizado (y nos han ahorrado) en pro de sistemas más seguros.

1.3.2.3 Puertas Traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos, por ejemplo: los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla se necesitan cuatro claves diferentes de diez caracteres cada una, pueden insertar una rutina para conseguir ese acceso mediante una única clave "especial", con el objeto de perder menos tiempo al depurar el sistema.

Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería, lo que obviamente supone un grave peligro para la integridad de nuestro sistema.

1.3.2.4 Bombas Lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la ejecución bajo un determinado usuario o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa, por ejemplo: el administrador del sistema, o el programa que contiene la bomba está definido a su nombre, por lo que los efectos obviamente pueden ser fatales.

1.3.2.5 Canales Cubiertos

Los canales cubiertos (o canales ocultos, según otras traducciones) son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema de información; dicho de otra forma, es un proceso que transmite información a otros (locales o remotos) que no están autorizados a leer dicha información[11,12].

Los canales cubiertos no son una amenaza demasiado habitual en los sistemas de información ubicados en redes de I+D, ya que suele ser mucho más fácil para un atacante aprovechar cualquier otro mecanismo de ataque lógico; sin embargo, es posible su existencia y en este caso su detección suele ser difícil, por ejemplo: algo tan simple como el puerto finger abierto en un sistema de información puede ser utilizado a modo de canal cubierto por un pirata con algo de experiencia.

1.3.2.6 Virus

Un virus es una secuencia de código que se inserta en un fichero y/o archivo ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Todo el mundo conoce los efectos de los virus en algunos sistemas operativos de sobremesa, es decir; bajo plataforma Intel; sin embargo,

[11] Consultar Bibliografía Libro (11)
[12] Consultar Bibliografía Libro (12)

en sistemas operativos de plataforma RISC, los virus aún no existen, por lo que no son un problema de seguridad, más sin embargo en plataformas de este tipo lo que puede ser más grave que un virus es un mecanismo lógico (que será el que hay que tener en cuenta a la hora de diseñar una política de seguridad en esta plataforma.)

Mientras los mecanismos lógicos en los sistemas de información bajo plataforma RISC son una amenaza real comparados con los virus de plataforma Intel; ciertos virus que atacan a esta plataforma especialmente los de boot, pueden tener efectos nocivos, como dañar el sector de arranque; aunque se trata de daños menores comparados con los efectos de otras amenazas, hay que tenerlos en cuenta.

1.3.2.7 Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande, por ejemplo: el mayor incidente de seguridad en Internet fue precisamente el Internet Worm, un gusano que en 1988 causó pérdidas millonarias al infectar y detener más de 6000 máquinas conectadas a la red.

Hemos de pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema de información, por ejemplo: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestro sistema de información (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos, de ahí su enorme peligro y sus devastadores efectos.

1.3.2.8 Caballos de Troya

Los troyanos o caballos de troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario, el caballo de troya de la mitología griega, - al que debe su nombre -; ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

Cuando un intruso consigue acceso al sistema de información instala troyanos para ocultar su presencia o para asegurarse la entrada en caso de ser descubierto, por ejemplo: es típico utilizar lo que se denomina un rootkit, que no es más que un conjunto de versiones troyanas de ciertas utilidades, para conseguir que cuando el administrador las ejecute no vea la información relativa al atacante, como sus procesos o su conexión al sistema. Otro programa que se suele suplantar es login, para que al recibir un cierto nombre de usuario y contraseña proporcione acceso al sistema de información sin necesidad de consultar la tabla de passwords.

1.3.2.9 Programas Conejo o Bacterias

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema de información (memoria, procesador, disco, etc.), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema de información, que en algunas situaciones pueden llegar a provocar la caída total del sistema de información.

1.3.2.10 Técnicas Salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad de origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección; si de una cuenta con varios millones de dólares se roban unos centavos, nadie va a darse cuenta de ello; si esto se automatiza para descontar un dólar de cada nómina pagada en una empresa o en la universidad de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima.

Las técnicas salami no suelen utilizarse para atacar sistemas de información normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, en una empresa o entidad con requerimientos de seguridad menores es posible que haya sistemas de información dedicados a la contabilidad, facturación de un departamento o gestión de nóminas del personal, ésta puede ser una potencial amenaza contra el sistema de información encargado de estas tareas.

1.3.3 Catástrofes

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales, simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas de información en una gran ciudad, es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen medidas básicas, ya que si se produjeran generarían los mayores daños.

Un subgrupo de las catástrofes es el denominado de riesgos poco probables. Obviamente se denomina así al conjunto de riesgos que, aunque existen, la posibilidad de que se produzcan es tan baja (menor incluso que la del resto de catástrofes) que nadie toma, o nadie puede tomar, medidas contra ellos. Ejemplos habituales de riesgos poco probables son un ataque nuclear contra el sistema de información, el impacto de un satélite contra la sala de operaciones, o la abducción de un operador por una nave extraterrestre. Nada nos asegura que este tipo de catástrofes no vaya a ocurrir, pero la probabilidad es tan baja y los sistemas de prevención tan costosos que no vale la pena tomar medidas contra ellas.

Como ejemplos de catástrofes hablaremos de desastres naturales (terremotos, tormentas eléctricas, inundaciones y humedades), de desastres del entorno (electricidad, ruido eléctrico, incendios, humo y temperaturas extremas) o atentados de baja magnitud (más comunes de lo que podamos pensar); obviamente los riesgos poco probables los trataremos como algo anecdótico. De cualquier forma, vamos a hablar de estas amenazas más adelante sin extendernos mucho, ya que el objetivo de este proyecto no puede ser el proporcionar las directrices para una construcción de edificios a prueba de terremotos, o un plan formal de evacuación en caso de incendio.

1.4 ¿Cómo nos Podemos Proteger?

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar nuestra visión de la seguridad, hemos de hablar de las formas de protección de nuestros sistemas de información. Cuando hayamos completado este punto, habremos

presentado a grandes rasgos los diferentes puntos a tratar en este proyecto.

Para proteger nuestro sistema de información hemos de realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar y la probabilidad de su ocurrencia; a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implantar esta política de seguridad, son denominados mecanismos de seguridad; son la parte más visible de nuestro sistema de seguridad y se convierten en la herramienta básica para garantizar la protección de los sistemas de información o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación. (1) Los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema de información durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema de información. (2) Por mecanismos de detección se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoría como Tripwire. Finalmente, (3) los mecanismos de recuperación son aquellos que se aplican cuando una violación del sistema de información se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de información.

Parece claro que, aunque los tres tipos de mecanismos son importantes para la seguridad de nuestro sistema de información, hemos de enfatizar en el uso de mecanismos de prevención y de detección; la máxima popular "más vale prevenir que lamentar" se puede aplicar a la seguridad informática; para nosotros, evitar un ataque, detectar un intento de violación o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y

menos comprometedor para el sistema de información que restaurar el estado tras una penetración al sistema. Es más, si consiguiéramos un sistema sin vulnerabilidades y cuya política de seguridad se implantara mediante mecanismos de prevención de una forma completa, no necesitaríamos mecanismos de detección o recuperación. Aunque esto es imposible de conseguir en la práctica, será en los mecanismos de detección y sobre todo en los de prevención, en los que centraremos más nuestro trabajo.

Los mecanismos de prevención más habituales en los sistemas de información son los siguientes[13]:

1.4.1 Mecanismos de Autenticación e Identificación

Estos mecanismos hacen posible identificar entidades del sistema de información de una forma única y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser.) Son los mecanismos más importantes en cualquier sistema de información, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.

Un grupo especialmente importante de estos mecanismos son los denominados sistemas de autenticación de usuarios, a los que prestaremos una especial atención por ser los más utilizados en la práctica.

1.4.2 Mecanismos de Control de Acceso

Cualquier objeto del sistema de información ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema. Dentro de un sistema de información, el control de acceso más habitual es el discrecional (DAC: Discretionary Access Control), implantado por los bits read, write, execute y las listas de control de acceso para cada fichero (objeto) del sistema; sin embargo, también se permiten especificar controles de acceso obligatorio (MAC: Must Access Control.)

[13] Consultar Bibliografía Libro (3)

1.4.3 Mecanismos de Separación

Cualquier sistema de información con diferentes niveles de seguridad ha de implantar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso.

Los mecanismos de separación se dividen en cinco grandes grupos, en función de como separan a los objetos, éstos son: separación física, temporal, lógica, criptográfica y fragmentación. Dentro de un sistema de información, el mecanismo de separación más habitual es el de separación lógica o aislamiento.

1.4.4 Mecanismos de Seguridad en las Comunicaciones

Es especialmente importante para la seguridad de nuestro sistema de información el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, hemos de utilizar ciertos mecanismos, la mayoría de los cuales se basan en la criptografía: cifrado de clave pública, de clave privada, firmas digitales, etc. Aunque cada vez se utilizan más los protocolos seguros, aún es frecuente encontrar conexiones en texto claro ya no sólo entre sistemas de información de una misma subred, sino entre redes diferentes. Una de las mayores amenazas a la integridad de los sistemas de información es este tráfico sin cifrar, que hace extremadamente fáciles los ataques encaminados a robar contraseñas o suplantar la identidad de los sistemas de información.

A lo largo de este trabajo intentaremos explicar el funcionamiento de algunos de estos mecanismos para conseguir sistemas de información más fiables; pero mucho más importante que el funcionamiento, es la concientización de usuarios y administradores de las ventajas en materia de seguridad que estos mecanismos y muchos otros, ofrecen. Hemos de recordar que un sistema de información instalado tal y como se distribuye suele representar una puerta abierta para cualquier pirata sin grandes conocimientos; si ese mismo sistema de información lo configuramos antes de ponerlo a trabajar, un intruso necesitará conocimientos del sistema operativo y de la red más o menos amplios (o mucha suerte) si quiere violar su seguridad. Como ya dijimos, el objetivo de este proyecto no es conseguir unos sistemas de

información con seguridad militar en un entorno normal (algo imposible), sino conseguir un entorno de trabajo fiable.

1.5 Tipos de Redes

En este trabajo, como ya hemos comentado, no se pretende ni mucho menos adentrarse en temas de seguridad que se podría considerar "de alto nivel", como la necesaria en un entorno militar, de inteligencia, o en una gran empresa que maneje datos muy apetecibles para sus competidores. Un fallo en la seguridad de los sistemas de información de una central nuclear puede ser catastrófico - en el más amplio sentido de la palabra -; un pequeño fallo en los sistemas de información encargados de lanzar un satélite nos costaría a todos miles de millones de dólares, si en lugar de ser un satélite es un misil, podemos imaginarnos las consecuencias. Por fortuna para todos nosotros, esos sistemas de información son altamente seguros y por supuesto no son simples ordenadores conectados a Internet ni siquiera a redes de propósito general.

Pero lo más probable es que todas estas cosas nos queden demasiado lejos a la mayoría de los mortales; para nosotros los problemas de seguridad diarios son intrusiones, virus (sin comentarios), negaciones de servicio contra un sistema de información que sirve páginas web; algo mucho más terrenal que todo lo anterior. Es en este tipo de entornos donde los mecanismos que estudiaremos se pueden aplicar más fácilmente, tanto por las características de los sistemas de información utilizados, como por el - relativamente - bajo peligro de nuestros atacantes. Imaginemos que la CIA o el FBI no están dispuestos a pagar piratas profesionales para que entren y lean nuestro correo; los intrusos potencialmente interesados en nuestros sistemas de información serán individuos que sólo buscan un cierto status social en un grupo de aficionados a la piratería, o que acaban de ver una película y tratan de emular a los actores. Gente que ante la más mínima dificultad para acceder a nuestro sistema de información, lo abandonará y se dedicará a objetivos más fáciles (como el sistema de información de nuestro vecino.) Contra este tipo de personas es contra quien debemos esforzarnos; ya hemos dicho que es inútil intentar parar a un atacante profesional, pagado o muy interesado en nuestros sistemas de información, el que su ataque tenga éxito es sólo cuestión de tiempo y seguramente depende más de la suerte que tenga él frente a la que tengamos nosotros. Pero estos atacantes son minoría y lo que debemos buscar es defendernos contra la mayoría.

Ejemplos de tipos de redes, de entornos con unos requerimientos de seguridad medios (pero requerimientos, al fin y al cabo), son las redes de I+D (universidades, centros de investigación, etc.), las redes empresariales y las redes de proveedores de acceso a Internet. Vamos a hablar en este punto de las características de cada una de ellas.

1.5.1 Redes I+D

En cualquier tipo de red, la seguridad es siempre un factor a tener en cuenta a la hora de administrar la propia red y sus sistemas de información. Por supuesto las redes de I+D no son ninguna excepción y aunque con demasiada frecuencia su seguridad es mínima - o ni siquiera existe - merece la pena invertir tiempo y por qué no, dinero, para garantizar un mínimo nivel de seguridad que proporcione un entorno de trabajo aceptable.

Las redes de I+D tienen una característica propia que no poseen otras redes, por ejemplo, las militares o las pertenecientes a empresas. El rasgo diferenciador de redes I+D más importante es su carácter extremadamente abierto; mientras que una empresa puede limitar el acceso exterior a través de un simple firewall u ofrecer sólo determinados servicios al exterior de la empresa, con unas páginas web, una red de I+D no puede permitirse este carácter tan cerrado. Esto es debido a que el aspecto de la seguridad más importante en las redes de investigación es la disponibilidad de su información; a todo el personal investigador le interesa que sus publicaciones sean lo más accesibles a través de la web; al alumnado le interesa poder consultar sus datos académicos desde casa, por Internet, etc. Y es muy difícil hacerles cambiar de opinión, o al menos concientizarlos de los problemas de seguridad que una excesiva apertura supone; si un profesor acude a una conferencia en cualquier lugar del mundo no se le puede obligar, por ejemplo, a limitar el acceso de todas las aplicaciones de su equipo portátil para poder leer el correo a distancia; simplemente desea ejecutar un telnet, igual como si estuviera en el campus, para hacerlo.

La característica que acabamos de comentar es negativa de cara a mantener la seguridad de los sistemas de información; no podemos limitarnos a establecer una férrea política de filtrado de paquetes o a restringir servicios, ya que los usuarios no van a aceptarlo. Sin embargo, no todas las características de las redes de I+D son un problema para su seguridad; por ejemplo, un importante punto a favor es el escaso interés para un pirata de los datos con los que se trabaja generalmente en institutos de investigación o centros universitarios. En entornos de estas características no se suele trabajar con datos que

impliquen información valiosa para un espía industrial o militar, ni tampoco se mueven grandes cantidades de dinero a través del comercio electrónico; casi todo lo que un intruso va a encontrar en un sistema de información de I+D son programas, documentos, resultados de simulaciones que a muy poca gente, aparte de sus autores, interesan.

Entonces, ¿contra quién nos enfrentamos?. Muy pocos de los intrusos que podamos encontrar en redes de I+D son piratas expertos; la mayoría son gente poco experimentada, que incluso ataca nuestros sistemas de información desde sus PC's en casa, sin saber nada sobre sistemas de información ni redes. La mejor defensa contra estos individuos consiste simplemente en cerrar los servicios que no sean estrictamente necesarios y mantener actualizado el software de nuestros sistemas de información que se puedan considerar crítico (sistema operativo, demonios, parches, antivirus, service packs, etc.) Casi todos ellos suelen actuar únicamente por el afán de conseguir un cierto status en comunidades virtuales de piratas, ni siquiera actúan por curiosidad o para ampliar sus conocimientos, con lo que tenemos una importante ventaja contra ellos; es muy raro - pero no imposible - que se obsesionen por nuestro sistema de información o por la red, de forma que si conseguimos que sus primeros intentos por acceder no sean fructíferos directamente dejarán el ataque para dedicarse a objetivos más fáciles. En cuanto a los piratas con un mayor nivel de conocimientos, si los encontramos en una red de I+D seguramente será porque utilizan nuestros equipos como plataforma para atacar sistemas de información más interesantes para un intruso, como los sistemas de información militares o de centros de investigación muy importantes, como la NASA; en estos casos es obligatorio poner sobre aviso al organismo de mayor nivel responsable de la seguridad de la red o del sistema de información.

1.5.2 Redes Empresariales

Las redes y los sistemas de información pertenecientes a empresas son, a priori, las que mayores ventajas presentan en lo relativo a su protección; en primer lugar, se trata de redes que suelen ser muy aislables; muchas empresas disponen de una LAN en el edificio donde están ubicadas, red que se puede aislar perfectamente del exterior mediante cortafuegos. Incluso si se han de ofrecer servicios hacia el exterior (típicamente, correo electrónico y web), se pueden situar los sistemas de información en una zona desmilitarizada entre el router y la red interna. Además, en muchos casos la LAN de la empresa ni siquiera es realmente necesario que esté conectada a Internet, aunque esto cada día es menos habitual más por requisitos humanos

que técnicos; aunque no haga falta para el trabajo la conexión a Internet, el clima de descontento entre nuestro personal que puede suponer bloquear el acceso hacia el exterior es una gran traba de cara al aislamiento - y por tanto, a la seguridad -.

Esta es la teoría; como siempre, casi perfecta; vamos a añadirle problemas reales para comprobar que las cosas no son tan bonitas como las acabamos de pintar. En primer lugar imaginemos una empresa con varias sucursales - oficinas, almacenes - separadas geográficamente. Si la distancia entre todas ellas es corta y la empresa solvente, quizás se puedan permitir una red propia, dedicada y protegida por los técnicos de la propia compañía, pero esto, rara vez es así; conforme aumenta la separación, la idea de la red dedicada se va difuminando (simplemente con una distancia de un par de kilómetros - o menos, dependiendo de la zona - ya resulta imposible esta aproximación.) Ahora entra en juego una red de propósito general como base de comunicaciones, seguramente la red telefónica, o incluso Internet; la protección de la red ya no depende exclusivamente de nuestra organización, sino que entran en juego terceras compañías - posiblemente telefónica, con todo lo que ello implica.-. Es casi indispensable recurrir a redes privadas virtuales (Virtual Private Networks, VPN), canales de comunicación seguros dentro de esa red insegura. Al menos podemos mantener comunicaciones seguras entre las diferentes sucursales, pero no todas las compañías recurren a estos mecanismos realmente, es más fácil utilizar la red de propósito general como si fuera segura, enviando por ella toda la información que queramos intercambiar entre oficinas, sin proteger. Además, la seguridad no suele ser tangible; seguramente nuestro jefe estará más contento si en un día tiene montada la red aunque sea insegura, sin esperar a la configuración de la red privada - evidentemente, más costosa -, aunque a la larga resulte una solución mucho peor.

Compliquemos aún más la seguridad de nuestra hipotética compañía; ahora entran en juego estaciones móviles, por ejemplo personal con equipos portátiles que deben comunicarse con los sistemas de información, o ejecutivos que al salir de viaje de negocios quieren poder seguir leyendo su correo. Estos equipos portátiles están dando muchos dolores de cabeza, tanto en el ámbito de conectividad como de seguridad. Otro potencial problema para nuestra empresa, realmente no tan potencial seguramente es esa persona que está de viaje, la cual acabará conectando su portátil a la línea telefónica de un hotel y conectándose a los sistemas de información vía módem. Por supuesto, esa persona ni ha oído, ni quiere oír hablar de conexiones cifradas; es más fácil un telnet o un rlogin hacia el sistema de información para

poder leer el correo; a fin de cuentas, los piratas son algo que sólo existe en las películas.

Hasta ahora todos los ataques contra la empresa eran - en principio - externos; pero imaginemos que uno de nuestros empleados no está contento con su sueldo y decide irse a la competencia. Y no sólo quiere irse, sino que decide llevarse varios documentos confidenciales, documentos a los que ha tenido un fácil acceso simplemente acercándose a una de las impresoras comunes, recogiendo los listados y fotocopiándolos antes de entregarlos a su dueño. O incluso más fácil en nuestra empresa los equipos de los empleados utilizan Windows y todos los equipos ofrecen los discos duros como recursos compartidos; a fin de cuentas, así es mucho más fácil el intercambio de información entre empleados. Esa persona, sin ni siquiera levantarse de su lugar de trabajo, tiene acceso a casi toda la información de nuestra empresa. Por cierto, esto no pretende ser un ataque a la seguridad de estos productos (aunque fácilmente podría serlo), sino una realidad que se puede ver en muchísimas empresas, sobre todo pequeñas y medianas.

Como acabamos de ver, ha sido suficiente con plantear un par de situaciones - de lo más normales - para romper toda la idea de seguridad fácil que teníamos al principio y eso sin plantear problemas más rebuscados; que sucede si a una empresa de la competencia le da por sabotear nuestra imagen atacando nuestras páginas web y si le interesa leer nuestros e-mail, no hace falta que se trate de una multinacional poderosa dispuesta a contratar piratas profesionales, es suficiente con que el administrador de la red de nuestra competencia tenga unas nociones sobre seguridad y bastantes ganas de fastidiarnos.

1.5.3 Redes ISP's

Las empresas dedicadas a ofrecer acceso a Internet a través de la línea telefónica, así como otros servicios de red (principalmente hospedaje de páginas web), son los conocidos ISP's (Internet Service Providers); conocidos tanto por sus servicios como por su inseguridad. Y es que realmente no es fácil compaginar una amplia oferta de servicios con una buena seguridad; cualquier administrador de un sistema de información sabe que cada puerto abierto en su sistema es una potencial fuente de problemas para el mismo, por lo que conviene reducir al mínimo su número. Si los ISP's viven justamente de permitir accesos - a Internet o a sus propios servidores - parece obvio que no podrán aplicar estrictas políticas de seguridad en los equipos; mientras que por ejemplo en una empresa el administrador puede obligar - relativamente - a sus usuarios a utilizar protocolos cifrados, si un ISP no

permite acceso ftp a los clientes que deseen colgar sus páginas web y les obliga a usar un protocolo de transferencia de archivos que aplique criptografía, es muy probable que muchos de esos clientes abandonen y se vayan a la competencia; es más fácil utilizar el ftp clásico que instalar software adicional para poder actualizar una página web.

Imaginemos un proveedor que ofrece conexión a Internet a sus clientes; sin duda esos clientes querrán conectarse a páginas web, transferir archivos o utilizar telnet. Nada problemático a primera vista; las conexiones se realizan hacia el exterior de nuestra red, no hacia el interior. Pero además esos clientes querrán chatear, instalar servidores de todo tipo en sus equipos para que sus amigos los utilicen - desde servicios web hasta NFS (Network File Systems) -, con lo que empiezan los primeros problemas. Y no nos quedamos aquí, seguramente quieren poder descargar su correo POP3 desde cualquier lugar, no sólo desde el rango de direcciones del proveedor (por supuesto, sin oír hablar de cifrado en la conexión) y también les hace gracia un espacio para publicar sus páginas web de forma permanente y mucho mejor para ellos si se les permite programar e instalar sus propias interfaces de aplicaciones en dichas páginas; aquí ya no hay opción, o simplemente se les niega esta última posibilidad, o si se les permite y deseamos un entorno medianamente seguro hemos de dedicar recursos - y no pocos - a verificar la seguridad de esos programas. Hagamos lo que hagamos, tenemos problemas, si no permitimos que los usuarios usen sus propias interfaces de aplicaciones y otro proveedor sí que lo permite, seguramente cambiarán de ISP. Si revisamos la seguridad, tampoco les va a hacer gracia tener que modificar su programa una y otra vez hasta que lo consideremos seguro; a fin de cuentas, estarán modificándolo para conseguir algo que probablemente ni siquiera entiendan.

Sigamos añadiendo problemas; puestos a pedir, los usuarios también pueden solicitar acceso a bases de datos en sus páginas, por ejemplo vía PHP3; ya nos afectan los problemas que pueda tener este tipo de software. Incluso pueden querer instalar sistemas completos de comercio electrónico, sistemas capaces de convertir nuestra red en un auténtico agujero. Es más, si se permite el hospedaje de equipos es muy probable que el cliente que usa este servicio quiera acceder remotamente vía telnet - o peor, rlogin -, incluso para tareas de administración; ni oír hablar de cosas como SSH o SSL telnet; a fin de cuentas, hacen lo mismo y son más complicados que un sencillo telnet.

La seguridad de los ISP’s sufre además el problema clásico de la seguridad en cualquier entorno, pero quizás de una forma mucho más grave; estamos trabajando con algo intangible, con algo muy difícil de

ver. Si se realiza una inversión de tiempo o dinero para adquirir equipos nuevos, la mejora se nota inmediatamente; si esa inversión se realiza para incrementar la seguridad, quizás las mejoras obtenidas nunca las pueda notar un usuario. Y si las nota, con toda probabilidad es peor, es porque han fallado. La mayor parte de los potenciales clientes de un ISP preferirá una conexión un poco más rápida frente a una conexión o unos servicios más seguros.

Con situaciones tan sencillas y comunes como las anteriores podemos hacernos una idea de la potencial inseguridad de los ISP's, se trata de problemas reales, no meramente teóricos, en ambientes undergrounds no es raro encontrar piratas con casi todas - o con todas - las claves de los clientes de un proveedor. Sólo tenemos un punto a nuestro favor, si se puede considerar así; hace un par de años esas claves eran algo más o menos valioso para un pirata, ya que con ellas conseguía un acceso a Internet gratuito y - más importante - si dar ninguno de sus datos. Hoy en día y debido a empresas que ofrecen ese tipo de acceso - por ejemplo como Alehop, con unas contraseñas genéricas y gratuitas para todo el mundo -, las claves de los clientes de un ISP no son tan codiciadas.

CAPÍTULO II

Consideraciones de la Seguridad de los Sistemas de Información

En Febrero del 2001, la IIA (Instituto de Auditores Internos) y sus organizaciones asociadas publicaron un reporte acerca de las 10 consideraciones que los Gerentes de empresas deberían tomar en cuenta para las acciones a tomar a favor de la seguridad de sus sistemas de información.

En el presente proyecto se proveen respuestas a estas 10 consideraciones, las cuales se describen a continuación:

2.1 Responsabilidad

¿Quién es responsable por la seguridad de los sistemas de información y cómo nos aseguramos de la responsabilidad del sistema?. La Gerencia es responsable y es parte de sus tareas cuidar y proveer una efectiva protección.

Según Dennis Weatherstone, presidente del comité de auditoría de General Motors, una responsabilidad clara de la Gerencia es fundamental, si usted mira los últimos problemas en seguridad de la información, eran debido a una carencia de la responsabilidad dentro de la organización. También hemos aprendido que tenemos que tener una definición más exacta del papel del comité de auditoría en esta materia y precisar cómo trabajará con los auditores internos, el departamento jurídico y el CIO (director de sistemas.) Finalmente, es también importante conseguir respaldo y la discusión con los interventores externos.

2.2 Conocimiento

¿Cómo nos aseguramos que todos los involucrados entiendan la importancia de la seguridad de la información?. El conocimiento de la seguridad debe comenzar con la alta Gerencia e impregnar los valores de la organización y su cultura.

Algunos expertos de la seguridad de la información creen que alrededor del 80% de los problemas de la seguridad provienen de la carencia de entendimiento o descuido y no de un ataque. Los ejemplos como el virus "I love you" (que infectó solamente a los que abrieron un mensaje inesperado y su documento anexo), una administración descuidada, el compartir palabras clave y dejar los equipos conectados y desatendidos son los ejemplos peligrosos, sobre todo comunes de la necesidad del mayor conocimiento de la seguridad.

2.3 ¿Qué está haciendo la Gerencia para asegurar el uso ético de la Información?

La alta Gerencia debe considerar que sus normas corporativas de la conducta estén reflejadas en el uso de equipos como en el resto de las actividades. Los propietarios y los usuarios de la información merecen el tratamiento ético tanto en línea como cuando no. La Gerencia debe asegurarse de que las políticas con respecto al uso ético de la información abarquen propiedad, asuntos de privacidad y una consideración de cómo los sistemas y la información se pueden manipular o utilizar de otra manera en detrimento de una organización, de sus accionistas, de los clientes o de los socios de negocio.

Debido a que la cadena de seguridad es solamente tan fuerte como su conexión más débil, permitir que los componentes débiles sean parte de la infraestructura, pone a nuestras organizaciones y a nuestros vecinos en riesgo. Las cortes judiciales comenzarán pronto a encontrar a propietarios de computadoras responsables negligentemente de permitir que sus equipos sean una plataforma de lanzamiento para los ataques de los hackers, de los terroristas y de otros.

2.4 Inclusión

¿Cómo tomamos en cuenta las preocupaciones de todas las partes afectadas al desarrollar nuestra política de la seguridad de la información?. La seguridad de la información se alcanza con los esfuerzos combinados de los propietarios de los sistemas de información, de los usuarios, de los guardianes y del personal responsable de la seguridad y está en la mente de los clientes, de socios y de los accionistas.

Las políticas de seguridad deben definirse sin perder de vista lo que se necesita proteger de un sistema de información, para ello es necesario realizar un análisis exhaustivo de todos los elementos involucrados en el entorno externo e interno de un sistema de información con el fin de cumplir con los tres objetivos de la seguridad: confidencialidad, integridad y disponibilidad. Este análisis se debe realizar con base a lo indicado en la figura 2.1.

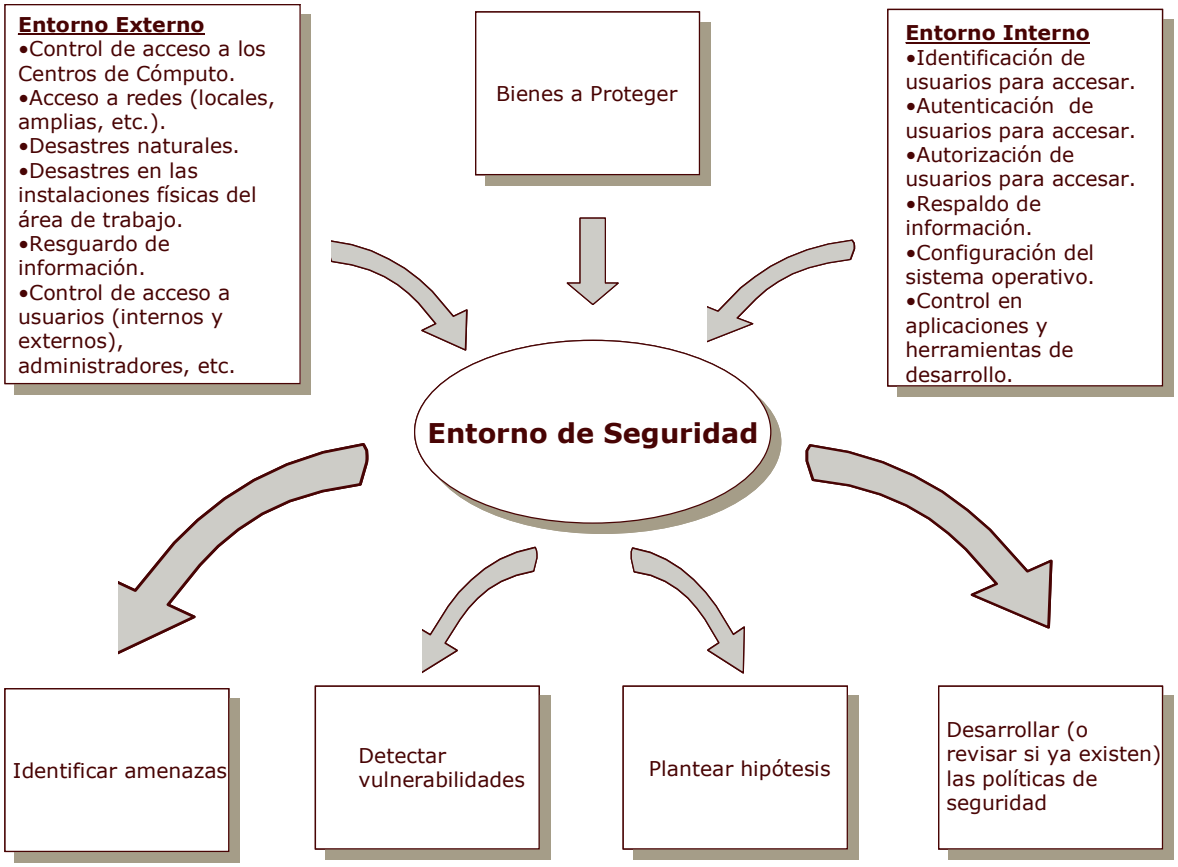

Figura 2.1 Análisis del Entorno de Seguridad

2.5 Asignación de Recursos

¿Cómo nos aseguramos que las inversiones en seguridad sean conmensuradas con los riesgos?. La decisión de los recursos que se invertirán en seguridad de la información se toma de igual manera que como cualquier otra asignación para la compra de activos, por medio de recomendaciones de la Gerencia.

¿Cuánta seguridad es necesaria?. Puede ser una de las preguntas más críticas y difícil de contestar. Hay muchos más riesgos a los sistemas de información que pueden ser tratados con eficacia y no hay un estándar uniforme o ninguna metodología global para definirlos.

Es muy conveniente identificar y cuantificar los bienes a proteger ya que de ello dependerá la inversión que la organización realizará para su protección. Por lo que es necesario realizar un levantamiento de la siguiente información (cabe mencionar que los puntos citados a continuación serán analizados más a detalle en el capítulo 3 del presente trabajo):

- ¿Cuánto tiempo máximo debe ser considerado para que un sistema de información este indisponible (es decir sin proporcionar servicio) sin poner en riesgo a la organización?

- ¿Cuánta información y de que tipo estaría dispuesta a perder la organización sin poner en riesgo a la misma?

- ¿Qué posibilidad existe de que se pierda información de los sistemas de información?

- ¿Qué información estaría dispuesta la organización a que fuera conocida por intrusos sin poner en riesgo a la misma?

- ¿Qué posibilidad existe de que se caiga el edificio en donde se encuentran los sistemas de información?

- ¿Qué posibilidad existe de que se incendie el edificio?

- ¿Qué posibilidad existe de que se inunde el edificio?

- ¿Qué posibilidad existe de que se caiga la red?

- ¿Qué posibilidad existe de que se caiga el sistema de información?

- ¿Qué posibilidad existe de que se pierda información de los sistemas de información?

- ¿Qué posibilidad existe de que un intruso ingrese a las instalaciones de la organización, accede a la red y a los sistemas de información en donde se encuentra información privilegiada y/o confidencial e inclusive la altere (modifique o borre) y la extraiga?

Todos los puntos citados anteriormente deben ser ponderados entre uno y cien por ciento de probabilidad de que sucedan, de tal manera que la relación entre las posibilidades y lo que se estaría dispuesto a perder indiquen el valor de los bienes informáticos para la organización y se convierte en un factor determinante de la inversión a realizar.

2.6 Continuidad

¿Cómo la Gerencia integra la seguridad de la información en todas las políticas?. Como cualquier proceso de la Gerencia de riesgo, la seguridad de la información se debe integrar completamente en todas

las políticas de la organización, que solamente puede ocurrir cuando el sentido de la seguridad se desarrolla en todos los niveles. La seguridad es un asunto global, incluyendo la cultura corporativa, gente, entrenamiento, procesos y comunicaciones; ubicándose más allá del hardware, software y asuntos técnicos. Bruce Harreld de IBM dijo: "establecemos políticas claras de la seguridad y guías de consulta detalladas y comunicamos esto a todos nuestros empleados. Un elemento importante de esto son los Gerentes de línea que comunicándose con los expertos en el área de seguridad, que ayudan a colocar los correctivos, independientemente si esos expertos son internos o externos."

2.7 Eficacia

¿Cómo aseguramos que los incidentes de seguridad no ponen en peligro la organización, sus unidades de negocio, aliados, socios, o sus activos de la información, ni deterioramos su capacidad de funcionar?. Los riesgos se deben atenuar en el costo apropiado basado en los sistemas de información en uso, su criticidad, el valor y la sensibilidad de los datos y enlaces a otros sistemas de información. Es trabajo de la Gerencia asegurar niveles apropiados de seguridad constante de la información.

Desarrollando y manteniendo las políticas de la seguridad de modo que la seguridad pueda desempeñar su papel, tal como las funciones de auditoría, garantía de calidad, protección ambiental, privacidad y de la redundancia. Se basa en un proceso sólido de la revisión continua. Entender los riesgos y hacer análisis en curso de costo versus beneficios de los controles, son las bases de una configuración sana, necesarias para responder apropiadamente a los incidentes de seguridad.

2.8 Evaluación Constante

No existe nunca un final al evaluar la seguridad de la información. El paso rápido de la tecnología hace necesario la actualización y mantenimiento continuos. La Gerencia, debe determinar el punto máximo económico al asignar recursos. Siempre existe una relación costo-beneficio entre los sacrificios a hacer y la necesidad de asignar prioridades y enfocar recursos a los activos que deben ser protegidos.

¿Cómo nos aseguramos de una evaluación constante de los riesgos de la información y las amenazas?. La alta Gerencia, o un comité apropiado de la alta Gerencia, debe requerir reportes periódicos de la

Gerencia de riesgos y reportes independientes de auditores tanto internos como externos.

Es muy importante que la Gerencia defina los lineamientos en cuanto a seguridad en los sistemas de información se refiere, a esto se le conoce como definición de las políticas de seguridad. Estas políticas de seguridad deben contemplar los puntos a cumplir del entorno externo e interno de un sistema de información - éstos se mencionarán más a detalle en el capítulo 3 y 4 del presente trabajo -, así mismo éstas políticas deben indicar la periodicidad en que se deben realizar y monitorear para su cumplimiento.

Por otro lado debe existir un área dentro de la organización dedicada a la seguridad informática que además de dar guía en la definición y cumplimiento de las políticas de seguridad en los sistemas de información se dedique a vigilar el cumplimiento de las mismas a través de revisiones periódicas – auditorías internas – Finalmente ésta misma área debe solicitar auditorías externas a una empresa, organización o equivalente que se dedique a esto; con el fin de realizar una evaluación del cumplimiento de las políticas de seguridad de alguien externo al área. El resultado de estas auditorías debe ayudar en la mejora continua de la definición y cumplimiento de las políticas de seguridad de los sistemas de información para ofrecer una mayor protección y disponibilidad a los sistemas de información con respecto a las amenazas de los avances tecnológicos.

2.9 Cumplimiento

¿Cómo nos aseguramos que nuestras medidas de seguridad de la información sean justas y legales?. Al nivel de la alta Gerencia, la parte legal y reguladora se asigna a menudo al comité de auditoría, que alternadamente trabaja de cerca con los auditores externos e internos para asegurar conformidad. Los estándares para la conformidad, revisión y monitoreo, se deben construir dentro de la configuración total de la seguridad para asegurarse de que las respuestas resuelven cualquier requisito legal u otros lineamientos aplicables.

Existen reglas internacionales que se aplican a los miembros de la alta Gerencia que comentan los llamados “crímenes de cuello blanco”, los cuales se aplican cuando se es negligente en la protección de los activos de la información. El personal del nivel ejecutivo puede también ser encontrado responsable, castigado con multas o el encarcelamiento.

2.10 Distribución de Información

¿Cómo compartimos la información apropiada con nuestros socios de negocio y las entidades gubernamentales?. El compartir de la información es una práctica común y se puede lograr por una variedad de medios tales como al interactuar con los grupos de la industria, asistiendo a reuniones, conferencias y trabajando activamente con los entes reguladores.

En muchos casos, los requisitos para reportar a las entidades gubernamentales se explican claramente. El formato y el contenido de informes no son ningún problema siempre que la organización tenga una metodología para recopilar y conservar estos datos en primer lugar. Es duro compartir la información que usted no tiene, así que el monitoreo y la vigilancia de la información sobre la seguridad, es crítica.

CAPÍTULO III

Seguridad en el Entorno Operativo de un Sistema de Información

3.1 Seguridad Física de los Sistemas de Información

3.1.1 Introducción

Según[14], la seguridad física de los sistemas de información consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial. Más claramente por "seguridad física" podemos entender todos aquellos mecanismos - generalmente de prevención y detección - destinados a proteger físicamente cualquier recurso del sistema de información; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema de información, pasando por la propia CPU del equipo.

Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia a la hora de hablar de seguridad informática en general; en muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema. Esto motiva que en determinadas situaciones un atacante se decline por aprovechar vulnerabilidades físicas en lugar de lógicas, ya que posiblemente le sea más fácil robar una cinta con una imagen completa del sistema de información que intentar acceder a él mediante fallos en el software. Hemos de estar conscientes en que la seguridad física es sumamente importante como para ignorarla: un ladrón que roba una computadora para venderla, un incendio o un pirata que accede sin problema a la sala de operaciones puede hacer mucho más daño que un intruso que intenta conectarse remotamente con un equipo no autorizado; no importa que utilicemos los más avanzados medios de cifrado para conectarnos a nuestros sistemas de información, ni que hayamos definido una política de firewall muy restrictiva: si no tenemos en cuenta factores físicos, estos esfuerzos para proteger nuestra información no van a servir de nada. Además, en el caso de organismos u organizaciones con requerimientos de seguridad medios, unas medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de los piratas: como casi todos los atacantes de los sistemas de información de estos entornos son casuales (esto es, no tienen interés específico sobre nuestros sistemas de información, sino sobre cualquier sistema de información), si notan a través de medidas físicas que

[14] Consultar Bibliografía Libro (12)

nuestra organización está preocupada por la seguridad, probablemente abandonarán el ataque para lanzarlo contra otro sistema de información menos protegido.

Aunque como ya dijimos en la introducción este proyecto no puede centrarse en el diseño de edificios resistentes a un terremoto o en la instalación de alarmas electrónicas, se van a comentar ciertas medidas de prevención y detección que se han de tener en cuenta a la hora de definir mecanismos y políticas para la seguridad de nuestros sistemas de información. Pero hemos de recordar que cada sitio es diferente y por lo tanto también lo son sus necesidades de seguridad; de esta forma, no se pueden dar recomendaciones específicas sino pautas generales a tener en cuenta, que pueden variar desde el simple sentido común (como es el cerrar con llave la sala de operaciones cuando salimos de ella) hasta medidas mucho más complejas, como la prevención de radiaciones electromagnéticas de los equipos o la utilización de degaussers. En entornos habituales suele ser suficiente con un poco de sentido común para conseguir una mínima seguridad física; de cualquier forma, en cada institución se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado. Por ejemplo, en una empresa ubicada en Nueva York quizás parezca absurdo hablar de la prevención ante terremotos (por ser esta un área de bajo riesgo), pero no sucederá lo mismo en una empresa situada en una zona sismicamente activa como México D.F.; de la misma forma, en entornos de redes I+D es absurdo hablar de la prevención ante un ataque nuclear, pero en sistemas militares esta amenaza se ha de tener en cuenta.

3.1.2 Protección del Hardware

El hardware es frecuentemente el elemento más caro de todo sistema de información. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización, especialmente en las dedicadas redes I+D: universidades, centros de investigación, institutos tecnológicos, etc., suelen poseer entre sus sistemas de información equipos muy caros, desde servidores con una gran potencia de cálculo hasta routers de última tecnología, pasando por modernos sistemas de transmisión de datos como la fibra óptica.

Son muchas las amenazas al hardware de una instalación informática; aquí se van a presentar algunas de ellas, sus posibles

efectos y algunas soluciones, si no para evitar los problemas sí al menos para minimizar sus efectos.

3.1.2.1 Acceso Físico

La posibilidad de acceder físicamente a un sistema de información - en general, a cualquier sistema operativo - hace inútiles casi todas las medidas de seguridad que hayamos aplicado sobre él: hemos de pensar que si un atacante puede llegar con total libertad hasta un equipo puede por ejemplo abrir la CPU y llevarse un disco duro; sin necesidad de privilegios en el sistema, sin importar la robustez de nuestro firewall, sin una clave de usuario, el atacante podrá seguramente modificar la información almacenada, destruirla o simplemente leerla. Incluso sin llegar al extremo de desmontar el equipo, que quizás resulte algo exagerado en entornos clásicos donde hay cierta vigilancia, como un laboratorio, sala de informática o centro de cómputo, la persona que accede al equipo puede pararlo o arrancar una versión diferente del sistema operativo sin llamar mucho la atención. Si por ejemplo, alguien accede a un laboratorio con equipos Linux, seguramente le resultará fácil utilizar un disco de arranque, montar los discos duros del equipo y extraer de ellos la información deseada; incluso es posible que utilice un disco externo con ciertas utilidades que constituyan una amenaza para otros equipos, como nukes o sniffers (analizadores de redes.)

Visto esto, parece claro que cierta seguridad física es necesaria para garantizar la seguridad global de la red y los sistemas de información conectados a ella; evidentemente el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger (no es necesario hablar de un sólo sistema de información, sino de cualquier elemento físico que se pueda utilizar para amenazar la seguridad, como una toma de red apartada en cualquier rincón de un edificio de nuestra organización.) Mientras que parte de los sistemas de información estarán bien protegidos, por ejemplo los sistemas de información de un departamento o despacho, otros muchos estarán en lugares de acceso semipúblico, como laboratorios de prácticas; es justamente sobre estos últimos donde debemos extremar las precauciones, ya que lo más fácil y discreto para un atacante es acceder a uno de estos equipos y en segundos, lanzar un ataque completo sobre el sistema de información o la red.

3.1.2.1.1 Prevención

¿Cómo prevenir un acceso físico no autorizado a un determinado punto?. Hay soluciones para todos los gustos y también de todos los

precios: desde analizadores de retina hasta videocámaras, pasando por tarjetas inteligentes o control de las llaves que abren determinadas puertas. Todos los modelos de autenticación de usuarios son aplicables, aparte de controlar el acceso lógico a los sistemas, para controlar el acceso físico; de todos ellos, quizás los más adecuados a la seguridad física sean los biométricos y los basados en algo poseído; aunque como comentaremos más tarde suelen resultar algo caros para utilizarlos masivamente en entornos de seguridad media.

Pero no hay que irse a sistemas tan complejos para prevenir accesos físicos no autorizados; normas tan elementales como cerrar las puertas con llave al salir de un laboratorio o un despacho o bloquear las tomas de red que no se suelan utilizar y que estén situadas en lugares apartados son en ocasiones más que suficientes para prevenir ataques. También basta el sentido común para darse cuenta de que el cableado de red es un elemento importante para la seguridad, por lo que es recomendable apartarlo del acceso directo; por desgracia, en muchas organizaciones podemos ver excelentes ejemplos de lo que no hay que hacer en este sentido: cualquiera que pasee por entornos más o menos amplios (el campus de una universidad, por ejemplo) seguramente podrá ver - o pinchar, o cortar - cables descolgados al alcance de todo el mundo, especialmente durante el verano, época que se suele aprovechar para hacer obras.

Todos hemos visto películas en las que se muestra un estricto control de acceso a instalaciones militares mediante tarjetas inteligentes, analizadores de retina o verificadores de la geometría de la mano; aunque algunos de estos métodos aún suenen a ciencia-ficción y sean demasiado caros para la mayor parte de entornos (recordemos que si el sistema de protección es más caro que lo que se quiere proteger tenemos un grave error en nuestros planes de seguridad), otros se pueden aplicar y se aplican, en muchas organizaciones. Concretamente, el uso de lectores de tarjetas para poder acceder a ciertas dependencias es algo muy a la orden del día; la idea es sencilla: alguien pasa una tarjeta por el lector, que conecta con un sistema de información - por ejemplo una computadora - en la que existe una base de datos con información de los usuarios y los recintos a los que se le permite el acceso. Si la tarjeta pertenece a un usuario capacitado para abrir la puerta, ésta se abre y en caso contrario se registra el intento y se niega el acceso. Aunque este método quizás resulte algo caro para extenderlo a todos y cada uno de los puntos a proteger en una organización, no sería tan descabellado instalar pequeños lectores de códigos de barras conectados a un equipo en las puertas de muchas áreas, especialmente en las que se maneja información más o menos sensible. Estos lectores

podrían leer una tarjeta que todos los miembros de la organización poseerían, conectar con la base de datos de usuarios y autorizar o denegar la apertura de la puerta. Se trataría de un sistema sencillo de implementar, no muy caro y que cubre de sobra las necesidades de seguridad en la mayoría de los entornos: incluso se podría abaratar si en lugar de utilizar un mecanismo para abrir y cerrar puertas el sistema se limitará a informar al administrador del área o a un guardia de seguridad mediante un mensaje en pantalla o una luz encendida: de esta forma los únicos gastos serían los correspondientes a los lectores de códigos de barras, ya que como equipo con la base de datos se puede utilizar un equipo viejo o un servidor de propósito general.

3.1.2.1.2 Detección

Cuando la prevención es difícil por cualquier motivo (técnico, económico, humano) es deseable que un potencial ataque sea detectado cuanto antes, para minimizar así sus efectos. Aunque en la detección de problemas, generalmente accesos físicos no autorizados, intervienen medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas, en entornos más normales el esfuerzo en detectar estas amenazas se ha de centrar en las personas que utilizan los sistemas y en las que sin utilizarlos están relacionadas de cierta forma con ellos; sucede lo mismo que con la seguridad lógica: se ha de ver toda la protección como una cadena que falla si falla su eslabón más débil.

Es importante concienciar a todos de su papel en la política de seguridad del entorno; si por ejemplo un usuario autorizado detecta la presencia de alguien quien sospecha que no tiene autorización para estar en una determinada estancia debe avisar inmediatamente al administrador o al responsable de los equipos, que a su vez puede avisar al servicio de seguridad si es necesario. No obstante, utilizar este servicio debe ser solamente un último recurso: generalmente en la mayoría de los entornos no estamos tratando con terroristas, sino por fortuna con elementos mucho menos peligrosos. Si cada vez que se sospecha de alguien se avisa al servicio de seguridad esto puede repercutir en el ambiente de trabajo de los usuarios autorizados estableciendo cierta presión que no es en absoluto recomendable; un simple "¿puedo ayudarle en algo?"; suele ser más efectivo que un guardia solicitando una identificación formal. Esto es especialmente recomendable en lugares de acceso restringido, como laboratorios de investigación o centros de cálculo, donde los usuarios habituales suelen conocerse entre ellos y es fácil detectar personas ajenas al entorno.

3.1.2.2 Desastres Naturales

En el anterior punto hemos hecho referencia a accesos físicos no autorizados a zonas o a elementos que pueden comprometer la seguridad de los sistemas de información o de toda la red; sin embargo, no son estas las únicas amenazas relacionadas con la seguridad física. Un problema que no suele ser tan habitual, pero que en caso de producirse pueden acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su (falta de) prevención.

3.1.2.2.1 Terremotos

Los terremotos son el desastre natural con mayor probabilidad en la mayoría de los organismos ubicados en México D.F., simplemente por su localización geográfica: nos encontramos en una zona donde suelen producirse temblores de intensidad considerable; incluso en zonas del sur del país, como Michoacán, Oaxaca o Guerrero, donde la probabilidad de un temblor es más elevada, en nuestro país los terremotos pueden alcanzan la magnitud necesaria para causar daños en los equipos. Por lo tanto, hay que tomar las medidas necesarias contra los movimientos sísmicos, ya que la probabilidad de que sucedan es un tanto elevada, por ello vale la pena invertir dinero para minimizar sus efectos.

De cualquier forma, aunque algunas medidas contra terremotos son excesivamente caras para la mayor parte de las organizaciones en México (evidentemente serían igual de caras en zonas como Los Angeles, pero allí el costo estaría justificado por la alta probabilidad de que se produzcan movimientos de magnitud considerable), no cuesta nada tomar ciertas medidas de prevención; por ejemplo, es muy recomendable no situar nunca equipos delicados en superficies muy elevadas (aunque tampoco es bueno situarlos a ras del suelo, como veremos al hablar de inundaciones.) Si lo hacemos, un pequeño temblor puede tirar desde una altura considerable un complejo hardware, lo que con toda probabilidad lo inutilizará; puede incluso ser conveniente (y barato) utilizar fijaciones para los elementos más críticos, como las CPU's, los monitores o los routers. De la misma forma, tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos, ya que si lo que cae son esos objetos también dañarán el hardware.

Para evitar males mayores ante un terremoto, también es muy importante no situar equipos cerca de las ventanas: si se produce un temblor pueden caer por ellas, y en ese caso la pérdida de datos o hardware pierde importancia frente a los posibles accidentes - incluso

mortales - que puede causar una pieza voluminosa a las personas a las que les cae encima. Además, situando los equipos alejados de las ventanas estamos dificultando las acciones de un potencial ladrón que se descuelgue por la fachada hasta las ventanas, ya que si el equipo estuviera cerca no tendría más que alargar el brazo para llevárselo.

Quizás hablar de terremotos en un trabajo dedicado a sistemas "normales" especialmente centrándonos en lugares con escasa actividad sísmica pueda resultar incluso gracioso, o cuanto menos exagerado. No obstante, no debemos entender por terremotos únicamente a los grandes desastres que derrumban edificios y destrozan vías de comunicación; quizás sería más apropiado hablar incluso de vibraciones, desde las más grandes (los terremotos) hasta las más pequeñas (un simple motor cercano a los equipos.) Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas y/o tarjetas. Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con hardware más mecánico, como las impresoras: estos dispositivos no paran de generar vibraciones cuando están en funcionamiento, por lo que situar una pequeña impresora encima de la CPU de un equipo es una idea muy mala. Como dicen algunos expertos en seguridad[15], el espacio en la sala de operaciones es un problema sin importancia comparado con las consecuencias de fallos en un disco duro o en la placa base de un equipo.

3.1.2.2.2 Tormentas Eléctricas

Las tormentas eléctricas, especialmente frecuentes en verano (cuando mucho personal se encuentra de vacaciones, lo que las hace más peligrosas) generan subidas súbitas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica, como veremos a continuación. Si cae un rayo sobre la estructura metálica del edificio donde están situados nuestros equipos es casi seguro que podemos ir pensando en comprar otros nuevos; sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede

[15] Consultar Bibliografía Libro (9)

inducir un campo magnético lo suficientemente intenso como para destruir hardware incluso protegido contra voltajes elevados.

Sin embargo, las tormentas poseen un lado positivo: son predecibles con más o menos exactitud, lo que permite a un administrador parar sus equipos y desconectarlos de la línea eléctrica. Entonces, ¿cuál es el problema?. Aparte de las propias tormentas, el problema son los responsables de los equipos: la caída de un rayo es algo poco probable - pero no imposible - en una gran ciudad donde existen artilugios destinados justamente a atraer rayos de una forma controlada; tanto es así que mucha gente ni siquiera ha visto caer cerca un rayo, por lo que directamente tiende a asumir que eso no le va a suceder nunca y menos a sus equipos. Por lo tanto, muy pocos administradores de los sistemas de información se molestan en parar equipos y desconectarlos ante una tormenta; si el fenómeno sucede durante las horas de trabajo y la tormenta es fuerte, quizás sí que lo hace, pero si sucede un sábado por la noche nadie va a ir a la sala de operaciones a proteger a los equipos y nadie antes se habrá tomado la molestia de protegerlos por una simple previsión meteorológica. Si a esto añadimos lo que antes hemos comentado, que las tormentas se producen con más frecuencia en pleno verano, cuando casi toda la plantilla esta de vacaciones y sólo hay un par de personas de guardia, tenemos el escenario ideal para que una amenaza que a priori no es muy grave, se convierta en el final de algunos de nuestros equipos. Conclusión: todos hemos de tomar más en serio a la naturaleza cuando nos avisa con un par de truenos.

Otra medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, especialmente las copias de seguridad; aunque hablaremos con más detalle de la protección de los backups más adelante, de momento podemos adelantar que se han de almacenar lo más alejados posible de la estructura metálica de los edificios. Un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas nuestras cintas o discos, lo que añade a los problemas por daños en el hardware la pérdida de toda la información de nuestros sistemas de información.

3.1.2.2.3 Inundaciones y Humedad

Cierto grado de humedad es necesario para un correcto funcionamiento de nuestros sistemas de información: en ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que, como veremos más tarde, puede transformar un pequeño contacto

entre una persona y un circuito, o entre diferentes componentes de un equipo, en un daño irreparable al hardware y a la información. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de un equipo.

Controlar el nivel de humedad en los entornos habituales es algo innecesario, ya que por norma nadie ubica computadoras en los lugares más húmedos o que presenten situaciones extremas; no obstante, ciertos equipos son especialmente sensibles a la humedad, por lo que es conveniente consultar los manuales de todos aquellos de los que tengamos dudas. Quizás sea necesario utilizar alarmas que se activan al detectar condiciones de muy poca o demasiada humedad, especialmente en sistemas de información de alta disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial.

Cuando ya no se habla de una humedad más o menos elevada sino de completas inundaciones, los problemas generados son mucho mayores. Casi cualquier medio (un equipo, una cinta, un router, etc.) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos.

Evidentemente, contra las inundaciones las medidas más efectivas son las de prevención (frente a las de detección); podemos utilizar detectores de agua en el piso o pisos falsos de las salas de operaciones y apagar automáticamente los sistemas en caso de que se activen. Tras apagar los sistemas de información podemos tener también instalado un sistema automático que corte la corriente: algo muy común es intentar sacar los equipos - previamente apagados o no - de una sala que se está empezando a inundar; esto, que a primera vista parece lo lógico, es el mayor error que se puede cometer si no hemos desconectado completamente el sistema eléctrico, ya que la mezcla de corriente y agua puede causar incluso la muerte a quien intente salvar a los equipos. Por muy caro que sea el hardware o por muy valiosa que sea la información a proteger, nunca serán magnitudes comparables a lo que supone la pérdida de vidas humanas. Otro error común relacionado con los detectores de agua es situarlos a un nivel superior que a los propios equipos a salvaguardar (incluso en el techo, junto a los detectores de humo); evidentemente, cuando en estos casos el agua llega al detector poco se puede hacer ya por los equipos o la información que contienen.

Medidas de protección menos sofisticadas pueden ser la instalación de un piso falso por encima del piso real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al piso, pero sin llegar a situarlos muy altos por los problemas que ya hemos comentado al hablar de terremotos y vibraciones.

3.1.2.3 Desastres del Entorno

3.1.2.3.1 Electricidad

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; corto-circuitos, picos de tensión, cortes de flujo, a diario amenazan la integridad tanto de nuestro hardware como de los datos que almacena o que circulan por él.

El problema menos común en las instalaciones modernas son las subidas de tensión, conocidas como "picos" porque generalmente duran muy poco: durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el límite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al hardware o a los datos gracias a que en la mayoría de los equipos hay instalados fusibles, elementos que se funden ante una subida de tensión y dejan de conducir la corriente, provocando que el equipo permanezca apagado. Disponga o no de fusibles el equipo a proteger (lo normal es que sí los tenga) una medida efectiva y barata es utilizar tomas de tierra para asegurar aún más la integridad; estos mecanismos evitan los problemas de sobre-tensión desviando el exceso de corriente hacia el suelo de una sala o edificio, o simplemente hacia cualquier lugar con voltaje nulo. Una toma de tierra sencilla puede consistir en un buen conductor conectado a los chasis de los equipos a proteger y a una barra maciza, también conductora, que se introduce lo más posible en el suelo; el costo de la instalación es pequeño, especialmente si lo comparamos con las pérdidas que supondría un incendio que afecte a todos o a una parte de nuestros equipos.

Incluso teniendo un sistema protegido con los métodos anteriores, si la subida de tensión dura demasiado, o si es demasiado rápida, podemos sufrir daños en los equipos; existen acondicionadores de tensión comerciales que protegen de los picos hasta en los casos más extremos y que también se utilizan como filtros para ruido eléctrico. Aunque en la mayoría de las situaciones no es necesario su uso, si nuestra organización tiene problemas por el voltaje excesivo quizás sea conveniente instalar alguno de estos aparatos.

Un problema que los estabilizadores de tensión o las tomas de tierra no pueden solucionar es justamente el contrario a las subidas de tensión: las bajadas, situaciones en las que la corriente desciende por debajo del voltaje necesario para un correcto funcionamiento del sistema de información, pero sin llegar a ser lo suficientemente bajo para que el equipo se apague[16]. En estas situaciones el equipo se va a comportar de forma extraña e incorrecta, por ejemplo; no aceptando algunas instrucciones, no completando escrituras en disco o memoria, etc. Es una situación similar a la de una bombilla que pierde intensidad momentáneamente por falta de corriente, pero trasladada a un sistema de información que en ese pequeño intervalo ejecuta miles o millones de instrucciones y transferencias de datos.

Otro problema, muchísimo más habitual que el anterior en redes eléctricas modernas, son los cortes en el fluido eléctrico que llega a nuestros equipos. Aunque un simple corte de corriente no suele afectar al hardware, lo más peligroso (y que sucede en muchas ocasiones) son las idas y venidas rápidas de la corriente; en esta situación, aparte de perder datos, nuestros sistemas de información pueden sufrir daños.

La forma más efectiva de proteger nuestros equipos contra estos problemas de la corriente eléctrica es utilizar una SAI (Servicio de Alimentación Ininterrumpido) conectada al equipo que queremos proteger. Estos dispositivos mantienen un flujo de corriente correcto y estable, protegiendo así los equipos de subidas, cortes y bajadas de tensión; tienen la capacidad para seguir alimentando los equipos incluso en caso de que no reciban electricidad (evidentemente no las alimentan de forma indefinida, sino durante un cierto tiempo - el necesario - para detener el sistema de forma ordenada.) Por lo tanto, en caso de fallo de la corriente el SAI informará al equipo, que a través de un programa como recibe la información y decide cuanto tiempo de corriente le queda para poder pararse correctamente; si de nuevo vuelve el flujo corriente eléctrica la SAI vuelve a informar de este evento y el sistema desprograma su parada. Así de simple: por poco más de cinco mil dólares podemos obtener una SAI pequeña, más que suficiente para muchos servidores o sistemas de información, que nos va a librar de la mayoría de los problemas relacionados con la red eléctrica.

Un último problema contra el que ni siquiera las SAI's nos protegen es la corriente estática, un fenómeno extraño del que la mayoría de la gente piensa que no afecta a los equipos, sólo a otras personas. Nada más lejos de la realidad: simplemente tocar con la mano

[16] Consultar Bibliografía Libro (13)

la parte metálica del teclado o un conductor de una tarjeta puede destruir un equipo completamente. Se trata de corriente de muy poca intensidad pero un altísimo voltaje, por lo que aunque la persona no sufra ningún daño - sólo un pequeño calambre - el equipo sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM. Contra el problema de la corriente estática existen muchas y muy baratas soluciones: spray antiestático, ionizadores antiestáticos, etc. No obstante en la mayoría de situaciones sólo hace falta un poco de sentido común del usuario para evitar accidentes: no tocar directamente ninguna parte metálica, protegerse si debe hacer operaciones con el hardware, no mantener el entorno excesivamente seco.

3.1.2.3.2 Ruido Eléctrico

Dentro del equipo citado anteriormente podríamos haber hablado del ruido eléctrico como un problema más relacionado con la electricidad; sin embargo este problema no es una incidencia directa de la corriente en nuestros equipos, sino una incidencia relacionada con la corriente de otros equipos que pueden afectar al funcionamiento del nuestro. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros equipos o por multitud de aparatos, especialmente muchos de los instalados en los laboratorios de organizaciones de I+D, y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

Para prevenir los problemas que el ruido eléctrico puede causar en nuestros equipos lo más barato es intentar no situar hardware cercano a la maquinaria que puede causar dicho ruido; si no tenemos más remedio que hacerlo, podemos instalar filtros en las líneas de alimentación que llegan hasta los sistemas de información. También es recomendable mantener alejados de los equipos a dispositivos emisores de ondas como teléfonos móviles, transmisores de radio o walkie-talkies; estos elementos pueden incluso dañar permanentemente a nuestro hardware si tienen la suficiente potencia de transmisión o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

3.1.2.3.3 Incendios y Humo

Una causa casi siempre relacionada con la electricidad son los incendios y con ellos el humo, aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga

de la red debido al gran número de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio o al menos en la planta, donde se encuentran invertidos millones de dólares en equipamiento.

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor. Algunos de ellos, los más antiguos, utilizaban agua para apagar las llamas, lo que provocaba que el hardware no llegara a sufrir los efectos del fuego si los extintores se activaban correctamente, pero quedará destrozado por el agua expulsada. Visto este problema, a mitad de los ochenta se comenzaron a utilizar extintores de halón; este compuesto no conduce electricidad ni deja residuos, por lo que resulta ideal para no dañar los equipos. Sin embargo, también el halón presentaba problemas: por un lado, resulta excesivamente contaminante para la atmósfera, y por otro puede asfixiar a las personas a la vez que acaba con el fuego. Por eso se han sustituido los extintores de halón (aunque se siguen utilizando mucho hoy en día) por extintores de dióxido de carbono, menos contaminante y menos perjudicial. De cualquier forma, al igual que el halón el dióxido de carbono no es precisamente sano para los humanos, por lo que antes de activar el extintor es conveniente que todo el mundo abandone la sala; si se trata de sistemas de activación automática suelen avisar antes de expulsar el compuesto mediante un pitido.

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos: el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos. Quizás ante un incendio el daño provocado por el humo sea insignificante en comparación con el causado por el fuego y el calor, pero hemos de recordar que puede existir humo sin necesidad de que haya un fuego: por ejemplo, en salas de operaciones donde se fuma. Aunque muchos no apliquemos esta regla y fumemos demasiado - siempre es demasiado - delante de nuestros equipos, sería conveniente no permitir esto; aparte de la suciedad generada que se deposita en todas las partes de un equipo, desde el teclado hasta el monitor, generalmente todos tenemos el cenicero cerca de los equipos, por lo que el humo afecta directamente a todos los componentes; incluso al ser algo más habitual que un incendio, se puede considerar más perjudicial - para los equipos y las personas - el humo del tabaco que el de un fuego.

En muchos manuales de seguridad se insta a los usuarios, administradores, o al personal en general a intentar controlar el fuego y salvar el equipamiento; esto tiene, como casi todo, sus pros y sus contras. Evidentemente, algo lógico cuando estamos ante un incendio de pequeñas dimensiones es intentar utilizar un extintor para apagarlo, de forma que lo que podría haber sido una catástrofe sea un simple susto o un pequeño accidente. Sin embargo, cuando las dimensiones de las llamas son considerables lo último que debemos hacer es intentar controlar el fuego nosotros mismos, arriesgando vidas para salvar hardware; como sucedía en el caso de inundaciones, no importa el precio de nuestros equipos o el valor de nuestra información: nunca serán tan importantes como una vida humana. Lo más recomendable en estos casos es evacuar el lugar del incendio y dejar su control en manos de personal especializado.

3.1.2.3.4 Temperaturas Extremas

No hace falta ser un genio para comprender que las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius[17], aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas de información.

Para controlar la temperatura ambiente en el entorno operativo de un sistema de información nada mejor que un equipo de aire acondicionado, aparato que también influirá positivamente en el rendimiento de los usuarios (las personas también tenemos rangos de temperaturas dentro de los cuales trabajamos más cómodamente.) Otra condición básica para el correcto funcionamiento de cualquier equipo es, que éste se encuentre correctamente ventilado sin elementos que obstruyan los ventiladores de la CPU. La organización física del equipo o sistema de información también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

[17] Consultar Bibliografía Libro (9)

3.1.3 Protección de la Información

La seguridad física también implica una protección a la información de nuestro sistema, tanto a la que está almacenada en él como a la que se transmite entre diferentes equipos. Aunque los equipos comentados en la sección anterior son aplicables a la protección física de los datos (ya que no olvidemos que si protegemos el hardware también protegemos la información que se almacena o se transmite por él), hay ciertos aspectos a tener en cuenta a la hora de diseñar una política de seguridad física que afectan principalmente, aparte de a los elementos físicos, a los datos de nuestra organización; existen ataques cuyo objetivo no es destruir el medio físico de nuestro sistema de información, sino simplemente conseguir la información almacenada en dicho medio.

3.1.3.1 Eavesdropping

La interceptación o eavesdropping, también conocida por passive wiretapping[18] es un proceso mediante el cual un agente capta información - en claro o cifrada - que no le iba dirigida; esta captación puede realizarse por muchísimos medios (por ejemplo, capturando las radiaciones electromagnéticas, como lo veremos más adelante.) Aunque es en principio un ataque completamente pasivo, lo más peligroso del eavesdropping es que es muy difícil de detectar mientras que se produce, de forma que un atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta hasta que dicho atacante utiliza la información capturada, convirtiendo el ataque en activo.

Un medio de interceptación bastante habitual es el sniffing, consistente en capturar tramas que circulan por la red mediante un programa ejecutándose en un equipo conectado a ella o bien mediante un dispositivo que se engancha directamente al cableado. Estos dispositivos, denominados sniffers de alta impedancia, se conectan en paralelo con el cable de forma que la impedancia total del cable y el aparato es similar a la del cable solo, lo que hace difícil su detección. Contra estos ataques existen diversas soluciones; la más barata es no permitir la existencia de segmentos de red de fácil acceso, lugares idóneos para que un atacante conecte uno de estos aparatos y capture todo nuestro tráfico. No obstante esto resulta difícil en redes ya instaladas, donde no podemos modificar su arquitectura; en estos existe una solución generalmente gratuita pero que no tiene mucho que ver

[18] Consultar Bibliografía Libro (14)

con el nivel físico: el uso de aplicaciones de cifrado para realizar las comunicaciones o el almacenamiento de la información (hablaremos más adelante de algunas de ellas.) Tampoco debemos descuidar las tomas de red libres, donde un intruso con un equipo portátil puede conectarse para capturar tráfico; es recomendable analizar regularmente nuestra red para verificar que todos los equipos activos están autorizados.

Como soluciones igualmente efectivas contra la interceptación podemos citar el uso de dispositivos de cifrado (no simples programas, sino hardware), generalmente chips que implantan algoritmos; ésta solución es muy poco utilizada en entornos de redes I+D, ya que es muchísimo más cara que utilizar implantaciones de software de tales algoritmos y en muchas ocasiones la única diferencia entre los programas y los dispositivos de cifrado es la velocidad. También se puede utilizar, como solución más cara, el cableado en vacío para evitar la interceptación de datos que viajan por la red: la idea es situar los cables en tubos donde artificialmente se crea el vacío o se inyecta aire a presión; si un atacante intenta "pinchar" el cable para interceptar los datos, rompe el vacío o el nivel de presión y el ataque es detectado inmediatamente. Como decimos, esta solución es enormemente cara y solamente se aplica en redes de perímetro reducido para entornos de alta seguridad.

Antes de finalizar este punto debemos recordar un peligro que muchas veces se ignora: el de la interceptación de datos emitidos en forma de sonido o simple ruido en nuestro entorno de operaciones. Imaginemos una situación en la que los responsables de la seguridad de nuestra organización se reúnen para discutir nuevos mecanismos de protección; todo lo que en esa reunión se diga puede ser capturado por multitud de métodos, algunos de los cuales son tan simples que ni siquiera se contemplan en los planes de seguridad. Por ejemplo, una simple tarjeta de sonido instalada en una PC situado en la sala de reuniones puede transmitir a un atacante todo lo que se diga en esa reunión; mucho más simple y sencillo: un teléfono mal colgado - intencionada o inintencionadamente - también puede transmitir información muy útil para un potencial enemigo. Para evitar estos problemas existen numerosos métodos: por ejemplo, en el caso de los teléfonos fijos suele ser suficiente un poco de atención y sentido común, ya que basta con comprobar que están bien colgados o incluso desconectados de la red telefónica. El caso de los móviles suele ser algo más complejo de controlar, ya que su pequeño tamaño permite camuflarlos fácilmente; no obstante, podemos instalar en la sala de reuniones un sistema de aislamiento para bloquear el uso de estos

teléfonos: se trata de sistemas que ya se utilizan en ciertos entornos (por ejemplo en conciertos musicales) para evitar las molestias de un móvil sonando y que trabajan bloqueando cualquier transmisión en los rangos de frecuencias en los que trabajan los diferentes operadores telefónicos. Otra medida preventiva (ya no para voz, sino para prevenir la fuga de datos vía el ruido ambiente) muy útil - y no muy cara - puede ser sustituir todos los teléfonos fijos de disco por teléfonos de teclado, ya que el ruido de un disco al girar puede permitir a un pirata deducir el número de teléfono marcado desde ese aparato.

3.1.3.2 Backups

En este apartado no vamos a hablar de las normas para establecer una política para realizar copias de seguridad correcta, ni tampoco de los mecanismos necesarios para implantarla o las precauciones que hay que tomar para que todo funcione correctamente; el tema que vamos a tratar en este apartado es la protección física de la información almacenada en backups, esto es, de la protección de los diferentes medios donde residen nuestras copias de seguridad. Hemos de tener siempre presente que si las copias contienen toda nuestra información tenemos que protegerlas igual que protegemos nuestros sistemas.

Un error muy habitual es almacenar los dispositivos de backup en lugares muy cercanos al centro de cómputo o la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (y cómodo si necesitamos restaurar unos archivos) puede convertirse en un problema: imaginemos simplemente que se produce un incendio de grandes dimensiones y todo el edificio queda reducido a cenizas. En este caso extremo tendremos que unir al problema de perder todos nuestros equipos - que seguramente cubrirá el seguro, por lo que no se puede considerar una catástrofe - el perder también todos nuestros datos, tanto los almacenados en los discos duros como los guardados en backups (esto evidentemente no hay seguro que lo cubra.) Como podemos ver, resulta recomendable guardar las copias de seguridad en una zona alejada del centro de cómputo o la sala de operaciones, aunque en este caso descentralicemos la seguridad y tengamos que proteger el lugar donde almacenamos los backups igual que protegemos el propio centro de cómputo o los equipos situados en él, algo que en ocasiones puede resultar caro.

También suele ser común etiquetar las cintas donde hacemos copias de seguridad con abundante información sobre su contenido (sistemas de ficheros almacenados, día y hora de la realización, sistema al que corresponde, etc.); esto tiene una parte positiva y una negativa.

Por un lado, recuperar un fichero es rápido: sólo tenemos que ir leyendo las etiquetas hasta encontrar la cinta adecuada. Sin embargo, si nos paramos a pensar, igual que para un administrador es fácil encontrar el backup deseado también lo es para un intruso que consiga acceso a las cintas, por lo que sí el acceso a las mismas no está bien restringido un atacante lo tiene fácil para sustraer una cinta con toda nuestra información; no necesita saltarse nuestro firewall, conseguir una clave del sistema o chantajear a un operador: nosotros mismos les estamos poniendo en bandeja todos nuestros datos. No obstante, ahora nos debemos plantear la duda habitual: si no etiqueto las copias de seguridad, ¿cómo puedo elegir la que debo restaurar en un momento dado?. Evidentemente, se necesita cierta información en cada cinta para poder clasificarlas, pero esa información nunca debe ser algo que le facilite la tarea a un atacante; por ejemplo, se puede diseñar cierta codificación que sólo conozcan las personas responsables de las copias de seguridad, de tal forma que cada cinta vaya convenientemente etiquetada, pero sin conocer el código sea difícil imaginar su contenido. Aunque en un caso extremo el atacante puede llevarse todos nuestros backups para analizarlos uno a uno, siempre es más difícil disimular una carretilla llena de cintas de 8mm que una pequeña unidad guardada en un bolsillo. Y si aún pensamos que alguien puede sustraer todas las copias, simplemente tenemos que realizar backups cifrados y controlar más el acceso al lugar donde las guardamos.

3.1.3.3 Otros Elementos

En muchas ocasiones los responsables de seguridad de los sistemas de información tienen muy presente que la información a proteger se encuentra en los equipos, en las copias de seguridad o circulando por la red (y por lo tanto toman medidas para salvaguardar estos medios), pero olvidan que esa información también puede encontrarse en lugares menos obvios, como listados de impresora, facturas telefónicas o la propia documentación de un sistema de información.

Imaginemos una situación muy típica en los sistemas de información: un usuario, desde su terminal o el equipo de su despacho, imprime en el servidor un documento de cien páginas, documento que ya de entrada ningún operador comprueba - y quizás no pueda comprobar, ya que se puede comprometer la privacidad del usuario - pero que puede contener, disimuladamente, una copia de nuestro fichero de contraseñas. Cuando la impresión finaliza, el administrador lleva el documento fuera del centro de cómputo o sala de operaciones, pone como portada una hoja con los datos del usuario (login

perfectamente visible, nombre del fichero, hora en que se lanzó la impresión, etc.) y lo deja, junto a los documentos que otros usuarios han impreso - y con los que se ha seguido la misma política - en una estantería perdida en un pasillo, lugar al que cualquier persona puede acceder con total libertad y llevarse la impresión, leerla o simplemente curiosear las portadas de todos los documentos. Así, de repente, se pueden generar bastantes problemas de seguridad derivados de esta política: sin revisar lo que un usuario pueda imprimir - que repetimos, quizás no sea legal, o al menos ético, curiosear -, cualquiera puede robar una copia de un proyecto o un examen, obtener información sobre nuestros sistemas de ficheros y las horas a las que los usuarios suelen trabajar, o simplemente descubrir, simplemente pasando por delante de la estantería, diez o veinte nombres válidos de usuario de nuestros equipos; toda esta información puede ser de gran utilidad para un atacante, que por si fuera poco no tiene que hacer nada para obtenerlas, simplemente darse un paseo por el lugar donde depositamos las impresiones. Esto, que a muchos les puede parecer una exageración, no es ni más ni menos la política que se sigue en muchas organizaciones hoy en día, e incluso en centros de proceso de datos, donde a priori ha de haber una mayor concienciación por la seguridad informática.

Evidentemente, hay que tomar medidas contra estos problemas. En primer lugar, las impresoras, plotters, faxes, teletipos o cualquier dispositivo por el que pueda salir información de nuestro sistema de información ha de estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que envían a estos dispositivos. Sería conveniente que un usuario que recoge una copia se acredite como alguien autorizado a hacerlo, aunque quizás esto puede ser imposible o al menos muy difícil, en grandes sistemas (imaginemos que en un equipo con cinco mil usuarios obligamos a todo aquél que va a recoger una impresión a identificarse y comprobamos que la identificación es correcta antes de darle su documento, con toda seguridad necesitaríamos una persona encargada exclusivamente de este trabajo), siempre es conveniente demostrar cierto grado de interés por el destino de lo que sale por nuestra impresora: sin llegar a realizar un control férreo, si un atacante sabe que el acceso a los documentos está minimamente controlado se lo pensará dos veces antes de intentar conseguir algo que otro usuario ha impreso.

Elementos que también pueden ser aprovechados por un atacante para comprometer nuestra seguridad son todos aquellos que revelen información de nuestros sistemas de información o del personal que los utiliza, como ciertos manuales (proporcionan versiones de los sistemas

operativos utilizados), facturas de teléfono del centro de cómputo (pueden indicar los números de nuestros módems) o agendas de operadores (revelan los teléfonos de varios usuarios, algo muy provechoso para alguien que intente efectuar ingeniería social contra ellos.) Aunque es conveniente no destruir ni dejar a la vista de todo el mundo esta información, si queremos eliminarla no podemos limitarnos a arrojar documentos a la papelera: en el capítulo siguiente hablaremos del basureo, algo que aunque parezca sacado de películas de espías realmente se utiliza contra todo tipo de entornos. Es recomendable utilizar una trituradora de papel, dispositivo que dificulta muchísimo la reconstrucción y lectura de un documento destruido; por poco dinero podemos conseguir uno de estos aparatos, que suele ser suficiente para acabar con cantidades moderadas de papel.

3.2 Administradores, Usuarios y Personal

3.2.1 Introducción

Con frecuencia se suele afirmar y no es una exageración[19], que el punto más débil de cualquier sistema informático son las personas relacionadas en mayor o menor medida con él; desde un administrador sin una preparación adecuada o sin la suficiente experiencia, hasta un guardia de seguridad que ni siquiera tiene acceso lógico al sistema, pero que deja acceder a todo el mundo al centro de cómputo o sala de operaciones, pasando por supuesto por la gran mayoría de usuarios, que no suelen ser conscientes de que la seguridad también les concierne a ellos. Frente a cada uno de estos grupos (administradores, usuarios y personal externo al sistema) un potencial atacante va a comportarse de una forma determinada para conseguir lograr sus objetivos, y sobre cada uno de ellos ha de aplicarse una política de seguridad diferente: obviamente podemos exigir a un administrador de sistemas unos conocimientos más o menos profundos de temas relacionados con la seguridad informática, pero esos conocimientos han de ser diferentes para el guardia de seguridad (sus conocimientos serían referentes a la seguridad física del entorno) y se convierten en simples nociones básicas si se trata de un usuario medio.

Hasta ahora hemos hablado de posibles ataques relacionados con el personal de un sistema de información; sin embargo, existen otras amenazas a la seguridad provenientes de ese personal que no son necesariamente ataques en un sentido estricto de la palabra; en muchos casos no son intencionados, se podrían catalogar como accidentes, pero

[19] Consultar Bibliografía Libro (15)

el que la amenaza no sea intencionada no implica que no se deba evitar: decir "no lo hice a propósito" no va ayudar para nada a recuperar unos datos perdidos. En un centro de cómputo o sala de operaciones, las personas realizan acciones sobre los sistemas basándose - en muchos casos - únicamente en su apreciación personal de lo que está sucediendo; en esas circunstancias, dichas acciones pueden ser sorprendentes y devastadoras, incluso si provienen de los mejores y más cuidadosos administradores[20].

3.2.2 Ataques Potenciales

3.2.2.1 Ingeniería Social

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían[21]; aunque a nadie le gusta ser manipulado, en algunos casos no es excesivamente perjudicial (por ejemplo un vendedor puede aplicar ingeniería social para conocer las necesidades de un cliente y ofrecer así mejor sus productos), si las intenciones de quien la pone en práctica no son buenas se convierte quizás en el método de ataque más sencillo, menos peligroso para el atacante y por desgracia en uno de los más efectivos. Ese atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad por parte de personas relacionadas de una u otra forma con el sistema de información para poder engañarlas en beneficio propio. Por ejemplo, imaginemos que un usuario de un sistema de información recibe el siguiente correo electrónico:

> From: Super-User <root@sistema.com>
> To: Usuario <user@sistema.com>
> Subject: Cambio de clave
>
> Hola, para realizar una serie de pruebas orientadas a conseguir un óptimo funcionamiento de nuestro sistema, es necesario que cambie su clave mediante la orden "passwd". Hasta que reciba un nuevo aviso (aproximadamente en una semana), por favor, asigne a su contraseña ya el valor "PEPITO" (en mayúsculas.)
>
> Rogamos disculpe las molestias. Saludos.
>
> Administrador

[20] Consultar Bibliografía Libro (16)
[21] Consultar Bibliografía Libro (17)

Si el usuario no sabe nada sobre seguridad, es muy probable que siga al pie de la letra las indicaciones de este e-mail; pero nadie le asegura que el correo no haya sido enviado por un atacante - es muy fácil camuflar el origen real de un mensaje -, que consigue así un acceso al sistema: no tiene más que enviar un simple correo, sin complicarse buscando fallas en los sistemas operativos o la red, para poner en juego toda la seguridad. Sin saberlo y encima pensando que lo hace por el bien común, el usuario está ayudando al pirata a romper todo el esquema de seguridad de nuestro sistema de información.

Pero no siempre el atacante se aprovecha de la buena fe de los usuarios para lograr sus propósitos; tampoco es extraño que intente engañar al propio administrador del sistema. Por ejemplo, imaginemos que el sistema de información tiene el puerto finger abierto y el atacante detecta un nombre de usuario que nunca ha conectado al sistema; en este caso, una simple llamada telefónica puede bastarle para conseguir el acceso, – veamos -:

Administrador: Buenos días, aquí área de sistemas, ¿en qué podemos ayudarle?
Atacante: Hola, soy José Luis Pérez, llamaba porque no consigo recordar mi password del sistema upves.
Administrador: Un momento, ¿me puede decir su nombre de usuario?
Atacante: Sí, claro, es jlperez.
Administrador: Muy bien, la nueva contraseña que acabo de asignarle es rudolf. Por favor, nada más al conectarse, no olvide cambiarla.
Atacante: Por supuesto. Muchas gracias, muy amable.
Administrador: De nada, un saludo.

Como podemos ver, estamos en la situación opuesta a la anterior: ahora es el administrador quien facilita la entrada del atacante al sistema de información; lo único que éste ha necesitado es un nombre de usuario válido.

Evidentemente, cualquier mensaje, llamada telefónica o similar que un usuario reciba debe ser puesto inmediatamente en conocimiento del administrador del sistema; hay que recordar a los usuarios que en ningún caso se necesita su contraseña para realizar tareas administrativas en el sistema de información. De la misma forma, si es el administrador quien directamente recibe algo parecido a lo que acabamos de ver, quizás sea conveniente notificar el hecho a los

responsables de la organización y por supuesto poner la máxima atención en la seguridad de los sistemas involucrados, ya que en este caso se sabe a ciencia cierta que alguien intenta comprometer nuestra seguridad; en[22 y 23] se muestran algunas de las reglas básicas que debemos seguir en nuestra organización para prevenir ataques de ingeniería social y también para, en el caso de que se produzcan, reducir al mínimo sus efectos.

3.2.2.2 Shoulder Surfing

Otro tipo de ataque relacionado con la ingenuidad de los usuarios del sistema de información (pero también con el control de acceso físico) es el denominado shoulder surfing. Este ataque consiste en "espiar" físicamente a los usuarios, para obtener generalmente claves de acceso al sistema de información. Por ejemplo, una medida que lamentablemente utilizan muchos usuarios para recordar sus contraseñas es apuntarlas en un papel pegado al monitor de su PC o escribirlas en la parte de abajo del teclado; cualquiera que pase por el lugar de trabajo de este usuario, sin problemas puede leer el login, password e incluso el nombre del equipo al que pertenecen. Esto, que nos puede parecer una gran tontería, por desgracia no lo es y se utiliza más de lo que muchos administradores o responsables de seguridad piensan; y no sólo en entornos "privados" o con un control de acceso restringido, como puede ser un centro de cómputo o sala de operaciones, sino en lugares a los que cualquiera puede llegar sin ninguna acreditación.

El shoulder surfing no siempre se ve beneficiado por la ingenuidad de los simples usuarios de un equipo; en determinadas ocasiones son los propios programadores (gente que teóricamente ha de saber algo más sobre seguridad que el personal de administración o de atención al público) los que diseñan aplicaciones muy susceptibles de sufrir ataques de este tipo. Por ejemplo, en ciertas aplicaciones - especialmente algunas que se ejecutan sobre MS Windows y que son más o menos antiguas - muestran claramente en pantalla las contraseñas al ser tecleadas. Cualquiera situado cerca de una persona que las está utilizando puede leer claramente esa clave; un perfecto ejemplo de lo que NO se debe hacer nunca.

[22] Consultar Bibliografía Libro (18)
[23] Consultar Bibliografía Libro (19)

3.2.2.3 Basureo

La técnica del basureo (en inglés, scavenging) está relacionada tanto con los usuarios como con la seguridad física de los sistemas de información, de la que hemos hablado en la sección anterior; consiste en obtener información dejada en o alrededor del sistema de información tras la ejecución de un trabajo[24]. El basureo puede ser físico, como buscar en cubos de basura (trashing, traducido también por basureo) listados de impresión o copias de documentos. El basureo también puede ser lógico, como analizar buffers de impresoras, memoria liberada por procesos o bloques de un disco que el sistema de información acaba de marcar como libres, en busca de información.

Aunque esta técnica no es muy utilizada en la mayoría de los entornos operativos de un sistema de información, hemos de pensar que si un usuario tira a la basura documentos que proporcionen información sobre nuestro sistema de información, cualquier potencial atacante puede aprovechar esa información para conseguir acceder al equipo; algo tan simple como una factura en la que se especifiquen números de teléfono o nombres (reales o de entrada al sistema) de usuarios puede convertirse en una valiosa información para un atacante. Además, en ocasiones ni siquiera es necesario andar revolviendo por los cubos de basura en busca de información comprometedora: la carencia de nociones básicas sobre seguridad informática hace posible que los usuarios dejen al alcance de cualquiera información vital de cara a mantener un sistema de información seguro.

Como hemos dicho el basureo no es un ataque habitual en organizaciones "normales", simplemente porque los datos con los que están trabajando no suelen ser de alta confidencialidad. De cualquier forma, si deseamos evitar problemas lo más inmediato es utilizar una máquina trituradora de papel (su precio no suele ser alto y la inversión quizás valga la pena) para destruir toda la documentación antes de arrojarla a la basura; incluso nos puede interesar contratar los servicios de compañías dedicadas exclusivamente a la destrucción de estos soportes. En el caso de sistemas de almacenamiento lógico (discos, CD-ROM's, cintas, etc.) también es importante una correcta inutilización de los mismos para que un potencial atacante no pueda extraer información comprometedora; no suele ser suficiente el simple borrado del medio o un leve daño físico (por ejemplo, partir un CD-ROM), ya que como comentaremos al hablar de recuperación de datos existen empresas capaces de extraer hasta el último bit de un medio borrado o

[24] Consultar Bibliografía Libro (10)

dañado. Lo más efectivo sería un borrado seguro, seguido de una destrucción física importante que haga imposible la reconstrucción del medio.

3.2.2.4 Actos Delictivos

Bajo este nombre englobamos actos tipificados claramente como delitos por las leyes mexicanas, como el chantaje, el soborno o la amenaza. Esto no implica que el resto de actividades no sean (o deban ser) delitos, sino simplemente que en la práctica a nadie se le castiga "legalmente" por pasear por un centro de cómputo o sala de operaciones en busca de claves apuntadas en teclados, pero sí que se le puede castigar por amenazar a un operador para que le permita el acceso al sistema.

Por suerte, la naturaleza de la información con la que se trabaja en la mayor parte de los entornos operativos de un sistema de información hace poco probable que alguien amenace o chantajee a un operador para conseguir ciertos datos; al tratarse de información poco sensible, en la mayoría de las situaciones los atacantes no llegan a estos extremos para acceder al sistema de información, sino que utilizan procedimientos menos arriesgados como la ingeniería social o la captura de datos que viajan por la red. No obstante, si en alguna ocasión nos encontramos en estas situaciones, siempre es conveniente la denuncia; aunque en principio podamos ceder ante las presiones de un delincuente, hemos de tener presente que si mostramos cierta debilidad, una vez que éste consiga sus propósitos nada le va a impedir seguir amenazándonos o chantajeándonos para obtener más información. Si actuamos con la suficiente discreción, las autoridades pueden fácilmente llevar al individuo ante la justicia sin necesidad de grandes escándalos que pueden afectar gravemente a la imagen de nuestra organización.

3.2.3 El Atacante Interno

En el punto anterior hemos presentado al personal de una organización como víctima de los ataques realizados por agentes externos a la misma; sin embargo, según[25] el 80% de los fraudes, robos, sabotajes o accidentes relacionados con los sistemas informáticos son causados por el propio personal de la organización propietaria de dichos sistemas de información, lo que se suele denominar el insider factor. ¿Qué significa esto?. Principalmente que la mayor amenaza a

[25] Consultar Bibliografía Libro (20)

nuestros sistemas de información viene de parte de personas que han trabajado o trabajan con los mismos. Esto, que es realmente preocupante, lo es mucho más si analizamos la situación con un mínimo de detalle: una persona que trabaje codo a codo con el administrador, el programador o el responsable de la seguridad del sistema de información conoce perfectamente el sistema, sus barreras, sus puntos débiles, etc., de forma que un ataque realizado por esa persona va a ser muchísimo más directo, difícil de detectar y sobre todo, efectivo, que el que un atacante externo (que necesita recopilar información, intentar probar fallas de seguridad o conseguir privilegios) pueda ejecutar.

Pero, ¿por qué va a querer alguien atacar a su propia organización?, ¿por qué alguien va a arriesgarse a perder su trabajo, romper su carrera o incluso a ir a la cárcel?. Como se acostumbra decir, todos tenemos un precio; no importa lo honestos que seamos o que queramos creer que somos: dinero, chantaje, factores psicológicos, nos pueden arrastrar a vender información, a robar ficheros o simplemente a proporcionar acceso a terceros que se encarguen del trabajo sucio. En una empresa, un empleado puede considerarse mal pagado e intentar conseguir un sueldo extra a base de vender información; en un banco, alguien que a diario trabaje con los sistemas informáticos puede darse cuenta de la facilidad para desviar fondos a una cuenta sin levantar sospechas; en una base militar, un país enemigo puede secuestrar a la mujer de un administrador para que éste les pase información confidencial. Existen numerosos estudios[26,27,28,29,30] que tratan de explicar los motivos que llevan a una persona a cometer delitos, informáticos o no, contra su propia organización, pero sea cual sea el motivo, la cuestión está en que tales ataques existen, son numeroso, y hay que tomar medidas contra ellos.

¿Cómo prevenir o defendernos de los atacantes internos?. En una empresa, una norma básica sería verificar el curriculum de cualquier aspirante a nuevo miembro (no simplemente leerlo y darlo por bueno, sino comprobar los datos y directamente descartar al aspirante sí se detecta una mentira); si buscamos algo más de seguridad - por ejemplo, sistemas militares - también es recomendable investigar el pasado de cada aspirante a pertenecer a la organización, buscando sobre todo espacios en blanco durante los que no se sabe muy bien qué ha hecho o a qué se ha dedicado esa persona (¿quién nos asegura que

[26] Consultar Bibliografía Libro (21)
[27] Consultar Bibliografía Libro (22)
[28] Consultar Bibliografía Libro (23)
[29] Consultar Bibliografía Libro (24)
[30] Consultar Bibliografía Libro (25)

ese paréntesis de tres años durante los que el aspirante asegura que estuvo trabajando para una empresa extranjera no los pasó realmente en la cárcel por delitos informáticos?). Si se siguen ejemplos como estos se podrán asegurar la integridad de todos los que entran a formar parte de la organización y habremos dado un importante paso en la prevención de ataques internos.

Tampoco debemos olvidar que el hecho de que alguien entre "limpio" a nuestra organización no implica que vaya a seguir así durante el tiempo que trabaje para la organización y mucho menos cuando abandone su trabajo. Para minimizar el daño que un atacante interno puede causar se suelen seguir unos principios fundamentales[31,32,33] que se aplican sobre el personal de la empresa:

- **Necesidad de Saber**

  A cada usuario se le debe otorgar el mínimo privilegio que necesite para desempeñar correctamente su función; es decir, se le debe permitir que sepa solamente lo que necesita para trabajar. De esta forma, un programador no tiene por qué conocer las políticas de copia de seguridad de un equipo o sistema de información, ni un alumno tiene que poseer privilegios en un sistema de prácticas.

- **Conocimiento Parcial**

  Las actividades más delicadas dentro de la organización en cuanto a seguridad se refieren (por ejemplo, el conocimiento de la clave del administrador de un sistema de información) deben ser realizadas por dos personas competentes, de forma que si uno de ellos comete un error o intenta violar las políticas de seguridad el otro pueda darse cuenta rápidamente y subsanarlo o evitarlo. De la misma forma, aplicar este principio asegura que si uno de los responsables abandona la organización o tiene un accidente el otro pueda seguir operando los sistemas mientras una nueva persona sustituye a su compañero.

- **Rotación de Funciones**

  Quizás la mayor amenaza al conocimiento parcial es la potencial complicidad que los dos responsables del sistema de información puedan llegar a establecer, de forma que entre los dos sean capaces

[31] Consultar Bibliografía Libro (26)
[32] Consultar Bibliografía Libro (9)
[33] Consultar Bibliografía Libro (27)

de ocultar las violaciones de seguridad que los sistemas de información puedan sufrir, incluso puede suceder lo contrario, que ambas personas sean enemigas y esto repercuta en el buen funcionamiento de la política de seguridad establecida. Para evitar ambos problemas, una norma común es rotar - siempre dentro de unos límites - a las personas a lo largo de diferentes responsabilidades, de forma que a la larga todos puedan vigilar a todos; esto también es muy útil en caso de que alguno de los responsables abandone la organización, ya que en este caso sus tareas serán cubiertas más rápidamente.

- **Separación de Funciones**

No es en absoluto recomendable que una sola persona (o dos, si establecemos un control dual) posea o posean demasiada información sobre la seguridad de la organización; es necesario que se definan y separen correctamente las funciones de cada persona, de forma que alguien cuya tarea es velar por la seguridad de un sistema de información no posea él mismo la capacidad para violar dicha seguridad sin que nadie se percate de ello.

Si aplicamos correctamente los principios anteriores en nuestra política de personal vamos a evitar muchos problemas de seguridad, no sólo cuando un usuario trabaja para nuestro entorno sino lo que es igual de importante, cuando abandona la organización. Cuando esto sucede se debe cancelar inmediatamente el acceso de esa persona a todos nuestros recursos (cuentas de usuario, servicio de acceso remoto, unidades de red, etc.), y también cambiar las claves que ese usuario conocía. Especialmente en los entornos de redes I+D quizás esto es algo complicado debido a la gran movilidad de usuarios (un profesor invitado durante un mes a la universidad, aún proyectando que sólo necesita acceso a un sistema de información mientras que realiza su proyecto), por lo que es aquí donde se suelen ver mayores barbaridades en los sistemas de información: desde cuentas que hace años que no se utilizan hasta direcciones de correo de gente que dejó de trabajar para la organización hace años. Evidentemente, este tipo de cosas es muy preocupante para la seguridad y es justo en estos accesos no utilizados donde un atacante puede encontrar una de las mejores puertas de entrada a los sistemas de información: simplemente hemos de pensar que si el usuario de una cuenta hace años que no la utiliza, por lógica hace años que esa clave no se cambia.

Hasta ahora hemos hablado principalmente de los problemas que nos pueden causar las personas que trabajan para la organización; no

obstante, las redes de I+D son bastante peculiares a la hora de hablar de ataques internos. Se trata de sistemas en los que un elevado número de usuarios - los alumnos - pueden considerar un reto personal o intelectual saltarse las medidas de protección impuestas en los sistemas de información; además y especialmente en universidades técnicas, por la naturaleza de sus estudios, muchos alumnos llegan a poseer elevados conocimientos sobre sistemas operativos y redes, lo que evidentemente es un riesgo añadido: no es lo mismo proteger de ataques internos a un sistema de información en una Facultad de Derecho, donde a priori muy pocos alumnos tendrán el interés o los conocimientos suficientes para saltarse la seguridad del sistema, que en una Facultad de Ingeniería Informática, donde el que más y el que menos, tiene nociones de seguridad y a diario se trabaja en estos entornos.

Las normas vistas aquí seguramente se pueden aplicar sobre el personal de la organización, pero no sobre los alumnos (que es justamente de quienes provienen la mayoría de ataques): no podemos obligar a un alumno de nuevo ingreso a que nos muestre un resumen de su vida, ni mucho menos tenemos capacidad para verificar los datos de treinta o cincuenta mil alumnos. Incluso si pudiéramos, ¿sería legal o ético denegar el acceso a la universidad a alguien con antecedentes penales, por ejemplo?. Seguramente no; de esta forma, en organismos I+D nos debemos ceñir a otros mecanismos de prevención, por ejemplo en forma de sanciones ejemplares para todos aquellos que utilicen los recursos de la institución para cometer delitos informáticos; sin llegar a los tribunales, las posibles penas impuestas dentro de la universidad son a veces más efectivas que una denuncia en el juzgado, donde los piratas despiertan cierta simpatía entre muchos abogados y jueces.

CAPÍTULO IV

Seguridad Interna en los Sistemas de Información

El control de la seguridad de la información es un componente vital en el éxito de las organizaciones, además de que posiciona a la empresa entre los líderes de la seguridad en los negocios y le ayuda a mantener un ambiente controlado en el acceso a los sistemas de información.

En este capítulo se analizan los elementos de la seguridad interna de un sistema de información. Estos elementos son aplicables a cualquier tipo de sistema independientemente de su tecnología o plataforma de sistema operativo. Estos elementos de la seguridad interna de un sistema de información se basan en los estándares internacionales de seguridad los cuales pueden ser consultados en las siguientes páginas de Internet:

- http://www.information-security-policies-and-standards.com (estándares y políticas internacionales de seguridad, normas de calidad ISO17799).
- http://www.isaca.org (estándares internacionales de seguridad y certificaciones).
- http://www.isc2.org (certificaciones de seguridad).

4.1 Identificación

El objetivo del elemento Identificación es establecer un mecanismo estándar de identificación de usuarios externos e internos y de los componentes de infraestructura que interactúan con el sistema de información.

4.1.1 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.
- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.

- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

Con ayuda del área de seguridad informática de la organización deberá tratarse y analizarse caso por caso, para dar guía en el cumplimiento de las políticas de seguridad en los sistemas de información definidas originalmente, esto deberá hacerse a través de las revisiones periódicas – auditorías internas - como resultado de esto, se deberán generar planes de acción que ayuden a la mejora continua de los procesos y como consecuencia, el cumplimiento de las políticas de seguridad.

4.1.2 Puntos de Cumplimiento

A continuación (tabla 4.1) se indican los puntos a cumplir para este elemento de seguridad interna – identificación - en un sistema de información:

IDENTIFICACIÓN **Puntos de Cumplimiento**	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)
1. Debe existir un identificador único (userid) asociado con cada usuario de un sistema o aplicación	
2. Todos los sistemas de información, los sistemas de conexión inter-empresarial y los dispositivos de red (servidores DNS, servidores DHCP, Firewalls) deben estar registrados en una	

base de datos de control y administración de sistemas	
3. Todas las aplicaciones identificadas en el alcance de este elemento de seguridad deben estar registradas en una base de datos de control y administración de aplicaciones	

Tabla 4.1: Puntos de Cumplimiento del Elemento de Seguridad Identificación

La información contenida en la tabla 4.1 debe ser utilizada para asegurar el cumplimiento de este elemento (identificación) de seguridad interna en un sistema de información, tabla que debe ser actualizada por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa, una copia de esta tabla 4.1 será solicitada y retenida por el auditor.

4.1.3 Descripción de los Requerimientos

- **Requerimiento 1**

Debe existir un identificador único (userid) asociado con cada usuario de un sistema o aplicación.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso para crear usuarios:** Este proceso deberá realizar una validación de la existencia del usuario en la organización a través de la consulta en la base de datos de empleados de la organización.

- **Desarrollar e implantar un proceso para remover usuarios:** Este proceso deberá ser solicitado por el Gerente del usuario y por el área de recursos humanos.

- **Desarrollar e implantar un proceso para revalidar trimestralmente usuarios:** Este proceso tiene por finalidad el validar la existencia del empleado contra la base de datos de recursos humanos de la organización.

- **Desarrollar e implantar un proceso para revalidar anualmente usuarios:** Este proceso tiene por finalidad el validar la existencia del empleado contra la base de datos de recursos humanos de la organización y la autorización del Gerente del empleado.

- **Requerimiento 2**

Todos los sistemas de información, los sistemas de conexión inter.-empresarial y los dispositivos de red (servidores DNS, servidores DHCP, Firewalls) deben estar registrados en una base de datos de control y administración de sistemas.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso para registrar los sistemas de información en una base de datos:** Este proceso deberá registrar todos los sistemas de información en una base de datos para su control y supervisión, así como la asignación de una dirección de red fija TCP/IP. En esta base de datos se deberán registrar todos los sistemas de información así como su dirección de red fija TCP/IP existente en la organización y las nuevas que se vayan integrando.

- **Requerimiento 3**

Todas las aplicaciones identificadas en el alcance de este elemento de seguridad deben estar registradas en una base de datos de control y administración de aplicaciones.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso para registrar las aplicaciones existentes en los sistemas de información en una base de datos:** Este proceso deberá registrar todas las aplicaciones que estén instaladas en los sistemas de información en una base de datos para su control y supervisión.

4.2 Autenticación de Usuarios

El objetivo del elemento Autenticación es proporcionar métodos y componentes simples y confiables para verificar la identidad de los usuarios al acceder a un sistema de información.

4.2.1 Introducción y Conceptos Básicos

Los requerimientos primordiales para acceder a los sistemas de información, son los mecanismos de seguridad adecuados para protegerlo; el conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a las entidades (elementos activos del sistema, generalmente usuarios) que intentan acceder a los objetos (elementos pasivos, como ficheros o capacidad de cómputo), mediante procesos tan simples como una contraseña o tan complejos como un dispositivo analizador de patrones de retina.

Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser identificar a una persona, si no autenticar que esa persona es quien dice ser realmente. Aunque como humanos seguramente ambos términos nos parecerán equivalentes, para un ordenador existe una gran diferencia entre ellos - imaginemos un potencial sistema de identificación estrictamente hablando, por ejemplo: uno biométrico basado en el reconocimiento de la retina; una persona miraría a través del dispositivo lector y el sistema sería capaz de decidir si es un usuario válido y en ese caso decir de quién se trata; esto es identificación -. Sin embargo, lo que habitualmente hace el usuario es introducir su identidad (un número, un nombre de usuario, etc.) además de mostrar sus retinas ante el lector; el sistema en este caso no tiene que identificar a esa persona, si no autenticarlo - comprobar los parámetros de la retina que está leyendo con los guardados en una base de datos para el usuario que la persona dice ser -. Se está reduciendo el problema de una población potencialmente muy elevada a un grupo de usuarios más reducido, el grupo de usuarios del sistema que necesita autenticarlos.

Los métodos de autenticación se suelen dividir en tres grandes categorías[34,35] en función de lo que utilizan para la verificación de identidad: (a) algo que el usuario sabe, (b) algo que éste posee y (c)

[34] Consultar Bibliografía Libro (28)
[35] Consultar Bibliografía Libro (29)

una característica física del usuario o un acto involuntario del mismo. Esta última categoría se conoce con el nombre de autenticación biométrica. Es fácil ver ejemplos de cada uno de estos tipos de autenticación: un password es algo que el usuario conoce y el resto de las personas no, una tarjeta de identidad es algo que el usuario lleva consigo, la huella dactilar es una característica física del usuario y un acto involuntario podría considerarse que se produce al firmar (al rubricar la firma no se piensa en el diseño de cada trazo individualmente). Por supuesto, un sistema de autenticación puede (y debe, para incrementar su fiabilidad) combinar mecanismos de diferentes tipos, como en el caso de una tarjeta de crédito junto al Número de Identificación Personal (NIP) a la hora de utilizar un cajero automático o en el de un dispositivo generador de claves para el uso de passwords de una sola vez.

Cualquier sistema de identificación posee una determinada característica para ser viable; obviamente, ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo en los sistemas menos seguros), económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto) y ha de soportar con éxito cierto tipo de ataques (por ejemplo, imaginemos que cualquier usuario puede descifrar el password utilizado en el sistema de autenticación en poco tiempo; esto sería inaceptable). Aparte de estas características tenemos otra, no técnica si no humana, pero quizás la más importante - un sistema de autenticación ha de ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen -. Por ejemplo: imaginemos un potencial sistema de identificación para acceder a los recursos de la Universidad, consistente en un dispositivo que fuera capaz de realizar un análisis de sangre a un usuario y así comprobar que es quien dice ser; seguramente sería barato y altamente fiable, pero nadie aceptaría dar un poco de sangre cada vez que desee consultar su correo.

4.2.2 Sistemas basados en algo conocido: Contraseñas

El modelo de autenticación más básico consiste en decidir si un usuario es quien dice ser simplemente basándonos en una prueba de conocimiento que a priori sólo ese usuario puede saber. Esa prueba de conocimiento no es más que una contraseña que en principio es secreta. Evidentemente, esta aproximación es la más vulnerable a todo tipo de ataques, pero también la más barata, por lo que se convierte en la técnica más utilizada en entornos que no precisan de una alta seguridad; otros entornos en los que se suele aplicar este modelo de

autenticación son las aplicaciones que requieren de alguna identificación de usuarios, como el pasword o una palabra clave. También se utiliza como complemento a otros mecanismos de autenticación, por ejemplo: en el caso del Número de Identificación Personal (NIP) a la hora de utilizar cajeros automáticos.

En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo - las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, clave que han de mantener en secreto si desean que la autenticación sea fiable -. Cuando una de las partes desea autenticarse ante la otra se limita a mostrarle su conocimiento de esa clave común y si ésta es correcta se otorga el acceso al sistema de información. Lo habitual es que existan unos roles preestablecidos, con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior.

Como hemos dicho, este esquema es muy frágil - basta con que una de las partes no mantenga la contraseña en secreto para que toda la seguridad del modelo se pierda - por ejemplo: si el usuario de un sistema de información comparte su clave con un tercero, o si ese tercero consigue leerla y rompe su cifrado, automáticamente esa persona puede autenticarse ante el sistema con éxito con la identidad de un usuario que no le corresponde.

4.2.3 Sistemas basados en algo poseído: Tarjetas Inteligentes

Hace más de veinte años un periodista francés llamado Roland Moreno patentaba la integración de un procesador en una tarjeta de plástico; sin duda, no podía imaginar el abanico de aplicaciones de seguridad que ese nuevo dispositivo, denominado chipcard, estaba abriendo. Desde entonces, cientos de millones de esas tarjetas han sido fabricadas y son utilizadas a diario para fines que varían desde las tarjetas monedero más sencillas hasta el control de acceso a instalaciones militares y agencias de inteligencia de todo el mundo; cuando a las chipcards se les incorporó un procesador inteligente nacieron las smartcards, una gran revolución en el ámbito de la autenticación de usuarios.

Desde un punto de vista formal[36], una tarjeta inteligente (o smartcard) es un dispositivo de seguridad del tamaño de una tarjeta de crédito, resistente a la falsificación, que ofrece funciones para un

[36] Consultar Bibliografía Libro (30)

almacenamiento seguro de información y también para el procesamiento de la misma. En la práctica, las tarjetas inteligentes poseen un chip integrado en la propia tarjeta, que contiene un sistema de ficheros cifrado y funciones criptográficas, además puede detectar intentos no válidos de acceso a la información almacenada.

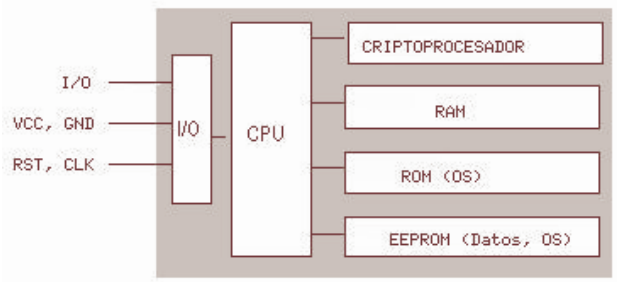

Figura 4.1: Estructura Genérica de una Smartcard

En la figura 4.1 se muestra la estructura general de una tarjeta inteligente; en ella podemos observar que el acceso a las áreas de memoria solamente es posible a través de la unidad de entrada/salida (I/O) y de una CPU (típicamente de 8 bits), lo que evidentemente aumenta la seguridad del dispositivo. Existe también un sistema operativo empotrado en la tarjeta - generalmente en ROM, aunque también se puede extender con funciones en la EEPROM - cuya función es realizar tareas criptográficas (algoritmos de cifrado como RSA o Triple DES); el criptoprocesador apoya estas tareas ofreciendo operaciones RSA con claves de 512 a 1024 bits.

Cuando el usuario poseedor de una smartcard desea autenticarse necesita introducir la tarjeta en un hardware lector; los dos dispositivos se identifican entre sí con un protocolo a dos bandas en el que es necesario que ambos conozcan la misma clave (CK o CCK, Company Key o Chipcard Communication Key), lo que elimina la posibilidad de utilizar tarjetas de terceros para autenticarse ante el lector de una determinada compañía; además, esta clave puede utilizarse para asegurar la comunicación entre la tarjeta y el dispositivo lector. Tras identificarse las dos partes, se lee la identificación personal (PID) de la tarjeta y el usuario teclea su PIN; se inicia entonces un protocolo desafío-respuesta: se envía el PID a la máquina y ésta desafía a la tarjeta, que responde al desafío utilizando una clave personal del usuario (PK, Personal Key). Si la respuesta es correcta, el sistema de información ha identificado la tarjeta y el usuario obtiene acceso al recurso pretendido.

Las ventajas de utilizar tarjetas inteligentes como medio para autenticar usuarios son muchas frente a las desventajas; se trata de un

modelo ampliamente aceptado entre los usuarios, rápido y que incorpora hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado. Además, su uso es factible tanto para controles de acceso físico como para controles de acceso lógico a los sistemas de información y se integra fácilmente con otros mecanismos de autenticación como las contraseñas; y en caso de desear bloquear el acceso de un usuario, no tenemos más que retener su tarjeta cuando la introduzca en el lector o marcarla como inválida en una base de datos (por ejemplo: si el usuario se equivoca varias veces al teclear su PIN, igual como sucede con una tarjeta de crédito normal). Como principal inconveniente de las smartcards podemos citar el costo adicional que supone para una organización el comprar y configurar la infraestructura de dispositivos lectores y las propias tarjetas; a parte, que un usuario pierda su tarjeta es bastante fácil y durante el tiempo que no disponga de ella o no pueda acceder al sistema, o hemos de establecer reglas especiales que pueden comprometer nuestra seguridad (y por supuesto se ha de marcar como tarjeta inválida en una base de datos central, para que un potencial atacante no pueda utilizarla). También la distancia lógica entre la smartcard y su poseedor - simplemente nos podemos fijar en que la tarjeta no tiene una interfaz para el usuario - puede ser fuente de varios problemas de seguridad.

Aparte de los problemas que puede implicar el uso de smartcards en sí, contra la lógica de una tarjeta inteligente existen diversos métodos de ataque, como realizar ingeniería inversa - destructiva - contra el circuito de silicio (y los contenidos de la ROM), adulterar la información guardada en la tarjeta o determinar por diferentes métodos el contenido de la memoria EEPROM.

4.2.4 Sistemas de Autenticación Biométrica

En un futuro no muy lejano estos serán los sistemas que se van a imponer en la mayoría de las situaciones en las que se haga necesario autenticar un usuario. Son más amigables para el usuario (no va a necesitar recordar passwords o números de identificación complejos y como se suele decir, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará de su mano o su ojo) y son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética; la principal razón por la que no se ha impuesto aún, es su elevado precio fuera del alcance de muchas organizaciones y su dificultad de mantenimiento.

Estos sistemas son los denominados biométricos, basados en las características físicas del usuario a identificar. El reconocimiento de

formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptografía se limita aquí a un uso secundario, como el cifrado de una base de datos de patrones de retina, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos. La autenticación basada en características físicas existe desde que existe el hombre y sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana - a diario identificamos a personas por los rasgos de su cara o por su voz -. Obviamente aquí el agente reconocedor le es fácil porque es una persona, pero en el modelo aplicable a los sistemas de información el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue el acceso a un determinado recurso del sistema.

Métodos Biométricos						
	Ojo – Iris	**Ojo - Retina**	**Huellas dactilares**	**Geometría de la mano**	**Escritura - Firma**	**Voz**
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenti-cación
Estándar	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas	Artritis, reumatismo	Firmas fáciles o cambiantes	Ruido, resfriado
Utilización	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio por nodo 2003 (USD)	7000	7000	3000	5000	3000	3000

Tabla 4.2: Comparación de Métodos Biométricos

Aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y mesurable del individuo (esto incluye desde la forma de teclear ante un ordenador hasta los patrones de ciertas venas, pasando por el olor corporal); tradicionalmente ha estado basada en cinco grandes grupos de verificación[37] : (voz, escritura, huellas, patrones oculares y geometría de la mano); en la tabla 4.2[38,39] se muestra una comparativa de sus

[37] Consultar Bibliografía Libro (29)
[38] Consultar Bibliografía Libro (31)
[39] Consultar Bibliografía Libro (32)

rasgos más generales, que vamos a ver con más detalle en los puntos siguientes.

Los dispositivos biométricos tienen tres partes principales; por un lado, disponen de un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar. Además disponen de una entidad para manejar aspectos como la compresión, almacenamiento o comparación de los datos capturados con los guardados en una base de datos (que son considerados válidos) y también ofrecen una interfaz para las aplicaciones que los utilizan. El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: **captura** o lectura de los datos que el usuario a validar presenta; **extracción** de ciertas características de la muestra (por ejemplo: las minucias de una huella dactilar); **comparación** de tales características con las guardadas en una base de datos y **decisión** de si el usuario es válido o no. Es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación), las tasas de falso rechazo y de falsa aceptación. Por tasa de **falso rechazo (FR)** se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente y por tasa de **falsa aceptación (FA)** se entiende la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo. Evidentemente, un FR alto provoca descontento entre los usuarios del sistema, pero una FA elevada genera un grave problema de seguridad, ya que estamos proporcionando acceso a un recurso a personal no autorizado para acceder a él.

Por último, y antes de entrar más a fondo con los esquemas de autenticación biométrica clásicos, quizás es conveniente desmentir uno de los grandes mitos de estos modelos: la vulnerabilidad a ataques de simulación. En cualquier película o libro de espías que se precie, siempre se consigue engañar a autenticadores biométricos para conseguir acceso a determinadas instalaciones mediante estos ataques: se simula la parte del cuerpo a analizar mediante un modelo o incluso utilizando órganos amputados a un cadáver o al propio usuario vivo (crudamente, se le corta una mano o un dedo, se le saca un ojo, etc., para conseguir que el sistema permita la entrada). Evidentemente, esto sólo sucede en la ficción: hoy en día cualquier sistema biométrico - con excepción, quizás, de algunos modelos basados en voz de los que hablaremos luego - son altamente inmunes a estos ataques. Los analizadores de retina, de iris, de huellas o de la geometría de la mano son capaces, aparte de decidir si el miembro pertenece al usuario legítimo, de determinar si éste está vivo o se trata de un cadáver.

4.2.4.1 Verificación de Voz

En los sistemas de reconocimiento de voz no se intenta, como mucha gente piensa, reconocer lo que el usuario dice, si no identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer por ejemplo: imaginemos que el usuario se limita a pronunciar su nombre, de forma que el reconocedor lo entienda y lo autentique. Como veremos a continuación, estos modelos proporcionan poca seguridad en comparación con los de texto independiente, donde el sistema va proponiendo a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande. De cualquier forma, sea cual sea el modelo, lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar por ejemplo: frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales, etc. Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos.

El principal problema del reconocimiento de voz es la inmunidad frente a un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo: por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos: volviendo al ejemplo anterior, el del nombre de cada usuario, un atacante no tendría más que grabar a una persona que pronuncia su nombre ante el autenticador y luego reproducir ese sonido para conseguir el acceso. La única solución consiste en utilizar otro sistema de autenticación junto al reconocimiento de voz. Contrariamente en los modelos de texto independientes y más interactivos, este ataque no es tan sencillo porque la autenticación se produce realmente por una especie de desafío-respuesta entre el usuario y la máquina, de forma que la cantidad de texto grabado habría

de ser mucho mayor y la velocidad para localizar la parte del texto que el sistema propone habría de ser elevada. Otro grave problema de los sistemas basados en reconocimiento de voz es el tiempo que el usuario emplea hablando delante del analizador, al que se añade el que éste necesita para extraer la información y compararla con la de su base de datos; aunque actualmente en la mayoría de los sistemas basta con una sola frase, es habitual que el usuario se vea obligado a repetirla porque el sistema le deniega el acceso (una simple congestión hace variar el tono de voz, aunque sea levemente y el sistema no es capaz de decidir si el acceso ha de ser autorizado o no; incluso el estado anímico de una persona varía su timbre). A su favor, el reconocimiento de voz posee la cualidad de una excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente.

4.2.4.2 Verificación de Escritura

Aunque la escritura (generalmente la firma) no es una característica estrictamente biométrica, como hemos comentado en la introducción se suele agrupar dentro de esta categoría; de la misma forma que sucedía en la verificación de la voz, el objetivo aquí no es interpretar o entender lo que el usuario escribe en el lector, si no autenticarlo basándose en ciertos rasgos tanto de la firma como de su rúbrica.

La verificación con base en firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios con base en la representación de los trazos de su firma. En los modelos biométricos se utiliza además la forma de firmar, las características dinámicas (por eso se les suele denominar verificación dinámica de firma): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo, etc.

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar

uniformemente. Contra este problema la única solución (aparte de una concienciación de tales usuarios) es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se decrementa su seguridad.

Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos) y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

4.2.4.3 Verificación de Huellas

Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Por tanto, parece obvio que las huellas se convertirían antes o después en un modelo de autenticación biométrico - desde el siglo pasado hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales - y el uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica.

Figura 4.2: Huella Dactilar con sus Minucias Extraídas

Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta). Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que tiene en su base de datos; es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí si no que son estas minucias, concretamente la posición relativa de cada una de ellas. Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes y cada uno tiene al menos 30 ó 40 de éstas (en la figura 4.2 podemos ver una imagen de una huella digitalizada con sus minucias). Si la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, denegándosele obviamente en caso contrario.

Los sistemas basados en reconocimiento de huellas son relativamente baratos (en comparación con otros biométricos, como los basados en patrones de retina); sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas. Otro factor a tener muy en cuenta contra estos sistemas es psicológico, no técnico: hemos dicho en la introducción que un sistema de autenticación de usuarios ha de ser aceptable por los mismos y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso[40].

4.2.4.4 Verificación de Patrones Oculares

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: o bien analizan patrones de retina, o bien analizan el iris. Estos métodos se suelen considerar los más efectivos: para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi cero y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

[40] Consultar Bibliografía Libro (33)

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación; el hecho de mirar a través de un binocular (o monocular), necesario en ambos modelos, no es cómodo para los usuarios, ni aceptable para muchos de ellos: por un lado, los usuarios no se fían de un haz de rayos analizando su ojo y por otro un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas. Aunque los fabricantes de dispositivos lectores aseguran que sólo se analiza el ojo para obtener patrones relacionados con la autenticación y en ningún caso se viola la privacidad de los usuarios, mucha gente no cree esta postura oficial (aparte del hecho de que la información es procesada vía software, lo que facilita introducir modificaciones sobre lo que nos han vendido para que un lector realice otras tareas de forma enmascarada). Por si esto fuera poco, se trata de sistemas demasiado caros para la mayoría de las organizaciones y el proceso de autenticación no es todo lo rápido que debiera en poblaciones de usuarios elevadas. De esta forma, su uso se ve reducido casi sólo a la identificación en sistemas de alta seguridad, como el control de acceso a instalaciones militares.

4.2.4.4.1 Retina

La vasculatura de retina (forma de los vasos sanguíneos de la retina humana) es un elemento característico de cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura.

En los sistemas de autenticación basados en patrones de retina el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia interocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

La compañía EyeDentify posee la patente mundial para analizadores de vasculatura retinal, por lo que es la principal desarrolladora de esta tecnología; su página web se puede encontrar en http://www.eyedentify.com.

4.2.4.4.2 Iris

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal, una estructura única por individuo que forma un sistema muy complejo - de hasta 266 grados de libertad - inalterable durante toda la vida de la persona. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.

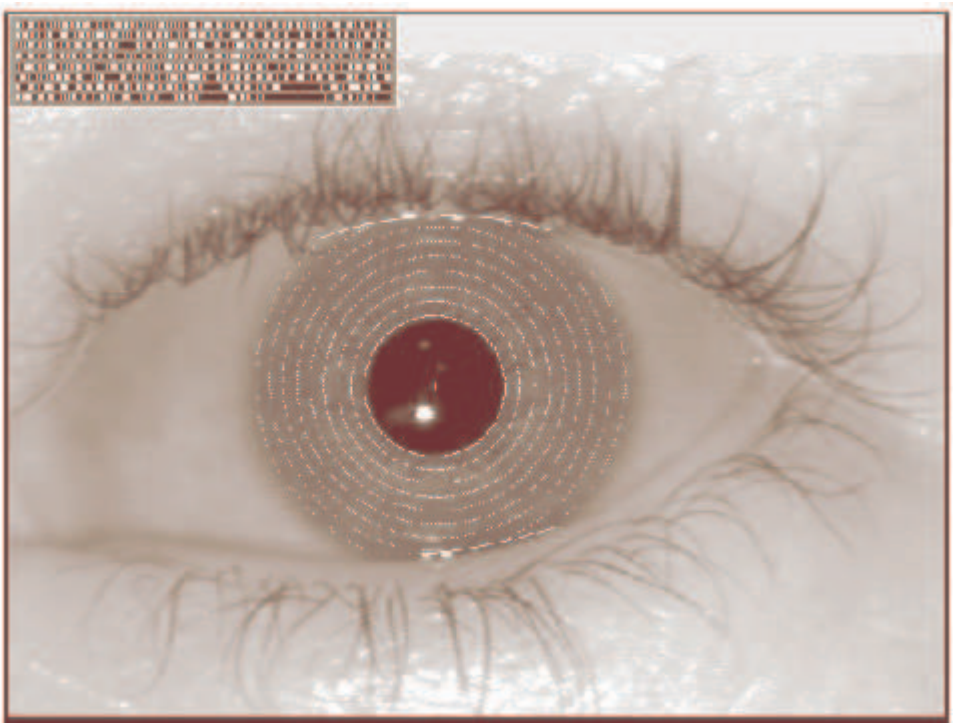

Figura 4.3: Iris Humano con la Extracción de su Código Iris

La identificación basada en el reconocimiento de iris (figura 4.3) es más moderna que la basada en patrones de retina; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios[41,42]. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas[43] hasta obtener una cantidad de datos (típicamente 256KBytes) suficiente para

[41] Consultar Bibliografía Libro (34)
[42] Consultar Bibliografía Libro (35)
[43] Consultar Bibliografía Libro (36)

los propósitos de autenticación. Esa muestra, denominada código iris (en la figura 4.3 se muestra una imagen de un iris humano con su código iris asociado) es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos[44].

La empresa estadounidense IriScan es la principal desarrolladora de tecnología (y de investigaciones) basada en reconocimiento de iris que existe actualmente, ya que posee la patente sobre esta tecnología; su página web, con interesantes artículos sobre este modelo de autenticación, se puede consultar en http://www.iriscan.com.

4.2.4.5 Verificación de la Geometría de la Mano

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de las ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

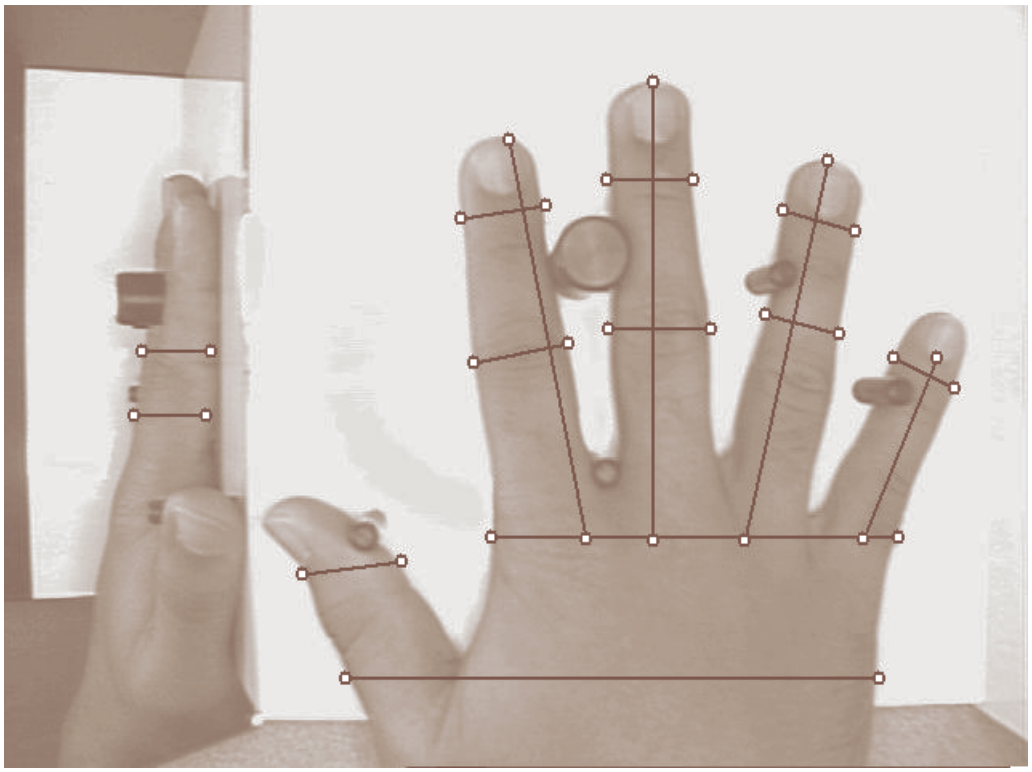

Figura 4.4: Geometría de una Mano con ciertos Parámetros Extraídos

[44] Consultar Bibliografía Libro (37)

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura (figura 4.4). Una vez que la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias, etc.) en un formato de tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de datos de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida, etc.). De esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones: no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

4.2.5 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.
- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.

- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

4.2.6 Puntos de Cumplimiento

A continuación (tabla 4.3) se indican los puntos a cumplir para este elemento de seguridad interna – autenticación - en un sistema de información:

AUTENTICACIÓN **Puntos de Cumplimiento**	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)
Autenticación de Usuario a Sistema	
1. Cada identidad del usuario debe ser verificada (autenticada) cuando éste solicita un acceso al sistema, aplicación o dispositivo de infraestructura.	
2. El password utilizado en la verificación de la identidad del usuario debe apegarse tanto a las reglas de sintaxis como se seguridad contempladas en las políticas de seguridad informática de la organización.	
3. El password utilizado en la verificación de la identidad del usuario debe estar protegido.	
4. La autenticación del paquete	

(token) utilizado en la verificación de la identidad del usuario debe estar protegida.	
Autenticación de Sistema a Sistema	
5. En los sistemas y/o aplicaciones en los cuales es requerido el uso de passwords para comunicarse entre el front-end y el back-end pueden usar passwords que no expiren. Es mandatorio el control de requerimientos para esos usuarios.	

Tabla 4.3: Puntos de Cumplimiento del Elemento de Seguridad Autenticación

La información contenida en la tabla 4.3 debe ser utilizada para asegurar el cumplimiento de este elemento (autenticación) de seguridad interna en un sistema de información, tabla que debe ser actualizada por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa una copia de esta tabla 4.3 será solicitada y retenida por el auditor.

4.2.7 Descripción de los Requerimientos

- **Requerimiento 1**

Cada Identidad del usuario debe ser verificada (autenticada) cuando éste solicita un acceso al sistema, aplicación o dispositivo de infraestructura.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso de autenticación de usuarios que requieran acceso al sistema, aplicación o dispositivo de red:** Este proceso deberá realizar una validación de la existencia del usuario en el sistema, aplicación o dispositivo de red para permitir el acceso. Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información y ser verificado periódicamente.

- **Requerimiento 2**

El password utilizado en la verificación de la identidad del usuario debe apegarse tanto a las reglas de sintaxis como de seguridad contempladas en las políticas de seguridad informática de la organización.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **El password debe ser mínimo de seis posiciones de longitud:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password debe contener mínimo un caracter alfanumérico y uno no-alfanumérico:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password debe contener un caracter no-numérico al principio y al final del password:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password no debe contener más de tres caracteres idénticos consecutivos del password anterior:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password no debe contener más de dos caracteres idénticos consecutivos:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password no debe contener el userid como parte del password:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password debe ser cambiado cada 186 días:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password debe ser bloqueado después de cuatro intentos de acceso:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password no debe ser compartido a menos que se mantenga la responsabilidad individual; es decir, bajo la responsabilidad del dueño del usuario y password:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **Requerimiento 3**

El password utilizado en la verificación de la identidad del usuario debe estar protegido.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **El password no debe ser transmitido en forma de texto a través de la Internet, Redes Públicas, Redes Inalámbricas, etc.:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **El password debe estar encriptado. Si no es posible esto porque el sistema, aplicación o dispositivo de red no lo permiten, debe buscarse implantar una herramienta que permita hacerlo, o bien, el uso del password debe ser limitado únicamente a los administradores del sistema, aplicación o dispositivo de red y se debe tener presente que esta situación demerita la seguridad del sistema:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **Desarrollar e implantar un proceso de reset de passwords de usuarios:** Este proceso debe tener la finalidad de controlar el reset de password del usuario, de tal forma que no cualquiera pueda solicitarlo, para ello este proceso debe solicitar información clave y/o personal del usuario y ser validada por el administrador del sistema quien enviará el nuevo password al Gerente del usuario.

- **El password del userid enviado por el reset debe ser cambiado por el usuario en el primer acceso al sistema:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **Requerimiento 4**

La autenticación del paquete (token) utilizado en la verificación de la identidad del usuario debe estar protegida.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **El tiempo de vida del paquete (token) para los usuarios (administradores y usuarios en general) no debe exceder una jornada laboral de trabajo:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **Las herramientas de autenticación de usuarios no deben exponer la des-encriptación de passwords:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **Todos los requerimientos de servicio o acceso a información deben basarse en un ticket de autenticación o en el userid y password del usuario:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

- **Requerimiento 5**

En los sistemas y/o aplicaciones en los cuales es requerido el uso de passwords para comunicarse entre el front-end y el back-end pueden usar passwords que no expiren. Es mandatorio el control de requerimientos para esos usuarios.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Los sistemas, aplicaciones o dispositivos de red que requieran el uso de passwords para comunicarse entre el front-end y el back-end pueden usar passwords sin expiración. Es mandatorio tener control sobre los userids de los usuarios que requieran acceder de esta forma:** Este parámetro técnico debe estar configurado en el sistema operativo del sistema de información. Así mismo se debe desarrollar e implantar un proceso que verifique periódicamente este parámetro técnico.

4.3 Autorización

El objetivo del elemento Autorización es otorgar o denegar el acceso a servicios o información de un sistema de información basada en la identidad autenticada del usuario y de las necesidades de negocio individuales del mismo.

4.3.1 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.
- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.
- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

Con ayuda del área de seguridad informática de la organización deberá tratarse y analizarse caso por caso, para dar guía en el cumplimiento de las políticas de seguridad en los sistemas de información definidas originalmente, esto deberá hacerse a través de las revisiones periódicas – auditorías internas - como resultado de esto, se deberán generar planes de acción que ayuden a la mejora continua de los procesos y como consecuencia el cumplimiento de las políticas de seguridad.

4.3.2 Puntos de Cumplimiento

A continuación (tabla 4.4) se indican los puntos a cumplir para este elemento de seguridad interna – autorización - en un sistema de información:

AUTORIZACIÓN Puntos de Cumplimiento	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o	

Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)
Autorización de Acceso al Sistema de Información	
1. El acceso al sistema de información solicitado por el usuario debe ser autorizado por el dueño del mismo con base en la necesidad del negocio.	
2. El acceso a la información confidencial solicitado por el usuario debe ser autorizado por el dueño de la misma con base en la necesidad del negocio.	
3. Realizar una verificación de empleo trimestral del usuario en cuanto a la asignación individual del userid.	
Acceso Remoto a Empleados	
4. Los empleados que requieran acceder remotamente los servicios de tecnología de información de la empresa deben utilizar las soluciones aprobadas por la compañía.	
Notificación del Uso del Negocio	
5. La siguiente notificación debe ser presentada al usuario al momento de acceder al sistema durante el proceso de identificación y autorización: "Los sistemas internos de la compañía deben solamente ser usados para propósitos del negocio autorizados por la compañía".	
Recursos de Usuario	
6. Los administradores del sistema deben otorgar al recurso la	

protección por default inicial para que los usuarios lo accedan. El dueño del recurso es el único que puede limitar el acceso al recurso.	
7. Los administradores del sistema deben asegurarse que el dueño del recurso esté informado cuando el acceso por default al recurso cambie a acceso público o universal.	

Tabla 4.4: Puntos de Cumplimiento del Elemento de Seguridad Autorización

La información contenida en la tabla 4.4 debe ser utilizada para asegurar el cumplimiento de este elemento (autorización) de seguridad interna en un sistema de información, tabla que debe ser actualizada por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa una copia de esta tabla 4.4 será solicitada y retenida por el auditor.

4.3.3 Descripción de los Requerimientos

- **Requerimiento 1**

El acceso al sistema de información solicitado por el usuario debe ser autorizado por el dueño del mismo con base en la necesidad del negocio.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **El dueño del sistema de información es quien determina los criterios de las necesidades del negocio para accederlo:** Esta persona deberá definir quien puede o no acceder a su sistema de información con base en los criterios que él considere pertinentes tomando en cuenta las necesidades del negocio.

- **Desarrollar e implantar un proceso de revalidación anual de la necesidad de negocio del usuario para acceder al recurso:** Este proceso deberá realizar una validación de la existencia del usuario en el sistema, para

permitir el acceso, así como la necesidad de negocio para accederlo.

- **Requerimiento 2**

El acceso a la información confidencial solicitado por el usuario debe ser autorizado por el dueño de la misma con base en la necesidad del negocio.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **El dueño de la información confidencial es quien determina los criterios de las necesidades del negocio para accederlo:** Esta persona deberá definir quien puede o no acceder a su información confidencial con base en los criterios que él considere pertinentes tomando en cuenta las necesidades del negocio.

- **Desarrollar e implantar un proceso de revalidación anual de la necesidad de negocio del usuario para acceder a la información confidencial:** Este proceso deberá realizar una revalidación de la justificación de negocio del usuario para permitirle el acceso al sistema. Esta justificación debe ser proporcionada por el gerente del usuario al dueño de la información confidencial.

- **Requerimiento 3**

Realizar una verificación de empleo trimestral del usuario en cuanto a la asignación individual del userid.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso de verificación de empleo trimestral del usuario:** Este proceso deberá realizar una verificación trimestral de que el usuario sigue empleado en la empresa. Esta verificación debe ser proporcionada por el gerente del usuario.

- **Requerimiento 4**

Los empleados que requieran acceder remotamente los servicios de tecnología de información de la empresa deben utilizar las soluciones aprobadas por la compañía.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso de verificación del tipo de acceso que el usuario está utilizando para acceder a los sistemas de información de la empresa:** Este proceso deberá realizar una verificación de la forma en que el usuario se conecta remotamente a los sistemas de información de la empresa, de tal forma que este proceso debe permitirle al área de seguridad de la empresa identificar desviaciones y/o anomalías en este tipo de conexiones. El área de seguridad de la compañía es quien autoriza el tipo de acceso remoto a los sistemas de información de la empresa.

- **Requerimiento 5**

La siguiente notificación debe ser presentada al usuario al momento de acceder al sistema durante el proceso de identificación y autorización: "Los sistemas internos de la compañía deben solamente ser usados para propósitos del negocio autorizados por la compañía".

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Los sistemas de información deben presentar esta notificación al usuario cada vez que éste lo accede:** Esta notificación debe estar contemplada explícitamente en las políticas de seguridad informática de la organización. Esta notificación debe ser configurada en los sistemas de información para ser presentada al usuario que lo accede.

- **Requerimiento 6**

Los administradores del sistema deben otorgar al recurso la protección por default inicial para que los usuarios lo accedan. El dueño del recurso es el único que puede limitar el acceso al recurso.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Los sistemas de información deben otorgar al recurso la protección por default para que sea accedido:** Esta protección al recurso debe ser configurada por default en los sistemas de información la cual depende de cada plataforma de sistema operativo.

- **Requerimiento 7**

Los administradores del sistema deben asegurarse que el dueño del recurso esté informado cuando el acceso por default al recurso cambie a acceso público o universal

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso de verificación de protección a recursos por default:** Este proceso debe asegurar que los recursos cuenten con la protección por default que ofrece el sistema operativo y debe identificar cualquier cambio en esta protección; es decir identificar si un recurso tiene protección de más o de menos. Así mismo este proceso debe informar al administrador del sistema de información de cualquier anomalía de este tipo.

4.4 Protección de la Información y Confidencialidad

El objetivo del elemento Protección de la Información y Confidencialidad es asegurar que la información privada o confidencial no sea accedida por individuos no autorizados durante transmisiones electrónicas o mientras esté almacenada en algún componente de infraestructura.

4.4.1 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.
- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.
- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

Con ayuda del área de seguridad informática de la organización deberá tratarse y analizarse caso por caso, para dar guía en el cumplimiento de las políticas de seguridad en los sistemas de información definidas originalmente, esto deberá hacerse a través de las revisiones periódicas – auditorías internas - como resultado de esto, se deberán generar planes de acción que ayuden a la mejora continua de los procesos y como consecuencia el cumplimiento de las políticas de seguridad.

4.4.2 Puntos de Cumplimiento

A continuación (tabla 4.5) se indican los puntos a cumplir para este elemento de seguridad interna – protección de la información y confidencialidad - en un sistema de información:

PROTECCIÓN DE LA INFORMACIÓN Y CONFIDENCIALIDAD Puntos de Cumplimiento	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)

Protección de la Información	
1. Prevenir el acceso no autorizado a la información confidencial, a la información del usuario, asociados de negocio, clientes o visitantes al web site.	
2. Etiquetar los medios de almacenamiento de información (cintas, cartuchos, diskettes, cd's, etc.), con la leyenda Información Confidencial.	
Información Residual	
3. Destruir totalmente los medios de almacenamiento de la información residual.	
Encriptación	
4. Encriptar la información confidencial que será enviada a través de Internet, redes públicas o dispositivos wireless.	
5. En las redes internas (LAN) la encriptación a nivel puerto es requerida en todos los servidores de dominio o de correo y el SSL (Secure Sockets Layer) es requerido en todos los servidores web que colectan o muestran información confidencial en la web.	

Tabla 4.5: Puntos de Cumplimiento del Elemento de Seguridad Protección de la Información y Confidencialidad

La información contenida en la tabla 4.5 debe ser utilizada para asegurar el cumplimiento de este elemento (protección de la información y confidencialidad) de seguridad interna en un sistema de información, tabla que debe ser actualizada por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa una copia de esta tabla 4.5 será solicitada y retenida por el auditor.

4.4.3 Descripción de los Requerimientos

- **Requerimiento 1**

Prevenir el acceso no autorizado a la información confidencial, a la información del usuario, asociados de negocio, clientes o visitantes al web site.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que prevenga accesos no autorizados a la información confidencial, de usuarios, de asociados de negocio, clientes, visitantes de web, etc.:** Este proceso debe a través de los dueños de la información otorgar acceso a la información confidencial, de usuario, de clientes, de asociados de negocio, etc., a quienes deban tener acceso bajo una justificación de negocio. Este proceso debe revalidar periódicamente – trimestral, semestral o anual con base en las políticas de seguridad establecidas por la organización - los accesos de quienes deben tener acceso a la información.

- **Requerimiento 2**

Etiquetar los medios de almacenamiento de información (cintas, cartuchos, diskettes, cd's, etc.), con la leyenda "Información Confidencial".

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que lleve a cabo el etiquetado de los medios de almacenamiento de la información confidencial:** Este proceso debe etiquetar todos los medios de almacenamiento de la información confidencial tales como: cintas, cartuchos, diskettes, cd's, etc., con una etiqueta que lleve la leyenda "Información Confidencial". Este etiquetado debe realizarse en los medios de almacenamiento desde que son nuevos e ingresan a este proceso y conservarlo hasta que por daño o tiempo de vida útil salen del proceso para su debida destrucción. Este proceso debe llevar a cabo una revalidación periódica – trimestral, semestral o anual con base en las políticas de

seguridad establecidas por la organización – de los medios de almacenamiento existentes con el fin de resguardar la información. Estos medios de almacenamiento de información deben mantenerse bajo llave conforme el esquema que la organización haya definido (cintoteca, bóvedas, gabinetes, cajoneras, etc.).

- **Requerimiento 3**

Destruir totalmente los medios de almacenamiento de la información residual.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que lleve a cabo la destrucción de los medios de almacenamiento de la información residual de la organización:** Este proceso debe destruir físicamente los medios de almacenamiento (cintas, cartuchos, diskettes, cd's, etc.), de la información residual que la organización ya no necesite. Este proceso debe llevar a cabo la destrucción de los medios de almacenamiento de manera continua para no exponer a que sea robada o sustraída la información residual de la organización.

- **Requerimiento 4**

Encriptar la información confidencial que será enviada a través de Internet, redes públicas o dispositivos wireless.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que verifique que la información confidencial es encriptada al ser enviada a través de Internet, redes públicas o dispositivos wireless:** Este proceso debe verificar de manera permanente que la información confidencial enviada a través de Internet, redes públicas, o wireless, debe viajar encriptada para evitar ser accedida, violada, alterada, sustraída o borrada evitando con ello que llegue a su destino correctamente.

- **Requerimiento 5**

En las redes internas (LAN) la encriptación o el cifrado a nivel puerto es requerida en todos los servidores de dominio o de correo y el SSL (Secure Sockets Layer) es requerido en todos los servidores web que colectan o muestran información confidencial en la web.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que verifique que la** encriptación o el cifrado **a nivel puerto es realizada por los servidores de dominio o correo y el SSL (Secure Sockets Layer) es ejecutado por los servidores web al momento de realizar transacciones de información a través de la red LAN:** Este proceso debe verificar de manera permanente que la encriptación o el cifrado a nivel puerto es realizada por los servidores de dominio o correo y el SSL es ejecutado por los servidores web al realizar transacciones de información a través de la red interna.

4.5 Integridad y Disponibilidad del Servicio

El objetivo del elemento Integridad y Disponibilidad del Servicio como estrategia de seguridad es prevenir cambios no autorizados a los componentes de la infraestructura y prevenir la interrupción del servicio causado por intrusos o por la propagación y ejecución de códigos perjudiciales.

4.5.1 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.

- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.
- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

Con ayuda del área de seguridad informática de la organización deberá tratarse y analizarse caso por caso, para dar guía en el cumplimiento de las políticas de seguridad en los sistemas de información definidas originalmente, esto deberá hacerse a través de las revisiones periódicas – auditorías internas - como resultado de esto, se deberán generar planes de acción que ayuden a la mejora continua de los procesos y como consecuencia el cumplimiento de las políticas de seguridad.

4.5.2 Puntos de Cumplimiento

A continuación (tabla 4.6) se indican los puntos a cumplir para este elemento de seguridad interna – integridad y disponibilidad del servicio - en un sistema de información:

INTEGRIDAD Y DISPONIBILIDAD DEL SERVICIO Puntos de Cumplimiento	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)
Administración de los Recursos del Sistema Operativo (OSR por sus siglas en inglés)	
1. Administrar los accesos a los Recursos del Sistema Operativo (OSR).	
Autoridad para la	

Administración del Sistema y la Seguridad	
2. Asignar o remover accesos para administrar el sistema y la seguridad.	
Código Dañoso	
3. Prevenir la ejecución y propagación de códigos dañosos.	
Vulnerabilidades	
4. Identificar vulnerabilidades al sistema.	
Administración de los Parches de Seguridad	
5. Aplicar los parches de seguridad al sistema.	
Administración del Software en Sistema	
6. Autorizar cualquier tipo de instalación, modificación o cambio al software del sistema.	
Administración de la Disponibilidad del Servicio	
7. Negar el Servicio.	
8. Ataques Sistemáticos de Login.	

Tabla 4.6: Puntos de Cumplimiento del Elemento de Integridad y Disponibilidad del Servicio

La información contenida en la tabla 4.6 debe ser utilizada para asegurar el cumplimiento de este elemento (integridad y disponibilidad del servicio) de seguridad interna en un sistema de información, tabla que debe ser actualizada por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa una copia de esta tabla 4.6 será solicitada y retenida por el auditor.

4.5.3 Descripción de los Requerimientos

- **Requerimiento 1**

Administrar los accesos a los Recursos del Sistema Operativo (OSR).

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que controle los accesos a los recursos del sistema operativo:** Este proceso debe controlar los accesos a los recursos del sistema operativo con base en las especificaciones técnicas de la plataforma que se esté utilizando. Este proceso debe ejecutarse de manera permanente y validar que los accesos a los recursos del sistema operativo sean los correctos con base en las especificaciones técnicas de la plataforma. Esto con el fin de proteger la integridad y disponibilidad del sistema operativo.

- **Requerimiento 2**

Asignar o remover accesos para administrar el sistema y la seguridad.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que permita administrar el control en la asignación y remoción de los privilegios para la administración del sistema y la seguridad:** Este proceso debe controlar la asignación y/o remoción de los privilegios para la administración del sistema y la seguridad del mismo. Este proceso debe ejecutarse de manera permanente y validar que los accesos sean los adecuados y autorizados por el dueño del sistema. El proceso debe realizar revalidaciones a estos accesos de manera trimestral y anual con el fin de asegurar que los usuarios que cuenten con este tipo de accesos sean revalidados y que estén haciendo buen uso de los mismos. Esto con el fin de proteger la integridad y disponibilidad del sistema operativo.

- **Requerimiento 3**

Prevenir la ejecución y propagación de códigos dañosos.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que permita prevenir la ejecución y propagación de códigos dañosos (virus):** Este proceso debe ejecutarse y contemplar las siguientes actividades con el fin de prevenir la propagación y ejecución de códigos dañosos (virus):

    - Definir por parte del área de seguridad informática de la organización el programa antivirus que se utilizará en los sistemas de información.

    - El área de seguridad informática de la organización deberá estar suscrita a un site para actualizar el programa antivirus.

    - Instalar la versión del programa antivirus más reciente en los sistemas de información.

    - Configurar el programa de antivirus de tal forma que se conecte al web site suscrito para actualizar la versión del mismo y la lista de virus. Esto debe hacerse al menor una vez al día. Si esto no es posible hacerlo de manera automática deberá hacerse de manera manual.

    - Configurar el programa de antivirus para ser ejecutado en todo el sistema de información al menos una vez por semana, si no es posible hacer esto de manera automática se deberá definir un proceso que asegure que se realizará manualmente.

    - En caso de que el sistema de información se contamine y/o infecte por un virus deberá ser desconectado de la red, ejecutar la última versión del programa de antivirus vigente y dar aviso al área de seguridad informática de la organización para que ésta tome las acciones pertinentes al respecto y registre el record por sistema de información de las infecciones acontecidas.

    - Antes de realizar la instalación de algún software, programa, paquete, desarrollo, etc., en un sistema de información se debe ejecutar el programa de antivirus con el fin de prevenir la ejecución y propagación de un código dañoso (virus).

- **Requerimiento 4**

Identificar vulnerabilidades al sistema.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que permita identificar las vulnerabilidades del sistema:** Este proceso debe identificar las vulnerabilidades del sistema, para lo cual es necesario ejecutar una herramienta que identifique las vulnerabilidades del mismo. Esta herramienta deberá ser definida por el área de seguridad informática de la organización. Dependiendo del tipo de sistema de información se deberá ejecutar esta herramienta periódicamente:

  - En Sistemas de Información bajo un ambiente operativo de Internet que proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes, servicios de web, la herramienta de identificación de vulnerabilidades deberá ejecutarse semanalmente.

  - En Sistemas de Información bajo un ambiente operativo de intranet que contengan aplicaciones confidenciales o que ejecuten directamente un proceso vital del negocio o financiero, la herramienta de identificación de vulnerabilidades deberá ejecutarse trimestralmente.

  - En Sistemas de Información bajo un ambiente operativo de intranet que se dediquen al correo electrónico, servicios web (interno), servicios de recuperación en caso de desastres, servicios de DNS (Domain Network Services), servicios de DHCP (Domain Host Communication Protocol), la herramienta de identificación de vulnerabilidades deberá ejecutarse trimestralmente.

  - En Sistemas de Información bajo un ambiente operativo de intranet que proporcionen servicio a áreas locales, departamentales o de desarrollo, la

herramienta de identificación de vulnerabilidades deberá ejecutarse semestralmente.

- En Sistemas de Información bajo un ambiente operativo de intranet que se dediquen a demostraciones, educación, propósitos especiales, sistemas de prueba, etc., la herramienta de identificación de vulnerabilidades deberá ejecutarse semestralmente.

- En Sistemas de Información bajo un ambiente operativo de intranet administrados por proveedores, la herramienta de identificación de vulnerabilidades deberá ejecutarse semestralmente.

- **Requerimiento 5**

Aplicar los parches de seguridad al sistema.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que aplique los parches de seguridad al sistema:** Este proceso debe contemplar el acceso al web site del fabricante de la plataforma del sistema operativo para bajar los parches de seguridad que se deben instalar en el sistema de información. Estos parches son actualizaciones al sistema operativo y se clasifican por severidad: alta, media y baja dependiendo de la criticidad del mismo y tienen un tiempo de instalación. El proceso para la aplicación de los parches de seguridad al sistema de información debe contemplar el acceso al web site y el tiempo en que se deben de instalar. Este proceso debe apoyarse a través de una herramienta que controle y administre la aplicación de parches de seguridad a los sistemas de información en tiempo y forma. Esta herramienta debe ser definida por el área de seguridad informática de la organización. A continuación se citan los tiempos promedio en que se deben instalar estos parches en los sistemas de información dependiendo de la severidad de los mismos.

Severidad Alta:

- Para Sistemas de Información bajo un ambiente operativo de Internet que proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes, servicios de web; los parches con severidad alta, deben instalarse en un tiempo promedio de 3 días.

- Para Sistemas de Información bajo un ambiente operativo de intranet que se dediquen al correo electrónico, servicios web (interno), servicios de recuperación en caso de desastres, servicios de DNS (Domain Network Services), servicios de DHCP (Domain Host Communication Protocol); los parches con severidad alta, deben instalarse en un tiempo promedio de 7 días.

- Para Sistemas de Información bajo un ambiente operativo de intranet que contengan aplicaciones confidenciales o que ejecuten directamente un proceso vital del negocio o financiero, los parches con severidad alta, deben instalarse en un tiempo promedio de 30 días.

- Para Sistemas de Información bajo un ambiente operativo de intranet que proporcionen servicio a áreas locales, departamentales, de desarrollo, de demostraciones, de educación, propósitos especiales, sistemas de prueba, de proveedores, etc., los parches con severidad alta, deben instalarse en un tiempo promedio de 60 días.

Severidad Media:

- Para Sistemas de Información bajo un ambiente operativo de Internet que proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes, servicios de web; los parches con severidad media, deben instalarse en un tiempo promedio de 7 días.

- Para Sistemas de Información bajo un ambiente operativo de intranet que se dediquen al correo electrónico, servicios web (interno), servicios de recuperación en caso de desastres, servicios de DNS

(Domain Network Services), servicios de DHCP (Domain Host Communication Protocol); los parches con severidad media, deben instalarse en un tiempo promedio de 60 días.

- Para Sistemas de Información bajo un ambiente operativo de intranet que contengan aplicaciones confidenciales o que ejecuten directamente un proceso vital del negocio o financiero, los parches con severidad media, deben instalarse en un tiempo promedio de 90 días.

- Para Sistemas de Información bajo un ambiente operativo de intranet que proporcionen servicio a áreas locales, departamentales, de desarrollo, de demostraciones, de educación, propósitos especiales, sistemas de prueba, de proveedores, etc., los parches con severidad media, deben instalarse en un tiempo promedio de 90 días.

Severidad Baja:

- Para Sistemas de Información bajo un ambiente operativo de Internet que proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes, servicios de web; los parches con severidad baja, deben instalarse en un tiempo promedio de 30 días.

- Para Sistemas de Información bajo un ambiente operativo de intranet que se dediquen al correo electrónico, servicios web (interno), servicios de recuperación en caso de desastres, servicios de DNS (Domain Network Services), servicios de DHCP (Domain Host Communication Protocol); los parches con severidad baja, deben instalarse en un tiempo promedio de 180 días.

- Para Sistemas de Información bajo un ambiente operativo de intranet que contengan aplicaciones confidenciales o que ejecuten directamente un proceso vital del negocio o financiero, los parches con severidad baja, deben instalarse en un tiempo promedio de 12 meses.

- Para Sistemas de Información bajo un ambiente operativo de intranet que proporcionen servicio a áreas locales, departamentales, de desarrollo, de demostraciones, de educación, propósitos especiales, sistemas de prueba, de proveedores, etc., los parches con severidad baja, deben instalarse en un tiempo promedio de 12 meses.

- **Requerimiento 6**

Autorizar cualquier tipo de instalación, modificación o cambio al software del sistema.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que autorice y administre la instalación, modificación o cambio al software del sistema de información:** Este proceso debe ejecutarse de manera permanente y contemplar la autorización por parte del dueño del sistema de información por cada instalación, modificación o cambio en el software del sistema de información. Este proceso debe apoyarse a través de una herramienta que controle y administre este tipo de eventos de tal forma que por cada sistema de información se tenga un historial de todos los eventos a los que fue sometido así como las autorizaciones correspondientes tanto de los dueños del sistema de información como de las áreas usuarias u operativas afectadas. Esta herramienta debe ser definida por el área de seguridad informática de la organización.

- **Requerimiento 7**

Negar el Servicio.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que administre la habilitación y/o deshabilitación de los servicios de un sistema de información:** Este requerimiento se refiere a la habilitación y/o deshabilitación de los puertos de servicio que conforme a las especificaciones técnicas de la

plataforma del sistema de información deben estar cerrados o abiertos ya que a través de ellos (los puertos) se realizan todas las transacciones del sistema de información con el medio exterior a nivel LAN y/o WAN. Por estos puertos el sistema de información puede ser vulnerable por lo que es de suma importancia tener una justificación de negocio y la autorización correspondiente del dueño de la aplicación y del sistema de información por cada puerto que requiera ser abierto. Por lo anterior el proceso que administre la activación o desactivación de los puertos del sistema de información debe ejecutarse de manera permanente y apoyarse de una herramienta que controle, administre e identifique a través de la red que puertos están abiertos o cerrados en el sistema de información. Esta herramienta debe ser definida por el área de seguridad informática de la organización.

- **Requerimiento 8**

Ataques Sistemáticos de Login.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que detecte ataques sistemáticos de acceso a los sistemas de información:** Este requerimiento se refiere a que un sistema de información puede ser atacado sistemáticamente a través de login; es decir, a través de un usuario y un password. Este tipo de ataque es secuencial y metódico (con metodología en acciones y tiempos). Este tipo de ataques se enfocan a intentar acceder al sistema de información a través de un usuario y un password que obtuvieron de alguna forma. Dependiendo del tipo de plataforma del sistema operativo es posible configurar un parámetro que limite el número de intentos de acceso de login por usuario con el fin de proteger al sistema de información de un ataque de este tipo (el estándar indica 5 intentos máximos por usuario). Por lo anterior el proceso que detecte ataques sistemáticos de acceso a los sistemas de información debe identificar y registrar los intentos que tiene cada usuario al acceder el sistema de información y al detectar 5 intentos seguidos por usuario, éste debe ser bloqueado ya que se le considerará como ataque sistemático. Este proceso debe

ejecutarse de manera permanente y apoyarse de una herramienta que identifique y registre los intentos de acceso al sistema de información por usuario, así mismo es conveniente que se lleve un record por usuario ya que un ataque sistemático se puede realizar en diferentes tiempos y circunstancias. Si un usuario es identificado porque realiza continuamente este tipo de acciones se le debe dar de baja. Esta herramienta debe ser definida por el área de seguridad informática de la organización.

4.6 Auditoría Activa

El objetivo del elemento Auditoría Activa como estrategia de seguridad es establecer un mecanismo para identificar anomalías en los usuarios internos y externos, así como en los componentes de infraestructura de la red.

4.6.1 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.
- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.
- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

Con ayuda del área de seguridad informática de la organización deberá tratarse y analizarse caso por caso, para dar guía en el cumplimiento de las políticas de seguridad en los sistemas de

información definidas originalmente, esto deberá hacerse a través de las revisiones periódicas – auditorías internas - como resultado de esto, se deberán generar planes de acción que ayuden a la mejora continua de los procesos y como consecuencia el cumplimiento de las políticas de seguridad.

4.6.2 Puntos de Cumplimiento

A continuación (tabla 4.7) se indican los puntos a cumplir para este elemento de seguridad interna – auditoría activa - en un sistema de información:

AUDITORÍA ACTIVA Puntos de Cumplimiento	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)
Registros de Auditoría	
1. Registrar los intentos de acceso de login con éxito y sin éxito incluyendo: fecha, horario, tipo de intento de acceso e identificación del usuario.	
2. Actualizar los intentos de acceso a los OSRs no listados como excepciones.	
3. Identificar los intentos de acceso a los OSRs listados como excepciones.	
4. Identificar los intentos de acceso de ejecución a los OSRs listados como excepciones.	
5. Asignar direcciones IP de red.	
6. Almacenar los logs del sistema de información en un sistema ajeno y fuera de la red del sistema de información.	

Retención de los Registros de Auditoría	
7. Retener los registros de auditoría por 60 días.	

Tabla 4.7: Puntos de Cumplimiento del Elemento de Seguridad Auditoría Activa

La información contenida en la tabla 4.7 debe ser utilizada para asegurar el cumplimiento de este elemento (auditoría activa) de seguridad interna en un sistema de información, tabla que debe ser actualizada por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa una copia de esta tabla 4.7 será solicitada y retenida por el auditor.

4.6.3 Descripción de los Requerimientos

- **Requerimiento 1**

Registrar los intentos de acceso de login con éxito y sin éxito incluyendo: fecha, horario, tipo de intento de acceso e identificación del usuario.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que registre los intentos de acceso de login exitosos o no a los sistemas que proporcionan servicios Inter-Empresa:** Este proceso debe registrar los intentos de acceso de login exitosos o no a los sistemas que proporcionan servicios de Inter-Empresa. El registro de estos intentos debe incluir lo siguiente: fecha de intento de acceso (exitoso o no), horario de intento de acceso (exitoso o no), tipo de intento de acceso (exitoso o no) e identificación de usuario. Este proceso debe estar activo en el sistema que proporciona servicios Inter-Empresa y debe ejecutarse constantemente.

- **Requerimiento 2**

Actualizar los intentos de acceso a los OSRs no listados como excepciones.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que actualice los intentos de acceso a los OSRs (Operating System Resources ó Recursos del Sistema Operativo) no listados como excepciones:** Este proceso debe actualizar los intentos de acceso a los Recursos del Sistema Operativo que no están identificados como excepciones. Este proceso debe estar activo en el sistema que proporciona servicios Inter-Empresa y debe ejecutarse constantemente.

- **Requerimiento 3**

Identificar los intentos de acceso a los OSRs listados como excepciones.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que identifique los intentos de acceso a los OSRs (Operating System Resources o Recursos del Sistema Operativo) listados como excepciones:** Este proceso debe identificar los intentos de acceso a los Recursos del Sistema Operativo que están identificados como excepciones. Este proceso debe estar activo en el sistema que proporciona servicios Inter-Empresa y debe ejecutarse constantemente.

- **Requerimiento 4**

Identificar los intentos de acceso de ejecución a los OSRs listados como excepciones.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que identifique los intentos de acceso de ejecución a los OSRs (Operating System Resources ó Recursos del Sistema Operativo) listados como excepciones:** Este proceso debe identificar los intentos de acceso de ejecución a los Recursos del Sistema Operativo que están identificados como excepciones. Este proceso debe estar activo en el sistema

que proporciona servicios Inter-Empresa y debe ejecutarse constantemente.

- **Requerimiento 5**

Asignar direcciones IP de red.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que controle la asignación de direcciones IP de red:** Este proceso debe controlar la asignación de direcciones IP de red. Así mismo este proceso debe identificar en todo momento las direcciones IP asignadas a los dispositivos conectados en la red. Este proceso debe revalidar periódicamente – trimestral, semestral o anualmente con base en las políticas de seguridad establecidas por la organización – la identificación de las direcciones IP de red de los dispositivos conectados a la misma.

- **Requerimiento 6**

Almacenar los logs del sistema de información en un sistema ajeno y fuera de la red del sistema de información.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que almacene los logs de los sistemas de información en un sistema ajeno a la red en donde se encuentra el sistema de información:** Por cuestiones de integridad de la información, este proceso debe realizar una copia intacta del log del sistema de información en otro sistema que se encuentre en una red diferente a la que se encuentra el sistema de información. El proceso debe especificar que la copia del log del sistema de información debe realizarse diario con el fin de mantener detalle de las transacciones que se realizan con respecto al sistema de información.

- **Requerimiento 7**

Retener los registros de auditoría por 60 días.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que retenga los registros de auditoría por 60 días:** Por cuestiones históricas, de auditoría y seguimiento de las transacciones que se realizan en el sistema de información, el proceso debe retener por 60 días los logs del sistema de información que resguardan los registros de estas transacciones.

4.7 Verificación

El objetivo del elemento Verificación como estrategia de seguridad es establecer un mecanismo consistente para verificar la adherencia del cumplimiento de la política de seguridad establecida por la organización.

4.7.1 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.
- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.
- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

Con ayuda del área de seguridad informática de la organización deberá tratarse y analizarse caso por caso, para dar guía en el cumplimiento de las políticas de seguridad en los sistemas de información definidas originalmente, esto deberá hacerse a través de las

revisiones periódicas – auditorías internas - como resultado de esto, se deberán generar planes de acción que ayuden a la mejora continua de los procesos y como consecuencia el cumplimiento de las políticas de seguridad.

4.7.2 Puntos de Cumplimiento

A continuación (tabla 4.8) se indican los puntos a cumplir para este elemento de seguridad interna – verificación - en un sistema de información:

VERIFICACIÓN **Puntos de Cumplimiento**	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)
Verificación de Salud	
1. Realizar la verificación de salud a los dispositivos de la infraestructura.	
2. Realizar la verificación de salud a las aplicaciones.	
3. Corregir las desviaciones identificadas en las verificaciones de salud realizadas a los dispositivos de la infraestructura como en las aplicaciones.	
Revisar Proceso de Seguridad	
4. Revisar el cumplimiento de los procesos de seguridad a una muestra significativa de la infraestructura.	

Tabla 4.8: Puntos de Cumplimiento del Elemento de Seguridad Verificación

La información contenida en la tabla 4.8 debe ser utilizada para asegurar el cumplimiento de este elemento (verificación) de seguridad interna en un sistema de información, tabla que debe ser actualizada

por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa una copia de esta tabla 4.8 será solicitada y retenida por el auditor.

4.7.3 Descripción de los Requerimientos

- **Requerimiento 1**

Realizar la verificación de salud a los dispositivos de la infraestructura.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que realice la verificación de salud a los dispositivos de la infraestructura de la organización:** Este proceso debe ejecutarse de la siguiente forma:

  - Trimestralmente para los sistemas de información críticos y/o vitales definidos por la organización tales como: sistemas de información de Internet, servicios a cliente, recuperación de desastres, etc.

  - Semestralmente para los sistemas de información de infraestructura de red definidos por la organización tales como: sistemas de información de servicios de DHCP, DNS, firewalls, etc.

  - Anualmente para los sistemas de información de aplicaciones definidas por la organización tales como: aplicaciones de facturación, contables, fiscales, nóminas, etc.

  Para los sistemas de información crítica y/o vital y de infraestructura de red definidos por la organización, este proceso debe hacer lo siguiente:

  - El control de acceso al sistema debe ser regulado acorde a las especificaciones técnicas de la plataforma operativa del sistema de información.

- Deben estar identificados los usuarios autorizados que administran y controlar la seguridad en estos sistemas de información.

- El acceso a los Operating Systems Resources (OSR) debe estar controlado acorde a las especificaciones técnicas que la plataforma del sistema de información especifique.

- **Requerimiento 2**

Realizar la verificación de salud a las aplicaciones.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que realice la verificación de salud a las aplicaciones de la organización:** Este proceso debe ejecutarse de la siguiente forma:

  - El proceso de verificación de la salud de las aplicaciones debe asegurar que los usuarios aprobados son los únicos que cuentan con los permisos para administrar la seguridad de las aplicaciones.

  - El log de las aplicaciones en donde se registran las actividades realizadas por todos los usuarios finales y administradores debe estar activo y contener un histórico de estas actividades de al menos 60 días.

- **Requerimiento 3**

Corregir las desviaciones identificadas en las verificaciones de salud realizadas a los dispositivos de la infraestructura como en las aplicaciones.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que elimine las desviaciones identificadas en las verificaciones de salud realizadas a los dispositivos de la infraestructura como en las aplicaciones de la**

organización: Este proceso debe contemplar todas las actividades que la organización y el área de seguridad interna consideren convenientes para eliminar todas las desviaciones reportadas durante la verificación de salud a los dispositivos de infraestructura y a las aplicaciones. Estas actividades van desde la reunión inicial para la presentación de estas desviaciones, presentación de planes de trabajo, instalación de software, desarrollos, reuniones periódicas de seguimiento, hasta la reunión final del cierre de todas las desviaciones. Una actividad inicial por parte del área de seguridad interna es la asignación apropiada del nivel de riesgo de cada desviación identificada, seguidamente otra actividad muy importante es la creación de un plan de trabajo que refleje todas las actividades necesarias para cerrar las desviaciones identificadas durante la verificación de la salud de los dispositivos de infraestructura y de las aplicaciones de la organización. Este plan de trabajo debe contener responsables y fecha de terminación de cada actividad. El área de seguridad interna de la organización es la responsable de darle seguimiento a este plan y por consecuencia al proceso, para el éxito del mismo. Las áreas proveedoras de los servicios (los que administran y manejan los dispositivos de infraestructura y las aplicaciones) son los responsables de ejecutar las actividades del plan de trabajo.

- **Requerimiento 4**

Revisar el cumplimiento de los procesos de seguridad a una muestra significativa de la infraestructura.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que revise el cumplimiento de los procesos de seguridad a una muestra significativa de la infraestructura de la organización:** Este proceso debe ser supervisado por el área de seguridad interna de la organización y ejecutado por el área que proporciona el servicio. Este proceso debe realizarse anualmente y revisar los elementos de seguridad listados a continuación. Este proceso debe aplicarse a una muestra significativa de los dispositivos de la infraestructura de la organización. Para fines de auditoría la evidencia generada de esta revisión debe conservarse. Los elementos

de seguridad a revisar que inclusive ya han sido tratados en el presente capítulo son los siguientes:

- Revisar los puntos de cumplimiento de cada elemento de seguridad, así como los procesos indicados en cada uno:

  - Para el elemento de seguridad Identificación revisar el punto 4.1.
  - Para el elemento de seguridad Autenticación revisar el punto 4.2.
  - Para el elemento de seguridad Autorización revisar el punto 4.3.
  - Para el elemento de seguridad Protección de la Información y Confidencialidad revisar el punto 4.4.
  - Para el elemento de seguridad Integridad y Disponibilidad del Servicio revisar el punto 4.5.
  - Para el elemento de seguridad Auditoría Activa revisar el punto 4.6.
  - Para el elemento de seguridad Verificación revisar el punto 4.7.
  - Para el elemento de seguridad Reporte de Incidentes de Seguridad y su Manejo revisar el punto 4.8.
  - Para el elemento de seguridad Controles de Acceso a Medios Magnéticos revisar el punto 4.9.

- El área que proporciona el servicio, es decir; la que ejecuta por cuestiones de auditoría debe generar y conservar la evidencia necesaria del cumplimiento de los procesos en los que se incurre en cada elemento de seguridad.

- El área de seguridad interna de la organización como responsable de la supervisión del cumplimiento de este proceso debe ser totalmente independiente y/o ajena al área que proporciona el servicio, es decir; la que ejecuta.

- El área de seguridad interna por cuestiones de seguridad debe conservar evidencia de las revisiones hechas del cumplimiento de este proceso.

4.8 Reporte de Incidentes de Seguridad y su Manejo

El objetivo del elemento Reporte de Incidentes de Seguridad y su Manejo como estrategia de seguridad es establecer un mecanismo consistente para identificar, reportar y manejar algún incidente de seguridad que atente contra la infraestructura o sistema de información y aportar con ello el cumplimiento de la política de seguridad establecida por la organización.

4.8.1 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.
- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.
- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

Con ayuda del área de seguridad informática de la organización deberá tratarse y analizarse caso por caso, para dar guía en el cumplimiento de las políticas de seguridad en los sistemas de información definidas originalmente, esto deberá hacerse a través de las revisiones periódicas – auditorías internas - como resultado de esto, se deberán generar planes de acción que ayuden a la mejora continua de los procesos y como consecuencia el cumplimiento de las políticas de seguridad.

4.8.2 Puntos de Cumplimiento

A continuación (tabla 4.9) se indican los puntos a cumplir para este elemento de seguridad interna – Reporte de Incidentes de Seguridad y su Manejo - en un sistema de información:

REPORTE DE INCIDENTES DE SEGURIDAD Y SU MANEJO Puntos de Cumplimiento	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)
Incidentes de Seguridad	
1. Reportar el incidente de seguridad.	
2. Reportar accesos no autorizados.	
3. Reportar el abuso de autoridad.	

Tabla 4.9: Puntos de Cumplimiento del Elemento de Seguridad Reporte de Incidentes de Seguridad y su Manejo

La información contenida en la tabla 4.9 debe ser utilizada para asegurar el cumplimiento de este elemento (reporte de incidentes de seguridad y su manejo) de seguridad interna en un sistema de información, tabla que debe ser actualizada por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa una copia de esta tabla 4.9 será solicitada y retenida por el auditor.

4.8.3 Descripción de los Requerimientos

- **Requerimiento 1**

  Reportar el incidente de seguridad.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que permita identificar, reportar y manejar algún incidente de seguridad que atente contra la infraestructura o sistema de información de la organización:** Este proceso debe ejecutarse de manera permanente y el responsable del cumplimiento del mismo es el área de seguridad interna de la organización. Este proceso debe contemplar las actividades necesarias desde identificar el incidente, darle el trato y el seguimiento adecuado hasta su cierre. Independientemente del tipo y/o clasificación del incidente de seguridad del que se trate tales como: accesos no autorizados (a información clasificada, confidencial, vital para el negocio, localidades, etc.), caída o alteración de la integridad de la infraestructura, destrucción de la información, fraude, crimen, etc., se deben de ejecutar las siguientes acciones:

    - Reportar el incidente al área de seguridad interna de la organización proporcionando los siguientes datos: descripción del incidente, la infraestructura afectada, ubicación del incidente, sospecho (si existe).

    - El área de seguridad interna de la organización como responsable del cumplimiento de este proceso es quien deberá reportar el incidente a las direcciones y áreas correspondientes dentro de la organización dependiendo del tipo de incidente y de la infraestructura afectada.

    - El área de seguridad interna de la organización debe tener una lista de contactos con nombre, puesto, responsabilidad, área, número telefónico, extensión, email, etc., esto con el fin de poder contactar a quien sea necesario.

    - El área de seguridad interna de la organización debe reportar el incidente ocurrido al área afectada para que ésta evalúe el daño y el riesgo. Así mismo el área afectada deberá declararse en contingencia y ejecutar su plan de recuperación de desastres y deberá tomar las acciones necesarias para minimizar el impacto por

el incidente de seguridad ocurrido y proteger la infraestructura de la organización.

- El área de seguridad interna de la organización debe iniciar una investigación del incidente de seguridad, para ello debe recolectar toda la información y evidencia posible sobre el incidente. El área de seguridad interna debe involucrar a todas las áreas internas de la organización que considere necesarias, así como a las dependencias externas a la organización para el esclarecimiento del incidente de seguridad y deslindar responsabilidades.

- **Requerimiento 2**

Reportar accesos no autorizados.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que identifique los accesos no autorizados a la infraestructura de la organización:** Este proceso debe ejecutarse de manera permanente y el responsable del cumplimiento del mismo es el área que proporciona el servicio. Este proceso debe contemplar las actividades necesarias para identificar los accesos no autorizados y los intentos de login a la infraestructura y deben ser reportados al área de seguridad interna de la organización para que se le de el trato adecuado.

- **Requerimiento 3**

Reportar el abuso de autoridad.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que identifique los abusos de autoridad en el manejo de los dispositivos de la infraestructura de la organización:** Este proceso debe ejecutarse de manera permanente e identificar los abusos de autoridad a través del registro de las actividades en los logs de los dispositivos de la infraestructura y de las

revisiones de auditoría interna o externa que éstos tengan. El responsable del cumplimiento de este proceso es el área que proporciona el servicio, quien deberá reportar estos abusos al área de seguridad interna. Esta última debe contemplar todas las acciones necesarias para evitar estos abusos de autoridad en cuanto al manejo de los dispositivos de la infraestructura de la organización.

4.9 Controles de Acceso a Medios Magnéticos

El objetivo del elemento Controles de Acceso a Medios Magnéticos como estrategia de seguridad es mitigar el riesgo de robo, daño, revelación o borrado de la información almacenada en los medios magnéticos de los sistemas de información y aportar con ello el cumplimiento de la política de seguridad establecida por la organización.

4.9.1 Alcance

Este elemento debe ser aplicable a cualquier tipo de sistema de información independientemente de su tecnología o plataforma de sistema operativo.

Los sistemas de información que están dentro del alcance de este elemento son aquellos que:

- Proporcionen servicio a la producción del negocio de la empresa.
- Proporcionen servicios de conexión inter-empresarial (conexiones remotas) a sus clientes.
- Contengan aplicaciones de negocio las cuales tienen procesos o acceso a información confidencial.
- Contengan aplicaciones que ejecuten directamente un proceso vital del negocio.
- Proporcionen servicio a áreas locales, departamentales o de desarrollo.
- Estén dedicados a demostraciones, educación, propósitos especiales, sistemas de prueba, etc.
- Sean administrados por proveedores.

Con ayuda del área de seguridad informática de la organización deberá tratarse y analizarse caso por caso, para dar guía en el cumplimiento de las políticas de seguridad en los sistemas de información definidas originalmente, esto deberá hacerse a través de las

revisiones periódicas – auditorías internas - como resultado de esto, se deberán generar planes de acción que ayuden a la mejora continua de los procesos y como consecuencia el cumplimiento de las políticas de seguridad.

4.9.2 Puntos de Cumplimiento

A continuación (tabla 4.10) se indican los puntos a cumplir para este elemento de seguridad interna – Controles de Acceso a Medios Magnéticos - en un sistema de información:

CONTROLES DE ACCESO A MEDIOS MAGNÉTICOS Puntos de Cumplimiento	
Nombre del Sistema, Aplicación o Dispositivo de Infraestructura:	
Dueño del Sistema, Aplicación o Dispositivo de Infraestructura:	
Fecha de Revisión:	
Versión de Revisión:	
Requerimientos:	**Estatus de Cumplimiento:** Sí / No (Riesgo: Aceptable & No Aceptable)
Protección Física de los Medios de Almacenamiento	
1. Almacenar los medios magnéticos en áreas con control de acceso.	
Control de Inventario de los Medios Custodiados	
2. Implantar un procedimiento para controlar el inventario de los medios magnéticos.	

Tabla 4.10: Puntos de Cumplimiento del Elemento de Seguridad Controles de Acceso a Medios Magnéticos

La información contenida en la tabla 4.10 debe ser utilizada para asegurar el cumplimiento de este elemento (controles de acceso a medios magnéticos) de seguridad interna en un sistema de información, tabla que debe ser actualizada por el área de seguridad informática de la organización, cada vez que revise y actualice las políticas de seguridad y del resultado de las revisiones periódicas – auditorías internas – que se le realicen al sistema de información. En una auditoría interna o externa una copia de esta tabla 4.10 será solicitada y retenida por el auditor.

4.9.3 Descripción de los Requerimientos

- **Requerimiento 1**

Almacenar los medios magnéticos en áreas con control de acceso.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que controle el almacenaje y el acceso a los medios magnéticos en áreas de acceso controlado de los sistemas de información de la organización:** Este proceso debe ejecutarse de manera permanente y el responsable del cumplimiento del mismo es el área que proporciona el servicio. Los medios de almacenamiento como cintas de respaldo, retención de registros, cintas para la recuperación de desastres, etc., deben ser almacenadas en áreas con controles de acceso con base en las políticas de seguridad establecidas por la organización. Estas áreas deben autenticar a los usuarios que las accedan a través de alguno de los siguientes sistemas:

  - Sistema de contraseñas.
  - Sistema de tarjetas inteligentes.
  - Sistemas biométricos como: reconocimientos de voz, escritura, huellas, oculares, geometría de mano, etc.
  - Sistema de videocámaras con circuito cerrado para vigilar constantemente los accesos al área.

  Este proceso debe controlar el almacenaje de los medios magnéticos y debe contemplar las siguientes actividades con base en las políticas de seguridad establecidas por la organización:

  - Identificar los medios de almacenamiento a través de etiquetas que contengan un número y/o nombre que los identifique y el emblema "Puede contener Información Confidencial"

  - Tener un procedimiento del montaje de los medios de almacenamiento en los sistemas de información.

- Los medios de almacenamiento utilizados para el respaldo de los sistemas de información deben estar separados de los medios de almacenamiento custodiados en el área de acceso controlado, para asegurar su disponibilidad en caso de ser requerida su recuperación.

- Tener una copia de los medios de almacenamiento custodiados en el área de acceso controlado en otra área fuera del área de custodia, esto con el fin de asegurar su disponibilidad en caso de ser requerida su recuperación.

- **Requerimiento 2**

Implantar un procedimiento para controlar el inventario de los medios magnéticos.

Las siguientes especificaciones deben ser incluidas en la implantación de este requerimiento:

- **Desarrollar e implantar un proceso que permita controlar el inventario de los medios magnéticos en las áreas de almacenaje de acceso controlado de los sistemas de información de la organización:** Este proceso debe ejecutarse de manera permanente y se debe hacer una reconciliación anual de los medios magnéticos. El responsable del cumplimiento de este proceso es el área que proporciona el servicio. Este proceso debe contemplar las siguientes actividades:

  - Hacer un inventario inicial de los medios de almacenamiento de las áreas de almacenaje de acceso controlado.

  - Identificar e incluir en el inventario los medios de almacenamiento que provienen de otra localidad.

  - Identificar e incluir en el inventario los medios de almacenamiento que se envían del área de almacenaje a otra localidad (como bajas).

  - Identificar e incluir en el inventario los medios de almacenamiento nuevos.

- Identificar e incluir en el inventario los medios de almacenamiento que se envían a scrap (medios que se destruyen por expiración de tiempo de vida o daño). Identificarlos como bajas.

- Todo el inventario anterior representa el inventario total de medios de almacenamiento ubicados en las áreas de almacenaje de acceso controlado.

- Todas las discrepancias o desviaciones detectadas deben ser reportadas al responsable del proceso de control del inventario de medios magnéticos de las áreas de acceso controlado para que tome las acciones pertinentes.

- El responsable del proceso de control del inventario de medios magnéticos debe firmar el inventario total.

- El último inventario anual de reconciliación de medios magnéticos debe estar firmado y retenido por el responsable del proceso de control del inventario de medios magnéticos.

- Es recomendable que al menos una persona totalmente ajena al proceso del control de inventarios de los medios magnéticos custodiados conduzca o participe en el proceso de inventario de custodia y reconciliación.

CAPÍTULO V

Auditoría de los Sistemas de Información

5.1 Introducción

La auditoría de los sistemas de la información adquiere cada vez mayor importancia, debido a la necesidad de garantizar la seguridad, continuidad y disponibilidad de las infraestructuras informáticas sobre las que se sustentan los procesos de negocio de toda empresa u organismo, necesitando adicionalmente que todos estos procesos se realicen de forma eficiente. Por otra parte los entornos legislativos actuales también hacen referencia a la obligatoriedad de acreditar el cumplimiento de sus normas mediante auditorías de sistemas de información y, como parte consustancial de la auditoría financiera, se está requiriendo cada vez más que los sistemas de información sean, a su vez, auditados.

5.2 Normas Generales

La Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información, o ISACA por sus siglas en inglés) comenzó operaciones en 1967, cuando un pequeño grupo de personas con trabajos similares -controles de auditoría en los sistemas computarizados que se estaban haciendo cada vez más críticos para las operaciones de sus organizaciones respectivas - se reunieron para ver la necesidad de tener una fuente centralizada de información y guía en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor del campo de gobernación y control de tecnología de información.

Hoy, los miembros de ISACA - más de 28,000 en todo el mundo - se caracterizan por su diversidad. Los miembros viven y trabajan en más de 100 países y cubren una variedad de puestos profesionales relacionados con la tecnología de información - sólo para nombrar algunos ejemplos de puestos tenemos: auditor de sistemas de información, consultor, educador, profesional de seguridad de sistemas de información, regulador, director ejecutivo de información y auditor interno -. Algunos son nuevos en el campo, otros están en niveles medios de supervisión y algunos otros están en los rangos más elevados. Trabajan en casi todas las categorías de industrias, incluyendo finanzas y banca, contaduría pública, gobierno y sector público, servicios públicos y manufactura. Esta diversidad permite que los miembros aprendan unos de otros, e intercambien puntos de vista con

divergencias significativas en una variedad de tópicos profesionales. Ha sido considerada durante largo tiempo como uno de los puntos fuertes de ISACA.

Otro de los puntos fuertes de ISACA es su red de centros de información. ISACA tiene centros de información en más de 60 países en todo el mundo, y dichos centros brindan a sus miembros educación, recursos compartidos, promociones, contactos profesionales y una amplia gama de beneficios adicionales.

En las tres décadas transcurridas desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de sistemas de información. Sus normas de auditoría y control de sistemas de información son respetados por profesionales de todo el mundo. Sus investigaciones resaltan temas profesionales que desafían a sus constituyentes. Su certificación Certified Information Systems Auditor (Auditor Certificado de Sistemas de Información, o CISA por sus siglas en inglés) es reconocida a nivel mundial y ha sido obtenida por más de 30,000 profesionales. Su nueva certificación Certified Information Security Manager (Gerente Certificado de Seguridad de Información, o CISM por sus siglas en inglés) se concentra exclusivamente en el sector de gerencia de seguridad de la información. Publica y organiza un periódico técnico líder en el campo de control de la información, el Information Systems Control Journal (Periódico de Control de Sistemas de Información) una serie de conferencias internacionales que se concentran en tópicos técnicos y administrativos pertinentes a las profesiones de gobernación de tecnología de información, aseguramiento, control, seguridad de sistemas de información, etc. Juntos, ISACA y su Instituto de Gobernación de Tecnología de Información (Information Technology Governance Institute) asociados lideren la comunidad de control de tecnología de la información y sirven a sus practicantes brindando los elementos que necesitan los profesionales de tecnología de la información en un entorno mundial en cambio permanente.

5.2.1 Introducción

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

Las normas promulgadas por la Asociación de Auditoría y Control de Sistemas de Información son aplicables al trabajo de auditoría realizado por miembros de la Asociación de Auditoría y Control de Sistemas de Información y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información.

5.2.2 Objetivo

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

5.2.3 Descripción de las Normas

5.2.3 1 Norma 010: Título de Auditoría

La Norma 010: Título de Auditoría, contempla una sola sección:

- **Sección 010.010: Responsabilidad, autoridad y rendimiento de cuentas.** La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

5.2.3 2 Norma 020: Independencia

La Norma 020: Independencia, contempla dos secciones:

- **Sección 020.010: Independencia Profesional.** En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

- **Sección 020.020: Relación Organizativa.** La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se esta auditando para permitir completar de manera objetiva la auditoría.

5.2.3 3 Norma 030: Ética y Normas Profesionales

La Norma 030: Ética y Normas Profesionales, contempla dos secciones:

- **Sección 030.010: Código de Ética Profesional.** El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

- **Sección 030.020: Atención Profesional.** En todos los aspectos del trabajo del auditor de sistemas de información se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

5.2.3 4 Norma 040: Idoneidad

La Norma 040: Idoneidad, contempla dos secciones:

- **Sección 040.010: Habilidades y Conocimientos.** El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

- **Sección 040.020: Educación Profesional Continua.** El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

5.2.3 5 Norma 050: Planificación

La Norma 050: Planificación, contempla una sección:

- **Sección 050.010: Planificación de la Auditoría.** El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

5.2.3 6 Norma 060: Ejecución del Trabajo de Auditoría

La Norma 060: Ejecución del Trabajo de Auditoría, contempla dos secciones:

- **Sección 060.010: Supervisión.** El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

- **Sección 060.020: Evidencia.** Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

5.2.3 7 Norma 070: Informes

La Norma 070: Informes, contempla una sección:

- **Sección 070.010: Contenido y Formato de los Informes.** En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe de formato apropiado a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura, la naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, así como cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

5.2.3 8 Norma 080: Actividades de Seguimiento

La Norma 080: Actividades de Seguimiento, contempla una sección:

- **Sección 080.010: Seguimiento.** El auditor de sistemas de información deberá solicitar y evaluar la información

apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implantado las acciones apropiadas de manera oportuna.

5.3 Auditoría de Sistemas de Información

El campo de la auditoría informática está fundamentado en dos aspectos que son la evaluación del software y hardware. El primero de ellos contiene el componente lógico de un sistema de información que va desde las aplicaciones informáticas hasta la configuración de los campos que se utilizan en el sistema de información.

El segundo componente físico o hardware comprende aquellos elementos físicos que intervienen en el sistema de información que comprenden los registros físicos, los periféricos y el ordenador central. En este último (hardware) se incide en auditoría sobre la salvaguarda de activos, esto es, tipos de custodia o requerimientos que comprenden todos los elementos físicos integrantes del sistema de información.

5.3.1 Concepto de Auditoría de Sistemas de Información

La palabra auditoría viene del latín auditorius y de ésta proviene auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se esta operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

Algunos autores proporcionan otros conceptos pero todos coinciden en hacer énfasis en la revisión, evaluación y elaboración de un informe para el ejecutivo encaminado a un objetivo específico en el ambiente computacional y los sistemas.

A continuación se citan algunas definiciones del concepto de Auditoría de Sistemas de Información:

- La Auditoría de los Sistemas de Información se define como la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los

procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

- La Auditoría de Sistemas de Información se define como la verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación, con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia.

- La Auditoría de Sistemas de Información es aquella revisión que se realiza sobre los entornos de tecnologías de la información, trasladando el papel de las revisiones tradicionales sobre estados financieros a los activos de hardware, software y elementos de comunicación que utilizan las organizaciones para el tratamiento informático.

- La Auditoría de Sistemas de Información es el proceso sistemático de obtención objetiva y evaluación de evidencias relativas a las declaraciones realizadas sobre sistemas informáticos y eventos (situaciones no habituales), para averiguar el grado de correspondencia entre las declaraciones y los criterios establecidos y comunicar los resultados a las personas interesadas.

- La Auditoría de Sistemas de Información es el proceso de recolección y evaluación de evidencias utilizadas para determinar cuando un sistema informático salvaguarda sus activos, mantiene la integridad de sus datos, ejecuta eficazmente los objetivos marcados por la organización con efectividad y consume los recursos eficientemente.

Los aspectos comunes a todas las definiciones anteriores de la Auditoría de Sistemas de Información son:

- **Examen Metódico:** dado que es del todo imprescindible para proceder a evaluar y verificar con éxito el servicio objeto de estudio es importante seguir un plan de trabajo sistematizado que permita llegar a conclusiones fundamentales.

- **Puntual y Discontinuo:** puntual o auditoría de corte, ya que la misma se hace sin un previo calendario y es discontinua en aras de buscar la independencia de quien la ejecuta respecto de la empresa.

- **Verificación y Evaluación de los Entornos Informáticos:** y no únicamente revisión, esto es, la auditoría de sistemas de información recoge el hecho de aportar valor añadido asesorando y proponiendo mejoras sobre la evidencia y puntos débiles.

La Auditoría de Sistemas de Información está destinada a mejorar la seguridad, eficacia, eficiencia y rentabilidad del entorno informático de la empresa.

La Auditoría de Sistemas de Información permite establecer una opinión objetiva fundada en evidencias encontradas.

5.3.2 Objetivos de la Auditoría de Sistemas de Información

Los objetivos a establecer en una auditoría de sistemas de información deben abarcar todo el entorno informático de la organización, que comprende desde el centro de proceso de datos hasta cualquier tipo de comunicación o redes que existan en el entorno físico del sistema de información.

Los factores determinantes para el establecimiento de los objetivos perseguidos por el auditor pueden ser los siguientes:

- Características de la organización objeto del estudio de auditoría.
- Características del departamento de informática de la organización a auditar.
- Limitaciones técnicas del auditor.
- Determinar el nivel de riesgo aparente del sistema de información a auditar.
- Identificar las áreas críticas de control en las que se detecten mayores índices de riesgo.
- Definir objetivos y alcance del trabajo a auditar.

Considerados estos factores podemos clasificar los objetivos que se persiguen con la Auditoría de Sistemas de Información en las siguientes categorías:

- Aquellos objetivos que colaboran a la mejora de la eficacia de la organización informática y protección de sus activos y recursos, como por ejemplo evaluación de los códigos de acceso.

- Aquellos objetivos que permitan garantizar que los sistemas de información produzcan resultados fiables en un plazo y costo aceptable y que satisfagan las necesidades de los usuarios.

- Aquellos objetivos que van destinados a mejorar los procedimientos, estándares y planificación, colaborando en su diseño y en la actualización de sus normas, esto es, no solo deben garantizar la efectividad del sistema (el logro de sus objetivos) sino también su eficiencia, o sea el que consume la mínima cantidad de recursos para conseguirlos.

5.3.3 Clasificación de Tipos de Auditorías Informáticas

5.3.3 1 Auditoría Informática de Aplicaciones, Bases de Datos, Programas

Una Auditoría Informática de Aplicaciones, Bases de Datos, Programas, etc., es una evaluación del llamado análisis de programación y sistemas, por ejemplo una aplicación podría tener las siguientes fases de auditoría:

- Prerrequisitos del usuario y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (preprogramación y programación)
- Pruebas
- Explotación

Todas estas fases deben estar sometidas a un exigente control interno, de lo contrario, puede producir insatisfacción del cliente, insatisfacción del usuario, altos costos, etc. Por lo tanto, la auditoría deberá comprobar la seguridad de los programas, bases de datos, aplicaciones, en el sentido de garantizar que el servicio ejecutado por el equipo en donde se ejecutan, los resultados sean exactamente los previstos y no otros.

5.3.3 2 Auditoría Informática de Sistemas de Información

Una Auditoría Informática de Sistemas de Información se ocupa de analizar la actividad que se conoce como técnica de sistemas, en todos sus factores, es decir; determina si un sistema de información salvaguarda sus activos, mantiene la integridad de sus datos, cumple con las normas de seguridad fijadas por la organización y la utilización de sus recursos es la adecuada. La importancia creciente de las telecomunicaciones ha propiciado que las redes LAN, WAN, MAN, cableado, etc., se auditen por separado, aunque formen parte del entorno general del sistema de información.

5.3.3 3 Auditoría Informática de Infraestructura de Red

Una Auditoría Informática de Infraestructura de Red deberá actuar sobre los equipos de comunicaciones tipo hubs, switches, routers, firewalls, con el fin de determinar si están operando adecuadamente y cumplen con las políticas de seguridad establecidas por la organización, por lo que es importante verificar las configuraciones de los equipos a detalle por ejemplo: a nivel puerto. Así mismo es la responsable de verificar si los enlaces de comunicación salvaguardan la seguridad de salida y acceso a la organización, para ello la auditoría debe verificar diagramas de conexión de los enlaces (incluir los enlaces de respaldo), cuántos son, de que tipo, de que ancho de banda, donde están instalados, que configuración tienen, a donde se conectan, que tipo de información viaje por ellos, etc. Otro punto importante a considerar es el cableado, la auditoría debe incluir la revisión de la topología de la red, longitudes, que tipo de cable es el que se está utilizando y si cumple con las políticas de seguridad definidas por la organización, se deben verificar las conexiones entre pisos, áreas, departamentos, centros de cómputo, áreas de comunicaciones, servidores, etc., con el fin de identificar puntos de conexión no permitidos o vulnerabilidades de accesos no autorizados.

5.3.3 4 Auditoría de la Seguridad Informática

Una Auditoría de la Seguridad Informática debe tener presente la cantidad de información almacenada en un sistema de información, la cual en muchos casos puede ser confidencial, ya sea para los usuarios, las empresas o las instituciones, lo que significa que se debe cuidar del mal uso de esta información, de los robos, los fraudes, sabotajes y sobre todo de la destrucción parcial o total. En la actualidad se debe

también cuidar la información de los virus informáticos, los cuales permanecen ocultos y dañan sistemáticamente los datos.

5.3.4 Desarrollo de una Auditoría de Sistemas de Información

El Desarrollo de una Auditoría de Sistemas de Información pudiese interpretarse como algo muy complicado y difícil de conducir y como consecuencia de cumplir con los objetivos y expectativas de la organización. Para ello el Desarrollo de una Auditoría de Sistemas de Información es más sencillo dividirla y llevarla a cabo a través de las siguientes fases:

1. Relación con la Organización.
2. Planificación de la Operación.
3. Desarrollo de la Auditoría.
4. Síntesis y Diagnóstico.
5. Presentación de Conclusiones.
6. Redacción de Informe y Formación del Plan de Mejoras.

1. Relación con la Organización. Comprende un análisis inicial que tiene que ver con la organización global de la empresa y también comprende el estudio sobre la estructura organizativa a nivel jerárquico y formal del departamento de sistemas de información. Posteriormente se procede a conocer con más profundidad o detalle la estructura organizativa de la empresa a través de los denominados papeles de trabajo que comprenden las entrevistas y cuestionarios que se formulan para la comprensión de la organización.

En esta fase se aplican las siguientes normas de auditoría de sistemas de información, la norma 010:Título de Auditoría, la norma 020:Independencia y la norma 030:Ética y Normas Profesionales. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas de información es resaltar la independencia y ética profesional del auditor con respecto a la organización.

2. Planificación de la Operación. Comprende el detalle de los aspectos relevantes que van a ser considerados en la realización de la auditoría, por ejemplo: áreas que cubrirá el estudio (alcance de la

auditoría), objetivos esperados de la auditoría, forma en que se llevará a cabo la auditoría (logística), personas que colaborarán en el desarrollo de la auditoría, documentación a reunir o solicitar (estadísticas, manuales de procedimientos, reportes, evidencias, etc.) y en que no intervendrán la auditoría.

En esta fase se aplican las siguientes normas de auditoría de sistemas de información, la norma 040:Idoneidad, la norma 050:Planificación. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas de información es resaltar la habilidad y capacidad (técnica y administrativa) del auditor para planear y conducir la auditoría.

3. Desarrollo de la Auditoría. Comprende la ejecución y evaluación de los puntos contemplados en el paso anterior y los temas específicamente analizados de esta fase serán:

- El entorno informático (interno y externo) del sistema de información.

- Los aspectos referidos al grado de utilización y satisfacción de los diferentes usuarios que manejan las aplicaciones.

En esta fase se aplica la siguiente norma de auditoría de sistemas de información, la norma 060:Ejecución del Trabajo de Auditoría. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas de información es garantizar el cumplimiento de los objetivos de la auditoría con base a la planeación realizada y a través de evidencias confiables y suficientes.

4. Síntesis y Diagnóstico. Como su nombre indica se procede a analizar e interpretar la información obtenida en las fases anteriores. En esta etapa se pretende poner en evidencia los puntos débiles y fuertes del sistema de información, los riesgos eventuales, las mejoras y las soluciones posibles a alcanzar (análisis costo-beneficio).

En esta fase se aplica la siguiente norma de auditoría de sistemas de información, la norma 070:Informes. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas de información es resaltar el alcance y el objetivo de la auditoría contra los hallazgos encontrados.

5. Presentación de Conclusiones. Debe efectuarse mediante hechos constatados, esto es; las conclusiones deben estar

argumentadas, probadas y documentadas evitando su posible refutación. Proposiciones realistas y constructivas. Análisis costo-beneficio.

En esta fase se aplica la siguiente norma de auditoría de sistemas de información, la norma 070: Informes. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas de información es resaltar las conclusiones y las recomendaciones del auditor con respecto a los hallazgos encontrados.

6. Redacción de Informe y Formación del Plan de Mejoras. En este sentido el informe final de auditoría constituye el documento que expresa el juicio emitido por el auditor y la única referencia oficial. El informe de auditoría debe estar estructurado de la siguiente forma:

- Carta de Presentación: Se debe presentar un resumen-conclusión del trabajo de auditoría.

- Introducción al Informe: Se deben exponer los objetivos evaluados, las condiciones en que se desarrolló la auditoría y un resumen de las observaciones y recomendaciones.

- Principales Observaciones y Recomendaciones: Se debe reflejar el detalle de las observaciones realizadas y las deficiencias constatadas de acuerdo con los siguientes criterios: descripción exacta, convincente y no repetitiva de las deficiencias. Consecuencias y repercusiones predecibles y breve recomendación del auditor.

- Plan de Acción-Mejoras: El plan de mejoras normalmente se puede contemplar en 3 plazos: A corto plazo con mejoras que supongan pequeña inversión en tiempo y dinero; a medio plazo con implantación de aplicaciones que exigen una mayor inversión en tiempo y dinero; a largo plazo con consideraciones que afectan a políticas o reorganizaciones estructurales de la empresa.

En esta fase se aplican las siguientes normas de auditoría de sistemas de información, la norma 070: Informes, la norma 080: Actividades de Seguimiento. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas de información es resaltar el informe final completo del resultado de la auditoría y los planes de acción a seguir para corregir las desviaciones detectadas, así

como el seguimiento a los planes de acción para asegurar el cierre de las desviaciones.

CAPÍTULO VI

Caso Práctico

Partiendo del hecho de que la Auditoría de Sistemas de Información es el proceso sistemático de obtención objetiva y evaluación de evidencias relativas a las declaraciones realizadas sobre sistemas informáticos y eventos (situaciones no habituales), para averiguar el grado de correspondencia entre las declaraciones y los criterios establecidos y comunicar los resultados a las personas interesadas.

El presente Caso Práctico habla de una empresa internacional del sector informático que por políticas de seguridad establecidas por la misma organización no es posible divulgar su razón social. Con base a las políticas de seguridad informática establecidas por el área de seguridad de la organización, tiene definido por procedimiento la revisión de su infraestructura tecnológica interna de manera periódica (en este caso es anual), por tal razón el presente Caso Práctico hace referencia a esta revisión anual hecha a la empresa por auditores externos a la organización.

El alcance de esta revisión anual - auditoría interna - del Caso Práctico esta enfocada al cumplimiento de la definición de la Auditoría de Sistemas de Información y de las políticas de seguridad en los sistemas de información definidas originalmente por la empresa a través de su área de seguridad informática. Cabe mencionar que la empresa definió su política de seguridad con base en los estándares internacionales de seguridad indicados en el Capítulo IV y en el Apéndice I de la presente tesis.

El tipo de Auditoría que se llevó a cabo en el presente Caso Práctico fue una Auditoría Informática de Sistemas de Información (como se indica en el Capítulo V punto 5.3.3.2 de la presente tesis), la cual se ocupa de analizar la actividad que se conoce como técnica de sistemas, en todos sus factores, es decir; determina si un sistema de información salvaguarda sus activos, mantiene la integridad de sus datos, cumple con las normas de seguridad fijadas por la organización y la utilización de sus recursos es la adecuada.

El Desarrollo de la Auditoría Interna a los Sistemas de Información se dividió en las siguientes fases (como se indica en el Capítulo V punto 5.3.4 de la presente tesis):

1. Relación con la Organización.

2. Planificación de la Operación.

3. Desarrollo de la Auditoría.

4. Síntesis y Diagnóstico.

5. Presentación de Conclusiones.

6. Redacción de Informe y Formación del Plan de Mejoras.

A continuación se presenta el contenido del reporte final por parte de los auditores en donde se indican los hallazgos encontrados y las recomendaciones hechas a las revisiones de los sistemas de información. El reporte final en su formato original como fue entregado a los auditores se presenta en el Apéndice III Reporte Final del Caso Práctico.

Objetivo de la Revisión Anual – Auditoría Interna -

- Confirmar el cumplimiento de los requerimientos de los Estándares Corporativos de la ITCS104.
- Identificar deficiencia en los Procesos.
- Recomendar soluciones.
- Asegurar que el análisis de la causa raíz de las desviaciones es hecha, investigada y determinada.
- Implantar las mejoras definidas.

Alcance de la Revisión Anual – Auditoría Interna -

- Revisión de la aplicación de los Estándares de Seguridad en los Sistemas de Información Distribuidos.
- Aplicación del Programa de Auditoría Corporativo 42-00-00.
- Revisión de la Revalidación Anual de la necesidad de la continuidad en el negocio.
- Revisión Trimestral de Empleados.
- Revisión del Proceso de Administración de Usuarios y su mejora.
- Revisión del Proceso de Detección de Ataques Sistemáticos y su mejora.

Descripción de las Actividades Realizadas a los Sistemas de Información Distribuidos

6.1 Identificación

El objetivo de la auditoría en cuanto a este elemento de seguridad – Identificación - es verificar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

6.1.1 Identificación

- Hay userids que están siendo compartidos.
  - 159 de 278 userids en el Servidor 1 están siendo compartidos.

6.1.2 Verificación de Empleados

- Cumplido (en el alcance revisado).

6.1.3 Registro

- Fueron detectadas divergencias entre los registros del MAD (Master Address Directory – Directorio Maestro de Direcciones) y del CEP (Computing Environment Physical – Ambiente Físico del Equipo).
- Los servidores listados a continuación son clasificados como Departamentales y de Desarrollo de Sistemas conforme la ITCS104 y se están aplicando controles de seguridad de Sistemas de Producción de una Unidad de Negocio.
  - Servidor 2.
  - Servidor 3.
  - Servidor 4.
  - Servidor 5.

6.2 Autenticación

El objetivo de la auditoría en cuanto a este elemento de seguridad – Autenticación - es verificar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

- Cumplido (en el alcance revisado).

6.3 Autorización

El objetivo de la auditoría en cuanto a este elemento de seguridad – Autorización - es verificar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

6.3.1 Autorización de Acceso

- El dueño del sistema de aplicación no es informado cuando un nuevo userid es creado y el acceso es a través del sistema operativo.
- Los Gerentes de los Usuarios no confirman la baja de sus empleados.
- La revalidación anual del proceso de la necesidad de la continuidad en el negocio puede ser mejorado.
    - El concepto de confirmación afirmativa esta siendo mal aplicado.
    - Si el Gerente no contesta hasta el último día el userid es revalidado, sin embargo éste debe ser cancelado.

6.3.2 Acceso Remoto para Empleados

- Cumplido (en el alcance revisado).

6.3.3 Notificar el Uso del Negocio

- Cumplido (en el alcance revisado).

6.3.4 Recursos de Usuario

- Cumplido (en el alcance revisado).

6.4 Protección de la Información y Confidencialidad

El objetivo de la auditoría en cuanto a este elemento de seguridad – Protección de la Información y Confidencialidad - es verificar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

6.4.1 Protección de la Información

- Cumplido (en el alcance revisado).

6.4.2 Información Residual

- Cumplido (en el alcance revisado).

6.4.3 Encriptación

- Cumplido (en el alcance revisado).

6.5 Integridad y Disponibilidad del Servicio

El objetivo de la auditoría en cuanto a este elemento de seguridad – Integridad y Disponibilidad del Servicio - es verificar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

6.5.1 Administración de los Recursos del Sistema Operativo

- Cumplido (en el alcance revisado).

6.5.2 Autoridad para la Administración del Sistema y la Seguridad

- Debe ser implantado un proceso para cambiar todos los passwords cuando el administrador del sistema deja de serlo.

6.5.3 Código Dañoso

- Cumplido (en el alcance revisado).

6.5.4 Vulnerabilidades

- Cumplido (en el alcance revisado).

6.5.5 Administración de los Parches de Seguridad

- Cuando un APAR (parche) no es aplicado en el sistema de información en el tiempo requerido, esto no es informado al dueño del proceso de negocio, solo es informado el retraso, más no el riesgo que esto representa para el sistema de información.

6.5.6 Modificación al Software

- Cumplido (en el alcance revisado).

6.5.7 Administración de la Disponibilidad del Servicio

- Negar el Servicio.
    - Cumplido (en el alcance revisado).
- Ataques Sistemáticos de Login.
    - La definición actual de ataque sistemático debe ser mejorada.

- Solo los intentos de login inválido son analizados y controlados.
- No hay una clara definición para analizar los intentos de login inválido relativo a:
  - Ambientes de red.
  - Ambientes de site.
  - Los ataques sistemáticos de login no son detectados y reportados inmediatamente.
- Definir un umbral adecuado para los intentos de acceso no autorizados.

- Activación de los Servicios y del Servidor.

  - El proceso de migración/actualización del sistema operativo de un servidor no esta definido/documentado.
    - El Servidor 6 tiene un CIRATS (reporte levantado en un sistema de seguimiento) de evidencia de búsqueda de vulnerabilidades, verificación de la salud del servidor y un registro cambiado.
    - El Servidor 7 no tiene un CIRATS (reporte levantado en un sistema de seguimiento) de evidencia de búsqueda de vulnerabilidades, verificación de la salud del servidor y un registro cambiado.

- Servicios de Cliente y Servidor.

  - El Servidor 8 permite el acceso a Internet sin restricción.

6.6 Auditoría Activa

El objetivo de la auditoría en cuanto a este elemento de seguridad – Auditoría Activa - es verificar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

- Cumplido (en el alcance revisado).

6.7 Verificación

El objetivo de la auditoría en cuanto a este elemento de seguridad – Verificación - es revisar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

6.7.1 Verificación de Salud

- El formato de Verificación de Salud del servidor para el AS/400 no cubre todos los puntos o requerimientos especificados en la política de seguridad.

6.7.2 Probando la Seguridad Técnica

- Cumplido (en el alcance revisado).
- Son ejecutados desde Brasil por el Auditor 5.

6.7.3 Revisión del Proceso de Seguridad

- Corresponde a esta revisión.

6.8 Incidentes de Seguridad

El objetivo de la auditoría en cuanto a este elemento de seguridad – Reporte de Incidentes de Seguridad y su Manejo - es verificar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

6.8.1 Reportar los Incidentes de Seguridad

- Revisar este Proceso con base en el Proceso de Ataques Sistemáticos.

6.8.2 Reportar Accesos no Autorizados

- Ningún análisis exhaustivo es hecho cuando son detectados accesos inválidos.

6.8.3 Reportar el abuso de Autoridad

- Cumplido (en el alcance revisado).

6.9 Controles de Acceso a Medios Magnéticos

El objetivo de la auditoría en cuanto a este elemento de seguridad – Controles de Acceso a Medios Magnéticos - es verificar el cumplimiento de la política de seguridad definida por la empresa en este elemento de seguridad.

A continuación se indican los puntos de cumplimiento revisados durante la auditoría para este elemento de seguridad, así como los comentarios y/o recomendaciones hechas por los auditores.

6.9.1 Protección Física de los Medios de Almacenamiento

- Cumplido (en el alcance revisado).

6.9.2 Control de Inventario de los Medios de Almacenamiento

- Cumplido (en el alcance revisado).

CONCLUSIONES

El objetivo del presente trabajo planteado originalmente fue: "Identificar los factores que ayuden a conseguir un nivel de Seguridad aceptable en los Sistemas de Información", entendiendo por "aceptable" un nivel de protección suficiente para que la mayoría de los intrusos potenciales interesados en los equipos de una organización fracase ante un ataque contra los mismos.

Con base en este objetivo que se estudió, analizó y desarrollo en el presente trabajo, concluimos que es muy difícil de conseguir que la Seguridad en los Sistemas de Información sea infalible, por lo que se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad, por lo tanto, se habla de sistemas fiables en lugar de sistemas seguros.

En el presente trabajo se analizaron los ambientes operativos (interno y externo) y los diferentes aspectos a los que un Sistema de Información se puede ver involucrado y/o afectado y concluimos que es imposible garantizar una plena seguridad ante cualquier atacante. Este hecho, aunque preocupante, es casi inevitable; lo evitable es que cualquier persona sea capaz de atacar con éxito un equipo simplemente por haber visto una película, descargando un par de páginas web y ejecutando un programa que ni ha hecho ni entiende.

Conseguir romper la seguridad de un sistema de forma no autorizada es, en la mayoría de los casos, un símbolo de inmadurez, y por supuesto ni denota inteligencia ni unos excesivos conocimientos. Es más productivo dedicar la inteligencia y conocimientos a tareas que ayuden a incrementar la seguridad, como la construcción de sistemas de autenticación fiables y económicos o el diseño de nuevos criptosistemas seguros. Eso es seguridad informática y no lo que habitualmente se nos quiere hacer creer: la seguridad informática no consiste en conocerse todos los bugs (fallas) de un sistema operativo, con sus correspondientes desviaciones ni en jugar a hackers (piratas informáticos). Lamentablemente, este es el panorama de la seguridad informática en nuestro país en la actualidad; esperemos que algún día cambie.

A pesar del elevado nivel de seguridad que pueda tener un Sistema de Información, basta con visualizar física o virtualmente el entorno (interno y externo) en el que se desarrolla y podría comprobarse que su seguridad es en la mayor parte de los casos pobre, cuando no inexistente. El problema no radica en el Sistema de Información, sino en las personas que están detrás de éste que generalmente son administradores y usuarios de cualquier tipo. Un

Sistema de Información dependiendo del tipo de plataforma (sistema operativo) ofrece los mecanismos suficientes como para conseguir un nivel de seguridad más que aceptable, pero somos nosotros los que en muchos casos no sabemos activarlos, utilizarlos y aprovecharlos o simplemente no estamos concientes de que existen. Para solucionar el problema, como ya hemos comentado a lo largo del presente trabajo, existen dos soluciones que todos deberíamos intentar aplicar: en primer lugar la concienciación de los problemas que nos pueden acarrear las fallas en la seguridad (a muchos aún les parece que el tema no va con ellos, que los piratas informáticos sólo existen en el cine y que en su máquina nada malo puede ocurrir). Tras la concienciación, la segunda solución indica que es necesaria una formación adecuada para cada tipo de persona (evidentemente no podemos exigir los mismos conocimientos a un administrador responsable de varios sistemas de información que a un usuario que sólo se conecta al sistema para realizar una transacción). No es necesario convertirse en un experto, simplemente hay que leer un poco, capacitarse y conocer las normas básicas de seguridad informática. Con estos pasos seguramente no pararemos a todos los piratas que nos intenten atacar, pero sí a la gran mayoría de ellos, que es lo que realmente interesa en el mundo de la seguridad informática.

Aparte del lógico incremento en el nivel de seguridad que se conseguiría mediante una mínima concienciación y formación de los administradores, gerentes de seguridad, usuarios, etc., existe el peligro que estas dos medidas difícilmente nos van a permitir superar la simpatía que socialmente despiertan muchos piratas informáticos; por desgracia, mucha gente aún considera a estos personajes son una especie de héroes. Si nadie aplaude al que roba un bolso en la calle, ¿Por qué aún existen defensores de los que roban contraseñas o información de un sistema? Mientras sigamos sin darnos cuenta de lo que realmente son los piratas (simplemente delincuentes) será difícil que la seguridad informática sea tomada en serio.

No nos gustaría terminar este trabajo sin una pequeña reflexión sobre el panorama de la seguridad informática en nuestro país, sólo cabe una definición: lamentable. Lo único que por suerte se toma un poco en serio es la criptografía, que cuenta con grupos de estudio y docencia en algunas universidades del país. Del resto, casi es mejor no hablar: no existe ningún grupo importante de investigación en ninguna universidad, el número de artículos publicados en revistas serias se reduce a cero y la docencia universitaria a unas pocas asignaturas genéricas - y que ni siquiera son obligatorias en algunos casos -.

De esta forma, si la mayor parte de los informáticos salen de las facultades sin conocer conceptos tan básicos como sniffer (analizador de protocolo) o caballo de troya (ya no hablamos de cosas como esteganografía o seguridad multinivel), no es de extrañar que la seguridad se encuentre actualmente - en la mayor parte de los casos - en manos de aficionados a la informática con ciertos conocimientos prácticos pero con una importante falta de bases teóricas sobre la materia. Si lo que queremos son sistemas inseguros y reportajes sensacionalistas sobre quinceañeros que violan la seguridad de los sistemas de información de grandes corporativos, lo estamos consiguiendo, pero quizás deberíamos plantearnos qué ha de pasar para que esto cambie.

Finalmente consideramos importante resaltar bajo este contexto, que los planes de estudio de la carrera de Ingeniero en Computación de la Facultad de Ingeniería de la UNAM, se han actualizado e inclusive incorporado nuevas materias relacionadas con el tema de la Seguridad en los Sistemas de Información. Ojalá que éstos sean los principios de la creación de grupos docentes serios y especializados en el ramo y que con ello se creen instituciones y/o empresas dedicadas a la Seguridad en los Sistemas de Información en nuestro país.

FIGURAS

TABLAS

APÉNDICE I

Apartado de Seguridad Interna en Sistemas de Información

I. Especificaciones Técnicas de Sistemas Operativos

1.1 Sistema Operativo AIX

Aplicable a la versión 4.3.3 – 5.0.

1.1.1 Elemento de Seguridad Interna – Identificación -

1.1.1.1 Userids

System Value/Parameter	Description	Required Setting
UID	Applies to all UIDs	Each UID must only be used once

1.1.2 Elemento de Seguridad Interna – Autenticación -

1.1.2.1 Reusable Passwords

System Value/ Parameter	Description	Required Setting
maxage	Maximum password age	26
maxrepeats	Number of repeating consecutive characters	2
minage	Minimum password age	0
minalpha	Minimum number of alphabetic characters	1
mindiff	Number of characters not found in last password	1
minother	Number of non-alphabetic characters	1
minlen	Minimum password length	6
histsize	Number of previous password that can not be used	4
flag=NOCHECK	option in /etc/security/passwd	not permitted on any userid with passwords

Exemptions to passwords rules

Option A: Userids with the following attributes set are allowed to have non expiring passwords:

/etc/security/user	Direct login	login = false
/etc/security/user	Remote login	rlogin = false
/etc/ftpusers	Restrict FTP access	Id must exist in file

Option B: Userids using native AIX authentication with the following attributes set are allowed to have non expiring passwords:

/etc/passwd	User Information	"*" specified in the password (2nd) field of the userid

1.1.2.2 Authentication

Not Aplicable.

1.1.3 Elemento de Seguridad Interna – Autorización -

1.1.3.1 Business Use Notice

Required	How implemented
Yes	Use /etc/motd
Yes	Common Desktop Environment must use dthello program to display Business Use Notice

1.1.3.2 User Resources

System Value/Parameter	Description	Required Setting
$HOME	User default home directory	x00
or System Default UMASK	User file creation default protection	x77

1.1.4 Elemento de Seguridad Interna – Protección de la Información y Confidencialidad -

Protection of password files		
/etc/password	Contains userid, uid, gid, and misc	Must not contain passwords

1.1.4.1 Encryption

Required	How implemented
Yes	Crypt()

1.1.5 Elemento de Seguridad Interna – Integridad y Disponibilidad del Servicio -

1.1.5.1 Operating System Resources

AIX OSRs are in the following directories and all subdirectories and **files under them**

System Value/Parameter	Description	Required Setting
/etc /bin /usr/sbin /usr/bin /usr/etc	OSRs	
executable *.a *.o *.so *.cf *.conf *.cfg	OSR File Types	Must be owned by one of the following userids and groupids Settings for other must be r-x or more stringent
/etc/locks	OSR directory	May contain world-writeable file
/etc/security/	OSR directory	Must have permission mode xx0
/tmp	Temporary space	(t) Sticky bit must be set
/etc/snmpd.conf	snmp configuration file	Must be 640 or more restrictive

Exception to OSRs (exempt from OSR requirements)

Files of the following types may be world writeable: • socket (s) • named pipe (p) • block special file (b) • character special file (c)	Special/device and socket files
symbolic links (l)	

The following systems ids and group ids must use the following UIDs and GIDs

Userids	Groupids
root:0	system:0
daemon:1	security:7
bin:2	bin:2
sys:3	sys:3
adm:4	adm:4
uucp:5	uucp:5
nuucp:6	mail:6
lpd:9	printq:9
imnadm (no assigned UID)	cron:8
ipsec (no assigned UID)	audit:10
ldap (no assigned UID)	shutdown:21
lp (no assigned UID)	ecs:28
snapp (no assigned UID)	imnadm (no assigned GID)
	ipsec (no assigned GID)
	ldap (no assigned GID)
	lp (no assigned GID)
	haemm (no assigned GID)
	snapp (no assigned GID)

1.1.5.2 Security & System Administrative Authority

System Value/Parameter	Description	Required Setting
Password must be assigned		
Login access to account must be restricted to the physical console, or to a method that provides accountability to an individual.		
ROOT	Super Userid	Direct login via FTP is allowed
Identify and Authenticate Users (2.1)		The "ROOT" userid is permitted to be shared as long as individual accountability is maintained.
System default for admin flag in /etc/security/user	Defines the administrative status of users	false

1.1.5.3 Harmful Code Detection

Not applicable

1.1.5.4 Systematic Logon Attacks

System Value/Parameter	Description	Required Setting
loginretries	Number of invalid attempts before ID is locked	5

1.1.6 Elemento de Seguridad Interna – Auditoría Activa

System Value/Parameter	Description	Required Setting
/usr/adm/wtmp	System access log	Must exist
/usr/adm/sulog	System access log	Must exist
/etc/security/failedlogin	System access log	Must exist

1.1.7 Elemento de Seguridad Interna – Verificación

1.1.7.1 Health Checking

Requirement	Description
Confirm that mandatory access control system options are as specified	Validate settings under 2.1, 3.1, 3.2, and 5.2
Validate that only approved users hold security administrative and system authority	Verify that only one uid of 0 exists
Expand the contents of the system group	Verify members of that group
Check that all OSR access controls are set	
Verify that only approved users are included in the access lists of OSRs beyond that allowed to general users.	Verify ownership of OSRs to users listed in 5.1
Ensure Harmful code detection programs are installed and operational	Does not apply to AIX at this time
Check that the required access and activity logs data do exist. (list logs to be verified)	Check logs under 6.1

1.1.8 Elemento de Seguridad Interna – Red

System Settings	Required Setting
Anonymous FTP System Settings AIX (with POSIX compliant ftp account home directory)	
ftpd daemon options	If any directories will be made writable, the -u option must be used.
Configuration of the ftp account home directory	Must be owned by root and grant write access only to the owner.
Configuration of bin subdirectory of the ftp account home directory.	Must be owned by root and grant write access only to the owner. Files contained in this directory must have mode 0111.
Configuration of lib subdirectory of the ftp account home directory.	Must be owned by root and grant write access only to the owner. Files contained in this directory must have a mode of 0555.
Configuration of etc subdirectory of the ftp account home directory.	Must be owned by root and grant write access only to the owner. If the directory contains a passwd file, the password fields must be empty.
Configuration of other subdirectories of the ftp account home directory	May not be owned by a general user account. The mode of the directory must be 0755.
Permission's of files and other directories descended from the ftp account home directory.	Files must allow only read access except to the user owner and group owner of the file. If write access is granted to the group owner of the file, membership in the group is a security administrative authority. Directories must allow only read access, only write and execute access, or no access; except to user owner and group owner of the directory. If any additional access permission is granted to the group owner of the directory, membership in the group is a security administrative authority.
AIX (with AFS based ftp account home directory)	
ftpd daemon options	If any directories will be made writable, the -u option must be used.
Configuration of the ftp account home directory	Must be owned by root and grant write access only to the owner.
Configuration of bin subdirectory of the ftp account home directory.	Must be owned by root and grant write access only to the owner. Files contained in this directory must have mode 0555.
Configuration of lib subdirectory of the ftp account home directory.	Must be owned by root and grant write access only to the owner. Files contained in this directory must have a mode of 0555.
Configuration of etc subdirectory of the ftp account home directory.	Must be owned by root and grant write access only to the owner. If the directory contains a passwd file, the password fields must be empty.
Configuration of other subdirectories of the ftp account home directory	May not be owned by a general user account. The ACL of a read-only directory must grant no more than rl permission to the system:anyuser and system:authuser entries. The ACL of a writable directory must grant no more than liw permission to the system:anyuser and system:authuser entries.
Trivial File Transfer Protocol (TFTP) System Setting	
tftp access control	The /etc/tftpaccess.ctl must exist when TFTP is active.
/etc/tftpaccess.ctl file	Must contain only **allow** statements.
Network File System (NFS) System Settings	
/etc/exports	The file must exist when NFS is active.

Berkeley Remote Access Commands System Settings	
/etc/hosts.equiv file	May not be used as an access control mechanism
.rhosts files	File permission's may only grant access to the owner of the file.
Remote Execution Daemon (rexd) System Settings	
rexd daemon	Must be disabled.
Line Printer Daemon (lpd) System Settings	
bsh queue	If supported, must be disabled or deleted.
.netrc files System Settings	
.netrc files	File permission's must grant access only to the owner of the file.
Post Office Protocol (POP) System Settings	
POP user authentication	POP daemons must be configured to require users to authenticate. POP daemons that do not support authentication must be disabled.
Net News Transfer Protocol (NNTP) System Settings	
NNTP authentication and identification	Must be configured to require authentication and identification of all users if any of the newsgroups on the server are classified IBM confidential.
IFOR/LS System Settings	
/var/ifor/i4ls.ini	DisableRemoteAdmin = yes DisableRemoteNdlAdmin = yes If service is active
X-Window System Settings	
X-server access control	Must not be disabled.
Denial of Service Prevention System Settings	
Must be disabled if not required to support an application	ECHO, CHARGEN, RSTAT, TFTP, RWALL, RUSER, DISCARD, DAYTIME, BOOTPS, FINGER, SPRAYD, PCNFSD, NETSTAT, REXD, WHO
Must be disabled on all Internet servers	ECHO, CHARGEN, FINGER, DISCARD, SYSTAT, DAYTIME, NETSTAT, WHO, SYSTAT
SNMP Service	Community names of 'public' and 'private" are not permitted if SNMP service is active
Network Information Services (NIS) System Settings (including NIS+ in NIS compatibility mode)	
yppasswd daemon	Must be disabled.
Anonymous FTP System Controls	
Access permission's for directories accessible via Anonymous FTP	Each directory may allow read access or write access to anonymous users, but not both.
Protecting Resources	
/.rhosts	Read access only by root, write access only by root
/.netrc	Read access only by root, write access only by root
/var/ifor/i4ls.ini	No write access by general users
Anonymous FTP	
Directories enabled for anonymous FTP access.	Access via anonymous FTP may be granted only to directories containing unclassified data, where the storage of IBM confidential data is prohibited. This restriction also applies to any subdirectories of the directory.
Trivial File Transfer Protocol (TFTP)	
Directories enabled for tftp access.	Access via TFTP may be granted only to directories containing unclassified data, where the storage of IBM confidential data is prohibited. This restriction also applies to any subdirectories

	of the directory.
Network File System (NFS)	
/etc/exports	Directories that are permitted to contain IBM confidential data may not be exported unless the -secure option is used, or the requirements specified in section E.3.2 are met.
Network Information Services (NIS) (including NIS+ in NIS compatibility mode)	
NIS maps	Must not be used to store IBM Confidential data, including user passwords or other authentication credentials in any form. If the NIS passwd maps are used, all encrypted user passwords must be removed from the source file before the maps are generated.
Network Information Services Plus (NIS+)	
NIS+ maps	If IBM Confidential data, including user passwords or other authentication credentials in any form, access may not be granted to the other or unauthenticated permission classes.
Encryption	
No standard TCP/IP application protocols have specifications for data encryption. Encryption of session data is not required when standard TCP/IP applications that do not include encryption features are used. If TCP/IP application protocols are transported via an encrypted session via technology such as SSH, the encryption used for the encrypted session must meet the requirements of section 1.4.3 of this document.	

1.2 Sistema Operativo Linux

Aplicable a las siguientes versiones:

RedHat Release 7.2
RedHat Release 7.3
RedHat Release 8.x
RedHat Release 9.x
SuSE Release 7.3
SuSE Ver 8.x
Turbo Linux Ver 7.0 Server
Caldera eServer V2.3
Debian

1.2.1 Elemento de Seguridad Interna – Identificación -

1.2.1.1 Userids

System Value/Parameter	Description	Required Setting
UID	Applies to all uid's	Each uid must only be used once

1.2.2 Elemento de Seguridad Interna – Autenticación -

1.2.2.1 Reusable Passwords

System	Description	Required Setting
Value/Parameter		
PASS_MAX_DAYS	Maximum password age	<=186 in /etc/login.defs
PASS_MIN_LEN Note: Appears to be hardcoded in Caldera 2.3	Minimum password length	=>6 in /etc/login.defs
Root	Super User ID	Login access to account must be restricted to the physical console, or to a method that provides accountability to an individual.
RedHat 7.1 and newer, Turbo Linux, and SuSE systems support the **remember** parameter to the pam_unix.so module note: May require **touch /etc/security/opasswd** if this file does not already exist. This file, if it exists, must have 0700 permissions.	Prevent reuse of last four passwords.	password required /lib/security/pam_unix.so remember=4 use_authtok md5 shadow OR password sufficient /lib/security/pam_unix.so remember=4 use_authtok md5 shadow Note: If /etc/pam.d/system-auth exists, this is the control file. Otherwise, it must appear in /etc/pam.d/passwd and /etc/pam.d/login. Note: If the IBM-security-compliance.x.x-x.noarch.rpm is installed on RedHat or SuSE systems, /etc/pam.d/local-auth replaces the use of /etc/pam.d/system-auth mentioned above. Note: For SuSe 7 and later systems, one of the following must be used: **password required /lib/security/pam_unix2.so shadow md5** and **password required /lib/security/pam_pwcheck.so remember=4** or **password required /lib/security/pam_unix_passwd.so remember=4 use_authtok md5 shadow** Note: On s390 SuSE SLES 7, the **remember** parameter is not supported. Note: On s390 SuSE SLES 7 and SLES 8 the **shadow** parameter is not supported.

1.2.2.2 Authentication Tickets / Tokens

Not applicable.

1.2.3 Elemento de Seguridad Interna – Autorización -

1.2.3.1 Business Use Notice

Required	How implemented
Yes	/etc/motd

1.2.3.2 User Resources

System Value/Parameter	Description	Required Setting
/home/<userid>	User's home directory	Default Permissions: 700. Must be owned by userid

1.2.4 Elemento de Seguridad Interna – Protección de la Información y Confidencialidad -

System Value/ Parameter	Description	Required Setting
/etc/passwd	Protection of password files: Contains userid, uid, gid, and misc	Must not contain passwords
Anonymous FTP, Process for Receiving Files form Anonymous Users	Files that have been stored into a writeable directory must be examined (checked for IBM Confidential information, checked for inappropriate materials, etc) before being moved to a readable directory.	
Network File System (NFS), Process for Exporting IBM Confidential Data Without Strong Authentication	Access to data classified IBM Confidential may be granted though NFS on an exception basis under the following conditions: • The -hosts option is specified in /etc/exports for all directories that may contain IBM Confidential files • A process is established to validate all hosts specified in -hosts options in /etc/exports, at the health checking interval, for all directories that may contain IBM Confidential files. If access to directories that may contain IBM Confidential files is provided to netgroups, the host in the netgroups must be validated at least quarterly. • A process is established to ensure that all hosts specified in -hosts options in /etc/exports, for all directories that may contain IBM Confidential files, share common userids and uid numbers and group and gid number mapping.	

1.2.4.1 Encryption

System Value/ Parameter	Description	Required Setting
Passwords in /etc/shadow	Passwords must be protected with 128-bit encryption	Default setting with use of **md5 shadow** parameters to pam_unix.so in the password stanza as set in /etc/pam.d/passwd or /etc/pam.d/system-auth is sufficient. Note: Any file in /etc/pam.d containing "password required" or "password sufficient" must carry the **md5 shadow** options. **Note:** If the IBM-security-compliance.x.x-x.noarch.rpm is installed on RedHat or SuSE systems, /etc/pam.d/local-auth replaces the use of /etc/pam.d/system-auth mentioned above. Note: On SuSE 8 and later use pam_unix2.or pam_unix_passwd.so Note: The **shadow** parameter is not supported on s390 SuSE SLES 7 and SLES 8.

1.2.5 Elemento de Seguridad Interna – Integridad y Disponibilidad del Servicio -

1.2.5.1 Operating System Resources

System Value/ Parameter	Required Setting
/root/.rhosts	Read access only by root; write access only by root
/root/.netrc	Read access only by root; write access only by root
/	Settings for other on this directory must be r-x or more stringent.
/usr	Settings for other on this directory must be r-x or more stringent.
/var	Settings for other on this directory must be r-x or more stringent.
/tmp	Settings for this directory must be rwxrwxrwt(1777).
/var/tmp	Settings for this directory must be rwxrwxrwt(1777).

1.2.5.2 Security & System Administrative Authority

System Value/ Parameter	Description	Required Setting
ROOT	Super Userid	Password must be assigned
		Login access to account must be restricted to the physical console, or to a method that provides accountability to an individual.
/etc/pam.d/other	Enforce a default no access policy	auth required /lib/security/pam_deny.so account required /lib/security/pam_deny.so

1.2.5.3 Harmful Code Detection

Not applicable

1.2.5.4 Systematic Logon Attacks

System Value/Parameter	Description	Required Setting
RedHat 7.x, Turbo Linux, SuSE and Caldera systems support the pam_tally.so module notes: Must precede any lines of same module-type with a control-flag of **sufficient** May require **touch /var/log/faillog** if this file does not already exist If an account is locked when the deny count is reached, it may be reset by the root account with **faillog -u <userid> -r**	Limit consecutive invalid login attempts to 5.	auth required /lib/security/pam_tally.so onerr=fail no_magic_root account required /lib/security/pam_tally.so deny=5 reset no_magic_root Note: If /etc/pam.d/system-auth exists, this is the control file. Otherwise, it must appear in all /etc/pam.d control files which require login authentication.

1.2.6 Elemento de Seguridad Interna – Auditoría Activa

1.2.6.1 Systematic Access Logging

System Value/Parameter	Required Setting
Login success or failure	The following requirements cover RedHat, SuSE, Caldera and Turbo Linux. File:/etc/syslog.conf *.info;mail.none;authpriv.none;cron.none /var/log/messages authpriv.* /var/log/secure Note: Log file permission must not have write for other and must not have write permission for group unless the associated group is used only by set-GID operating system programs to avoid a need for root only update privileges. The following requirements cover Debian Linux: auth,authpriv.* /var/log/auth.log *.*;auth,authpriv.none\ -/var/log/syslog
	.=info;.=notice;*.=warning;\ auth,authpriv.none;\ cron,daemon.none;\ mail,news.none -/var/log/messages
/var/log/wtmp	Must exist
/var/log/messages	Must exist
/var/log/faillog	Must exist
/var/log/secure or /var/log/auth.log	Must exist Note: /var/log/secure is required on all Linux distributions except Debian Note: /var/log/auth.log is required on Debian Linux

1.2.7 Elemento de Seguridad Interna – Verificación

1.2.7.1 Health Checking

Requirement	Description
Confirm that mandatory access control system options are as specified	Validate: Password minimum length and maximum lifetime in 2.1 Reusable Passwords
Confirm that encrypted passwords are properly protected.	Validate: • /etc/passwd does not contain encrypted passwords in the second field • /etc/shadow exists and has permission bits set to 0600, or 640 where the associated group is used only by set-GID operating system programs to avoid a need for root only access privileges.
Where supported, confirm that password reuse and invalid login attempts are controlled and logged	On recent RedHat systems, this is all managed in **/etc/pam.d/system-auth** where the **pam_stack.so** module exists. On older RedHat and SuSE systems, this is managed in the /etc/pam.d directory in the files **login, rlogin, and ftp**
Validate that only approved users hold security administrative and system authority	Root and any userids that are members of groups which have gid's less than 99.
Check that all OSR access controls are set	Validate settings in section 5.1 Operating System Resources.
Check that the required access and activity logs data do exist and are retained for 60 days. This may be accomplished by configuring syslog to send log records to a remote ITCS104 compliant server.	Check logs: /var/log/secure or /var/log/auth.log /var/log/messages /var/log/wtmp

1.2.8 Elemento de Seguridad Interna – Red

System Settings	Required Setting
Anonymous FTP System Settings	
ftpd daemon options	If any directories will be made writable, the **-u 027** option must be used. Note: this is a wu-ftpd specific requirement
Configuration of the ftp account home directory	Must be owned by root and grant write access only to the owner

Configuration of the bin subdirectory of the ftp account home directory	Must be owned by root and grant write access only to the owner. Files contained in this directory must have a mode of 0111.
Configuration of the lib subdirectory of the ftp account home directory	Must be owned by root and grant write access only to the owner. Files contained in this directory must have a mode of 0555.
Configuration of the etc subdirectory of the ftp account home directory	Must be owned by root and grant write access only to the owner. If the directory contains a passwd file, the password fields (field 2) must be empty
Configuration of other subdirectories of the ftp account home directory	Must not be owned by a general user account. If write access is granted to the group owner of the file, membership in the group is a security administrative authority. Directories must allow only read/execute access or write/execute access or no access for other.
Permissions of files and other directories descended from the ftp account home directory	Files must allow only read access except to the user owner and group owner of the file. If write access is granted to the group owner of the file, membership in the group is a security administrative authority. Directories must allow only read access, only write and execute access, or no access; except to user owner and group owner of the directory. If any additional access permission is granted to the group owner of the directory, membership in the group is a security administrative authority.
Directories enabled for Anonymous FTP access	READ access via anonymous FTP must not be granted to directories containing classified data.
Access permissions for directories accessible via Anonymous FTP	Each directory may allow read access or write access to anonymous users, but not both.
Trivial File Transfer Protocol (TFTP) System Settings	
tftp access control	The list of permitted directories must be specified with the -s parameter.
Directories enabled for TFTP access	Access via TFTP may be granted only to directories containing unclassified data, where the storage of IBM Confidential data is prohibited. This restriction also applies to any subdirectories of the directory.
Network File System (NFS) System Settings	
/etc/exports	The file must exist, if NFS server is installed and running, and must be owned by root and have 0644 permissions.
/etc/exports	Directories that are permitted to contain IBM Confidential data may not be exported unless the requirements specified in section 4 Information Protection & Confidentiality titled "Network File System (NFS), Process for Exporting IBM Confidential Data Without Strong Authentication" are met.
Berkeley Remote Access Commands System Settings	
/etc/hosts.equiv	Must not be used as an access control mechanism.
/etc/pam.d/rlogin /etc/pam.d/rsh	If a /lib/security/pam_rhosts_auth.so stanza exists, the **no_hosts_equiv** parameter must be present.
<$HOME>/.rhosts	Files permissions must only grant access to the owner of the file.

Remote Execution Daemon (rexd) System Settings	
rexd daemon	Must be disabled
.netrc files System Settings	
<$HOME>/.netrc files	File permissions must grant access only to the owner of the file.

Post Office Protocol (POP) System Settings	
POP user authentication	POP daemons must be configured to require users to authenticate. POP daemons that do not support authentication must be disabled.
Net News Transfer Protocol (NNTP) System Settings	
NNTP authentication and identification	Must be configured to require authentication and identification of all users if any of the newsgroups on the server are classified IBM Confidential
TCP/IP Denial of Service Prevention	
Must be disabled on all internet servers	CHARGEN, DAYTIME, DISCARD, ECHO, FINGER, SYSTAT, WHO, NETSTAT
Must be disabled if not required to support an application	BOOTPS, CHARGEN, DAYTIME, DISCARD, ECHO, FINGER, NETSTAT, PCNFSD, REXD, RSTAT, RUSER, RWALL, SPRAYD, TFTP, WHO
SNMP Service	Community name of 'public' and 'private' are not permitted if the SNMP service is active
/etc/sysctl.conf	net.ipv4.tcp_syncookies =1 note: Enable tcp syncookies to prevent syn flooding note: directly supported on RedHat 7.x and 8.x, Turbo Linux Server 7.0 and on Debian. Users of other distributions should add the following, as a single line, to a boot startup script: **echo 1 >/proc/sys/net/ipv4/tcp_syncookies**
/etc/sysctl.conf	net.ipv4.icmp_echo_ignore_broadcasts = 1 note: Turn off ICMP broadcasts note: directly supported on RedHat 7.x and 8.x, Turbo Linux Server 7.0 and on Debian. Users of other distributions should add the following, as a single line, to a boot startup script: **echo 1 >/proc/sys/net/ipv4/ icmp_echo_ignore_broadcasts**
/etc/sysctl.conf	net.ipv4.conf.all.accept_redirects = 0 note: Disable ICMP Redirect Acceptance note: directly supported on RedHat 7.x and 8.x, Turbo Linux Server 7.0 and on Debian. Users of other distributions should add the following, as a single line, to a boot startup script: **echo 0 >/proc/sys/net/ipv4/conf/all/accept_redirects**
Network Information Services (NIS) Settings, including NIS+ in NIS compatibility mode	
yppasswd daemon	Must be disabled.
NIS maps	Must not be used to store IBM Confidential data, including user passwords or other authentication credentials, in any form. If the NIS passwd maps are used, all encrypted passwords must be removed from the source file before the maps are generated.
Network Information Services Plus (NIS+) Settings	
NIS+ maps	If IBM Confidential data, including user passwords or other authentication credentials in any form, access may not be granted to the other or unauthenticated permissions class.

1.3 Sistema Operativo Windows 2000 Server

Aplicable a las siguientes versiones:

Microsoft Windows 2000 Server
Microsoft Windows 2000 Advanced Server
Microsoft Windows 2000 Professional

1.3.1 Elemento de Seguridad Interna – Identificación -

1.3.1.1 Userids

System Value/Parameter	Required Setting
Creating new userids	Set an initial password and force the user to change it. The check box 'User Must Change Password at Next Logon' must be selected.

1.3.2 Elemento de Seguridad Interna – Autenticación -

1.3.2.1 Reusable Passwords

System Value/Parameter	Required Setting
Passwords - minimum required password-related policy settings	
Enforce password history	4 passwords remembered
Maximum password age	186 days
Minimum password length	6 characters
Store password using reversible encryption	Disabled
'Password never expires'	May not be enabled for any userids except on: • Replicate • Guest • IUSR_{system} and IWAM_{system} user accounts created by Internet Information Server (IIS) • User accounts that are only associated with a started process(es) and are set to 'Disabled' status, so they can not be logged onto. (example: tmersrvd) User accounts that satisfy all of the following criteria:
	1. 'Logon locally' user right is disabled 2. Userid is not a member of the Administrators group 3. All interactive login methods (FTP, telnet, rexec, SSH, etc) are disabled for the userid

1.3.2.2 Authentication Tickets / Tokens

Standard requirements apply if Kerberos authentication is enabled.

1.3.3 Elemento de Seguridad Interna – Autorización -

1.3.3.1 Business Use Notice

Required	How implemented
No	

1.3.3.2 User Resources

System Value/Parameter	Required Setting
Creating new user home directories	At creation time, the home directory must be owned by the resource owner, and the maximum allowed permissions granted on the home directory to anyone other than the resource owner and administrators is: • Traverse Folder / Execute File • Read Attributes • Read Permissions
Note: If home directories are designed with subdirectories under them such as a 'public' folder or a folder for storing web pages that are readable by general users, the above permissions would be needed for users to traverse through and access the subdirectories. Otherwise granting no access to general users would be the more common approach for initial home directory permission settings set by the Provider of Service.	
Guest account	If the Guest account is enabled, it must comply with the following: • Only one ID of Guest allowed per server and one per domain • No access to IBM confidential data • Listed only in the Guests and/or Domain Guests account group and not included in any other groups
IUSR_{system} account	If the IUSR_{system} account is enabled, it must comply with the following: • No access to IBM confidential data • Listed only in the Guests and/or Domain Guests account group and not included in any other groups

1.3.4 Elemento de Seguridad Interna – Protección de la Información y Confidencialidad -

1.3.4.1 Encryption

System Value/Parameter	Setting information
Encryption for transmission over the Internet, public networks or wireless devices	Refer to the following for requirements criteria: • ITCS104 - Information Protection / Confidentiality The Windows 2000 High Encryption Pack provides 128-bit encryption support for Windows 2000 encryption-based services, including Kerberos, remote access, Remote Procedure Call (RPC), Secure Sockets Layer/Transport Layer Security (SSL/TLS), Cryptography Application Programming Interface (CryptoAPI), Terminal Services Remote Desktop Protocol (RDP), and IP Security (IPSec). Vendor software that supports encryption requirements of the main standard may also be used.
Encryption for storage of identity verification password files and/or e-payment data	Refer to the following for requirements criteria: • ITCS104 - Information Protection / Confidentiality • ITCS104 - Authentication Windows 2000 supports 128-bit encryption of folders/files with the Encrypting File System (EFS) when the Windows 2000 High Encryption Pack is installed. Vendor software that supports encryption requirements of the main standard may also be used.

1.3.5 Elemento de Seguridad Interna – Integridad y Disponibilidad del Servicio -

1.3.5.1 Operating System Resources

System Value/Parameter	Required Setting
The following objects are designated as OSRs. The access listed in the 'Required Setting' column is the maximum authority permitted to general users (e.g. Everyone, Users or other groups containing general users).	
%SystemRoot%	Read & Execute List Folder Contents Read
%SystemRoot%\Repair	no specific authorizations granted (normally implemented via omitting Everyone or Users groups from the ACL)
%SystemRoot%\System	Read & Execute List Folder Contents Read
%SystemRoot%\System32	Read & Execute List Folder Contents Read
%SystemRoot%\System32\Config	List Folder / Read Data
%SystemRoot%\System32\Drivers	Read & Execute List Folder Contents Read
%SystemRoot%\System32\Spool	Read & Execute List Folder Contents Read
%SystemDrive%\Boot.Ini	Read
%SystemDrive%\NTDetect.Com	Read
%SystemDrive%\NTLDR	Read
%SystemDrive%\AutoExec.Bat	Read
%SystemDrive%\Config.Sys	Read
%SystemDrive%	Read & Execute List Folder Contents Read

Notes:
- The above permissions are required on the specified directories and files listed only; not subfolders and files under them.
- Certain privileged ids/groups (e.g. Server Operator, Power User, Print Operator, SYSTEM) are granted default permissions to some OSRs. These defaults are acceptable and need not be changed.
- Administrators and SYSTEM may be granted Full Control to all OSRs.

Process exception: In environments where the Provider of Service can guarantee that no userid is able to access the file & directory OSRs (non-registry OSRs), the file/directory permissions defined in the in the table entries above need not be applied. One acceptable example of this would be an environment where both of the following apply:
- No general users are active at the NT Operating System layer (no shares are open to general users, users are not allowed to logon locally, etc)
- All Guest, IUSR_{system} and Anonymous userids have been disabled

Registry Controls required on Windows Terminal Servers:

hkey_classes_root	Maximum authorization allowed for **Everyone** or other general user groups such as Users & INTERACTIVE is **Read**

Registry Settings required on all servers:

System Value/Parameter	Required Setting
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application	Name: RestrictGuestAccess Type: REG_DWORD Value: 1
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security	Name: RestrictGuestAccess Type: REG_DWORD Value: 1
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\System	Name: RestrictGuestAccess Type: REG_DWORD Value: 1

1.3.5.2 Security & System Administrative Authority

System & Security Administrative userids include accounts within the following groups, as well as any others locally defined or that ship with services/applications, which have privileges as defined in ITCS104:
- Administrators
- Backup Operators
- Power Users
- Account Operators
- Pre-Windows 2000 Compatible Access
- Print Operators
- Server Operators
- Domain Admins
- Enterprise Admins
- Group Policy Creator Owners
- Schema Admins

1.3.5.3 Harmful Code Detection

Standard requirements apply

1.3.5.4 Systematic Logon Attacks

System Value/Parameter	Required Setting
Account lockout threshold	5 (or less)
Account lockout duration	Forever

1.3.6 Elemento de Seguridad Interna – Auditoría Activa

System Value/Parameter	Required Setting
Audit Policy - minimum logging requirements:	
Event	**Auditing enabled**
Account logon events	Success & Failure
Account management	Success & Failure
Directory service access	Failure
Logon events	Success & Failure
Object access	Failure
Policy change	Success & Failure
Privilege use	Success & Failure
Process Tracking	(not required to be set)
System events	Failure
'Security' log retained	60 days (minimum)

1.3.7 Elemento de Seguridad Interna – Verificación

1.3.7.1 Health Checking

Requirement	Description
Confirm that mandatory access control system options are as specified	Validate: • Password settings in Section 2.1 & 5.4 • Guest account restrictions in Section 3.2
Validate that only approved users hold security administrative and system authority	Validate users with system & security administrative privileges, as defined in Section 5.2
Check that all OSR access controls are set:	Validate settings in Section 5.1
Verify that only approved users are included in the access lists of OSRs beyond that allowed to general users.	Reference Section 5.1
Ensure Harmful code detection programs are installed and operational	Standard requirements apply
Check that the required access and activity logs data do exist	Validate security logs as per Section 6

1.3.8 Elemento de Seguridad Interna – Red

System Settings	Required Setting
TCP/IP Post Office Protocol (POP)	
Post Office Protocol (POP) authentication	If activated, POP services must be configured to require users to authenticate. POP services that do not support authentication must be disabled.
TCP/IP Net News Transfer Protocol (NNTP)	
Net News Transfer Protocol (NNTP) authentication & identification	If activated, must be configured to require authentication and identification of all users if any of the newsgroups on the server are classified confidential.
TCP/IP X-Windows	
X-Windows access control	If X-Windows service is active, access control must not be disabled
TCP/IP REXD	

REXD daemon	May not be enabled
TCP/IP Anonymous FTP	
Directories enabled for Anonymous FTP access	READ access via anonymous FTP must not be granted to directories containing classified data
Access permissions for directories accessible via Anonymous FTP	Each directory may allow read access or write access to anonymous users, but not both
Process Control: Anonymous FTP, Process for Receiving Files from Anonymous Users	Files that have been stored into a writeable directory must be examined (scanned for viruses, checked for IBM Confidential information, checked for inappropriate material, etc.) before being moved to a readable directory.
TCP/IP Trivial FTP (TFTP)	
Directories enabled for TFTP (Trivial File Transfer Protocol) access	Access via TFTP may be granted only to directories containing unclassified data. IBM confidential data is not permitted in directories accessible via TFTP or any subdirectories of the directory.
Denial of Service Prevention	
Internet Servers: Services to be disabled	ECHO, CHARGEN, FINGER, DISCARD, SYSTAT, DAYTIME, NETSTAT, WHO
Services to be disabled if not required to support an application	ECHO, CHARGEN, RSTAT, TFTP, RWALL, RUSER, DISCARD, DAYTIME, BOOTPS, FINGER, SPRAYD, PCNFSD, NETSTAT, WHO
SNMP service	Community names of 'public' and 'private' are not permitted if the SNMP service is active.

1.4 Sistema Operativo Windows NT Server

Aplicable a las siguientes versiones:

Microsoft Windows NT Version 4.0

1.4.1 Elemento de Seguridad Interna – Identificación -

1.4.1.1 Userids

System Value/Parameter	Required Setting
Creating new userids	Set an initial password and force the user to change it. The check box 'User Must Change Password at Next Logon' must be selected.

1.4.2 Elemento de Seguridad Interna – Autenticación -

1.4.2.1 Reusable Passwords

System Value/Parameter	Required Setting
Passwords - minimum required password-related policy settings	
Maximum password age	186 days
Minimum password length	6 characters
Password Uniqueness	4
'Password never expires'	May not be enabled for any userids except on: • Replicate • Guest • IUSR_{system} and IWAM_{system} user accounts created by Internet Information Server (IIS) • User accounts that are only associated with a started process(es) and are set to 'Disabled' status, so they can not be logged onto. (example: tmersrvd) • User accounts that satisfy all of the following criteria:
	1. 'Logon locally' user right is disabled 2. Userid is not a member of the Administrators group 3. All interactive login methods (FTP, telnet, rexec, SSH, etc) are disabled for the userid

1.4.2.2 Authentication Tickets / Tokens

Not applicable

1.4.3 Elemento de Seguridad Interna – Autorización -

1.4.3.1 Business Use Notice

Required	How implemented
No	

1.4.3.2 User Resources

System Value/Parameter	Required Setting
Creating new user home directories	At creation time, the home directory must be owned by the resource owner, and the maximum allowed permissions granted on the home directory to anyone other than the resource owner and administrators is: • Special Access: Execute [X]
Guest account	If the Guest account is enabled, it must comply with the following: • Only one ID of Guest allowed per server and one per domain • No access to IBM confidential data • Listed only in the Guests and/or Domain Guests account group and not included in any other groups
IUSR_{system} account	If the IUSR_{system} account is enabled, it must comply with the following: • No access to IBM confidential data • Listed only in the Guests and/or Domain Guests account group and not included in any other groups

1.4.4 Elemento de Seguridad Interna – Protección de la Información y Confidencialidad -

1.4.4.1 Encryption

System Value/Parameter	Setting Information
Encryption for transmission over the Internet, public networks or wireless devices	Refer to the following for requirements criteria: ITCS104 - Information Protection / Confidentiality Windows NT supports 128-bit encryption for select services when the 128-bit service pack is installed. Vendor software that supports encryption requirements of the main standard may also be used.
Encryption for storage of identity verification password files and/or e-payment data	Refer to the following for requirements criteria: ITCS104 - Information Protection / Confidentiality ITCS104 - Authentication Windows NT does not have native support for 128-bit encryption of folders/files. Vendor software that supports encryption requirements of the main standard must be used when this is required.

1.4.5 Elemento de Seguridad Interna – Integridad y Disponibilidad del Servicio -

1.4.5.1 Operating System Resources

System Value/Parameter	Required Setting
The following objects are designated as OSRs. The access listed in the 'Required Setting' column is the maximum authority permitted to general users (e.g. Everyone, Users or other groups containing general users).	
%SystemRoot%	Read
%SystemRoot%\Repair	no specific authorizations granted (normally implemented via omitting Everyone or Users groups from the ACL)
%SystemRoot%\System	Read
%SystemRoot%\System32	Read (** see subnote below)
%SystemRoot%\System32\Config	List
%SystemRoot%\System32\Drivers	Read
%SystemRoot%\System32\Spool	Read
%SystemDrive%\Program Files	Read
%SystemDrive%\Boot.Ini	Special Access: Read [R]
%SystemDrive%\NTDetect.Com	Special Access: Read [R]
%SystemDrive%\NTLDR	Special Access: Read [R]
%SystemDrive%\AutoExec.Bat	Read
%SystemDrive%\Config.Sys	Read
Subnote: ** Because some 3rd party and Microsoft applications currently require this, Everyone:Read / Users:Change permission is allowed on servers which run applications that require general users have this level of authority. For servers which do not run applications requiring Change authority for general users, the Users group must either be omitted from the System32 ACL or must have no greater than "Read" permission.	
Notes: • The above permissions are required on the specified directories and files listed only; not subfolders and files under them. • Certain privileged ids/groups (e.g. Server Operator, Power User, Print Operator, SYSTEM) are granted default permissions to some OSRs. These defaults are acceptable and need not be changed. • Administrators and SYSTEM may be granted Full Control to all OSRs.	
Process exception: In environments where the Provider of Service can guarantee that no userid is able to access the file & directory OSRs (non-registry OSRs), the file/directory permissions defined in the OSR table in the table above need not be applied. One acceptable example of this would be an environment where both of the following apply: • No general users are active at the NT Operating System layer (no shares are open to general users, users are not allowed to logon locally, etc) • All Guest, IUSR_{system} and Anonymous userids have been disabled	
Registry Controls required on all servers:	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Maximum authorization

- and - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	allowed for **Everyone** or other general user groups such as Users & INTERACTIVE is **Read**
Registry Controls required on Windows Terminal Servers and WinFrame Servers:	
hkey_classes_root	Maximum authorization allowed for **Everyone** or other general user groups such as Users & INTERACTIVE is **Read**

Registry Settings required on all servers:

System Value/Parameter	Required Setting
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application	Name: RestrictGuestAccess Type: REG_DWORD Value: 1
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security	Name: RestrictGuestAccess Type: REG_DWORD Value: 1
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\System	Name: RestrictGuestAccess Type: REG_DWORD Value: 1
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Name: ShutdownWithoutLogon Type: REG_SZ Value: 0

1.4.5.2 Security & System Administrative Authority

System & Security Administrative userids include accounts within the following groups, as well as any others locally defined or that ship with services/applications, which have privileges as defined in ITCS104:

- Administrators
- Backup Operators
- Domain Administrators
- Account Operators
- Print Operators
- Server Operators
- Power Users

1.4.5.3 Harmful Code Detection

Standard requirements apply

1.4.5.4 Systematic Logon Attacks

System Value/Parameter	Required Setting
Account lockout	5 (or less)
Account lockout duration	Forever

1.4.6 Elemento de Seguridad Interna – Auditoría Activa

System Value/Parameter	Required Setting
Audit Policy - minimum logging requirements:	
Event	**Auditing enabled**
Logon and Logoff	Success & Failures
File and Object Access	Failures
Use of user rights	Success & Failures
User and Group Management	Success & Failures
Security Policy Changes	Success & Failures
Start/Restart/Shutdown Server	Success & Failures
Process Tracking	Logging Not Required
'Security' log retained	60 days (minimum)

1.4.7 Elemento de Seguridad Interna – Verificación

1.4.7.1 Health Checking

Requirement	Description
Confirm that mandatory access control system options are as specified	Validate: • Password settings in Section 2.1 & 5.4 • Guest account restrictions in Section 3.2
Validate that only approved users hold security administrative and system authority	Validate users with system & security administrative privileges, as defined in Section 5.2
Check that all OSR access controls are set:	Validate settings in Section 5.1
Verify that only approved users are included in the access lists of OSRs beyond that allowed to general users.	Reference Section 5.1
Ensure Harmful code detection programs are installed and operational	Standard requirements apply
Check that the required access and activity logs data do exist	Validate security logs as per Section 6

1.4.8 Elemento de Seguridad Interna – Red

System Settings	Required Setting
TCP/IP Post Office Protocol (POP)	
Post Office Protocol (POP) authentication	If activated, POP services must be configured to require users to authenticate. POP services that do not support authentication must be disabled.
TCP/IP Net News Transfer Protocol (NNTP)	
Net News Transfer Protocol (NNTP) authentication & identification	If activated, must be configured to require authentication and identification of all users if any of the newsgroups on the server are classified confidential.
TCP/IP X-Windows	
X-Windows access control	If X-Windows service is active, access control must not be disabled
TCP/IP REXD	
REXD daemon	May not be enabled
TCP/IP Anonymous FTP	
Directories enabled for Anonymous FTP access	READ access via anonymous FTP must not be granted to directories containing classified data
Access permissions for directories accessible via Anonymous FTP	Each directory may allow read access or write access to anonymous users, but not both
Process Control: Anonymous FTP, Process for Receiving Files from Anonymous Users	Files that have been stored into a writeable directory must be examined (scanned for viruses, checked for IBM Confidential information, checked for inappropriate material, etc.) before being moved to a readable directory.
TCP/IP Trivial FTP (TFTP)	
Directories enabled for TFTP (Trivial File Transfer Protocol) access	Access via TFTP may be granted only to directories containing unclassified data. IBM confidential data is not permitted in directories accessible via TFTP or any subdirectories of the directory.
Denial of Service Prevention	
Internet Servers: Services to be disabled	ECHO, CHARGEN, FINGER, DISCARD, SYSTAT, DAYTIME, NETSTAT, WHO
Services to be disabled if not required to support an application	ECHO, CHARGEN, RSTAT, TFTP, RWALL, RUSER, DISCARD, DAYTIME, BOOTPS, FINGER, SPRAYD, PCNFSD, NETSTAT, WHO
SNMP service	Community names of 'public' and 'private' are not permitted if the SNMP service is active.

1.5 Sistema Operativo Novell NetWare

Aplicable a las siguientes versiones:

Novell NetWare Server versiones 5 y 6 en un ambiente bajo IP.

1.5.1 Elemento de Seguridad Interna – Identificación -

1.5.1.1 Userids

System Controls	Required Setting
Guest ID Restrictions	Remove the guest account and create meaningful unique accounts for the business need.

1.5.2 Elemento de Seguridad Interna – Autenticación -

Standard requirements apply.

1.5.2.1 Reusable Passwords

System Controls	Description	Required Setting
Defaults Account Balance/Restrictions settings	Password Controls	• Set "Account Has Expiration Date" to YES. (This should be done for Supplemental and Non-IBM Employees). • Set "Allow User to Change Password" to YES. • Set "Require Password" to YES. • Set "Minimum Password Length" to 6. • Set "Force Periodic Password Change" to Yes and the duration to 186 days. • Set "Require Unique Password" to Yes. • Set "Allow Graceful Login" to 5.
DETECT INTRUDERS within the Organizational Container	This allows the OS to detect invalid login attempts.	Set to YES.
INCORRECT LOGIN ATTEMPTS within the Organizational Container		Set to five (5)
BAD LOGIN COUNT		Set to one (1) day or 24

RETENTION TIME within the Organizational Container		hours
LOCK ACCOUNT AFTER DETECTION within the Organizational Container	This will lock the account when the number of invalid login attempts has been reached within the specified period.	Set to YES
LENGTH OF ACCOUNT LOCKOUT within the Organizational Container		Set to 365 days.

1.5.2.2 Authentication Tickets / Tokens

Standard requirements apply.

1.5.3 Elemento de Seguridad Interna – Autorización -

1.5.3.1 Business Use Notice

Required	Description	Required Setting
Yes	IBM Systems must only be used for conducting IBM business or for purposes authorized by IBM management. Use is subject to audit at any time by IBM management.	Include the business use notice text in the SYSTEM LOGIN SCRIPT file of every user. Also specify LASTLOGINTIME in the System Login Script file of every user.

1.5.3.2 User Resources

Standard requirements apply.

1.5.4 Elemento de Seguridad Interna – Protección de la Información y Confidencialidad -

Standard requirements apply.

1.5.4.1 Encryption

Standard requirements apply.

1.5.5 Elemento de Seguridad Interna – Integridad y Disponibilidad del Servicio -

1.5.5.1 Operating System Resources

System Value/Parameter	Description	Required Setting
SYS:SYSTEM ROOT Objects NetWare Directory Services (NDS) SYS$LOG.ERR VOL$LOG.ERR NET$AUD.DAT AUD$HIST.DAT NET$AUD.CAF		Non-administrative users must not be granted any access or rights
Remote Access to the server console		1. If remote access is enabled you must enable a password protected screen saver that is unique from any other password. 2. If remote access is not enabled, and the server is in a CA2 secure area, no password protected screen saver is required.
RCONAG6.NLM	Replaces rconsole.	Assign a unique password and change every 186 days. Password must be different from admin equivalents and encrypted.
SCRSAVER.NLM	Replaces Monitor Password	Loaded during system start-up in the server AUTOEXEC file.
SCRSAVER and RCONAG6 Passwords		Change when any of the following occurs: • Password was last changed 186 days ago. • The password was provided to someone outside of the support staff who has RCONAG6 access. • Any person leaving the support staff and the business need to have access to RCONAG6 no longer exist.

1.5.5.2 Security & System Administrative Authority

Standard requirements apply.

1.5.5.3 Harmful Code Detection

Standard requirements apply

1.5.5.4 Systematic Logon Attacks

System Value/Parameter	Required Setting
INCORRECT LOGIN ATTEMPTS within the Organizational Container	Set to five (5)

1.5.6 Elemento de Seguridad Interna – Auditoría Activa

System Value/Parameter	Required Settings
1. Are audit records created for: a. successful and unsuccessful logon access attempts? b. update access attempts to OSRs not listed as exceptions? c. read access attempts to OSRs that are listed as exceptions? d. execution access attempts to OSRs that are listed as exceptions? e. activities performed using security administrative authority? f. successful assignment and release of network IP addresses?	• Implement Auditcon for NetWare 5.x systems. • NAAS for NetWare 6.x. • Novell NSure Audit for all encompassing NetWare OS's. • Ensure FTP and HTTP logs are active. • Ensure console.log is set to archive.

1.5.7 Elemento de Seguridad Interna – Verificación

1.5.7.1 Health Checking

Requirement	Description/Comments
Confirm that mandatory access control system options are as specified	
Validate that only approved users hold security	• Userids with SUPERVISOR EQUIVALENT or ADMINISTRATIVE EQUIVALENT have security

administrative and system authority	administrative authority. Server Manager, Workgroup Manager and Console Operator have system authority. • Is root NFS access restricted only to clients with a business need?
Check that all OSR access controls are set	
Verify that only approved users are included in the access lists of OSRs beyond that allowed to general users.	
Ensure Harmful code detection programs are installed and operational	
Check that the required access and activity logs data do exist.	

1.5.8 Elemento de Seguridad Interna – Red

TCP/IP Anonymous FTP	
Directories enabled for Anonymous FTP access	READ access via anonymous FTP must not be granted to directories containing classified data
Access permissions for directories accessible via Anonymous FTP	Each directory may allow read access or write access to anonymous users, but not both.
Denial of Service Prevention	
Internet Servers: Services to be disabled	ECHO, CHARGEN, FINGER, DISCARD, SYSTAT, DAYTIME, NETSTAT, WHO
Services to be disabled if not required to support an application	ECHO, CHARGEN, RSTAT, TFTP, RWALL, RUSER, DISCARD, DAYTIME, BOOTPS, FINGER, SPRAYD, PCNFSD, NETSTAT, WHO
SNMP service	Community names of 'public' and 'private' are not permitted if the SNMP service is active.

1.6 Sistema Operativo OS/2

Aplicable a las siguientes versiones:

OS/2 Release 2.0 y superiores donde la plataforma es usada como base para cualquier servidor.

1.6.1 Elemento de Seguridad Interna – Identificación -

1.6.1.1 Userids

Not applicable.

1.6.2 Elemento de Seguridad Interna – Autenticación -

Not applicable.

1.6.2.1 Reusable Passwords

Not applicable.

1.6.2.2 Authentication Tickets / Tokens

Not applicable.

1.6.3 Elemento de Seguridad Interna – Autorización -

1.6.3.1 Business Use Notice

Required	How implemented
No	

1.6.3.2 User Resources

Not applicable.

1.6.4 Elemento de Seguridad Interna – Protección de la Información y Confidencialidad -

1.6.4.1 Encryption

Standard requirements apply.

Description	Supported
Encryption for transmission over the Internet, public networks or wireless devices	No
Encryption for storage of identity verification password files, e-payment data, etc.	No

1.6.5 Elemento de Seguridad Interna – Integridad y Disponibilidad del Servicio -

1.6.5.1 Operating System Resources

System Value/Parameter	Description	Required Setting
CONFIG.SYS OS2.INI STARTUP.CMD desktop directory delete directory		Must be write protected

1.6.5.2 Security & System Administrative Authority

Not applicable.

1.6.5.3 Harmful Code Detection

Standard requirements apply.

1.6.5.4 Systematic Logon Attacks

Not applicable.

1.6.6 Elemento de Seguridad Interna – Auditoría Activa

Not applicable.

1.6.7 Elemento de Seguridad Interna – Verificación

1.6.7.1 Health Checking

Requirement	Description
Confirm that mandatory access control system options are as specified	N/A
Validate that only approved users hold security administrative and system authority	N/A
Check that all OSR access controls are set	Validate settings under section 5.1 in this document.
Verify that only approved users are included in the access lists of OSRs beyond that allowed to general users.	N/A
Ensure Harmful code detection programs are installed and operational	Standard requirements apply
Check that the required access and activity logs data do exist	N/A

1.6.8 Elemento de Seguridad Interna – Red

System Settings	Required Setting
TCP/IP Anonymous FTP	
Directories enabled for Anonymous FTP access	Access via anonymous FTP may be granted only to directories containing unclassified data. IBM confidential data is not permitted in directories accessible via Anonymous FTP.
Access permissions for directories accessible via Anonymous FTP	Each directory may allow read access or write access to anonymous users, but not both
Anonymous FTP access rights for user:anonymous in TRUSERS file	Access may not be specified for a directory if access is also specified for a component of its path
Files that have been stored into a writeable directory via Anonymous FTP	Must be examined (scanned for viruses, checked for IBM Confidential information, checked for inappropriate material, etc.) before being moved to a readable directory
TCP/IP Trivial FTP (TFTP)	
TFTP Service	Must be disabled on all servers.
TCP/IP NFS (Network File System) Server	
If NFS server is active	The \etc\exports file must exist.
If NFS server is active	Each exported directory must use either the "-readonly"

	or "-hosts" option.
If NFS server is active	Directories that are permitted to contain IBM Confidential data may not be exported.
TCP/IP Berkeley Remote Access Commands	
rshd daemon	Must be disabled.
\etc\rhosts file	Must not exist.
TCP/IP REXD Daemon	
REXD daemon	Must be disabled on all servers.
TCP/IP Telnet daemon	
LOGINUNX.EXE	Must be used on systems subject to Disaster Recovery.
TCP/IP Netrc File	
\ETC\NETRC file	File must not exist.
TCP/IP Post Office Protocol (POP)	
POP user authentication	If activated, POP services must be configured to require users to authenticate. POP services that do not support authentication must be disabled.
TCP/IP Net News Transfer Protocol (NNTP)	
NNTP authentication & identification	If activated, must be configured to require authentication and identification of all users if any of the newsgroups on the server are classified IBM confidential.
TCP/IP X-Windows	
X-Windows access control	Must not be disabled.
TCP/IP Denial of Service Prevention	
Internet Servers: Services to be disabled	ECHO, CHARGEN, FINGER, DISCARD, SYSSTAT, DAYTIME, NETSTAT, WHO
Services to be disabled if not required to support an application	ECHO, CHARGEN, RSTAT, RWALL, RUSER, DISCARD, DAYTIME, BOOTPS, FINGER, SPRAYD, PCNFSD
TCP/IP Simple Network Management Protocol (SNMP)	
SNMP service	Community names of 'public' and 'private' are not permitted if the SNMP service is active.

1.7 Sistema Operativo OS/400

Aplicable a las siguientes versiones:

OS/400 V3R1M0 - VSR2M0.

1.7.1 Elemento de Seguridad Interna – Identificación -

1.7.1.1 Userids

System Value/Parameter	Description	Required Setting
Non-IBM supplied user profiles • User Profile AUT Parameter	User profile public authority parameter	Restricted from public use • *EXCLUDE
IBM-supplied user profiles	Some userids are shipped with public authority greater than *EXCLUDE	Authority parameter settings should not be changed
Job descriptions public authority (AUT parameter) for systems operating at security level 30	Ensure jobs cannot gain use of user profile authorities	If the User parameter contains a user profile name, set to PUBLIC *EXCLUDE
Exemption to Job Description Public Authority *EXCLUDE Parameter Setting:		
IBM-supplied job descriptions are exempt from the public authority *EXCLUDE parameter setting requirement. The public authority parameter on IBM-supplied job descriptions should not be altered from its shipped value.		

1.7.2 Elemento de Seguridad Interna – Autenticación -

1.7.2.1 Reusable Passwords

System Value/Parameter	Description	Required Setting
Password Syntax - minimum required settings		
QPWDEXPITV	Password expiration interval value	186
QPWDLMTAJC	Restrictions of consecutive digits in passwords	0
QPWDLMTCHR	Restricted number of characters for passwords	*NONE
QPWDLMTREP	Restriction of repeated characters in passwords	set to 0 in conjunction with use of password validation program
QPWDMINLEN	Minimum length of	6

System Value/Parameter	Description	Required Setting
	passwords	
QPWDPOSDIF	Position difference of characters in successive passwords	set to 0 in conjunction with use of password validation program
QPWDRQDDGT	Requirement for numeric characters in passwords	1
QPWDRQDDIF	Required difference in passwords	8
QPWDVLDPGM	Password validation program	PWVAL/PWV0010, PWVAL/D510W1C or PWVAL/SEPV510C
User Profile PWDEXPITV Parameter	User profile password expiration interval parameter	*SYSVAL or 186
QPGMR, QSECOFR, QSRV, QSRVBAS, QSYSOPR and QUSER passwords	IBM-Supplied User Profiles	Set to *NONE or set to minimum required password syntax settings
Dedicated Service Tools (DST) Passwords	Security, Full and Basic Levels	Set to minimum required password syntax settings and change at least once every 186 days
	Full and Basic Levels	Sharable by all authorized systems support and operations personnel
Exemptions from Password Syntax Requirements:		
User profiles with a password parameter set to *NONE	These user profiles cannot be signed on	Exempt from all the password syntax required settings
User profiles shipped as part of program products with a non-expiring password unknown to the installer or service provider, Initial Menu set to *SIGNOFF and Limit Capabilities set to either *YES or *PARTIAL (i.e., RBTNETPT)		Exempt from the password expiration value of 186 and may retain the value of *NOMAX.

1.7.2.2 Authentication Tickets / Tokens

Not applicable.

1.7.3 Elemento de Seguridad Interna – Autorización -

1.7.3.1 Business Use Notice

Required	How Implemented
Yes	The Business Use Notice must be displayed during the signon process or placed on all sign-on screens for subsystems that support interactive jobs (with the exception of the controlling subsystem if it limits interactive sessions to the system console and subsystem QSYSSBSD).

1.7.3.2 User Resources

OS/400 User Resources (URs) are defined as libraries, first-level folders and first-level directories that are owned by individuals or a group of individuals, which do not influence the integrity or functions of the operating system and/or other software products.

System Control	Description	Required Setting
CRTLIB command	Change initial default protection setting for 'Create Library' command	Set public access authority parameter to: AUT = *EXCLUDE
CRTDIR command	Change initial default protection setting for 'Create Directory' command	Set public access authority parameters to: DTAAUT = *EXCLUDE OBJAUT = *NONE
MD command	Change initial default protection setting for 'Make Directory' command	Set public access authority parameters to: DTAAUT = *EXCLUDE OBJAUT = *NONE
MKDIR command	Change initial default protection setting for 'Make Directory' command	Set public access authority parameters to: DTAAUT = *EXCLUDE OBJAUT = *NONE

1.7.4 Elemento de Seguridad Interna – Protección de la Información y Confidencialidad -

1.7.4.1 Encryption

System Value/Parameter	Required Setting
See the following for requirements criteria: ITCS104 - Information Protection / Confidentiality ITCS104 - Authentication	How implemented will depend on the data transfer services in use in the particular environment.

1.7.5 Elemento de Seguridad Interna – Integridad y Disponibilidad del Servicio -

System Value	Description	Required Setting
Minimum required settings:		
QSECURITY	Operating system security level If it is necessary to use an application that fails at security level 40, the security level (QSECURITY) must be set to 30. A risk assessment/acceptance is not required; however, the Provider of Service must document the following: • The name of each application which fails at security level 40 • The reasons why it is necessary to use each application. (This information should be provided to the Provider of Service by each application owner.) • If appropriate, the target dates for installation of alternative applications and/or addition of level 40 support to existing applications.	40 (or 30 - see description)
QALWOBJRST	Allow object restore option	*NONE or *ALWPTF
QDEVRCYACN	Device recovery action	*DSCMSG
QRMTSIGN	Remote sign-on control	*VERIFY

1.7.5.1 Operating System Resources

OS/400 Operating System Resources (OSRs) are defined as libraries, first-level folders and first-level directories that are part of the OS/400 program and other software products which are related to system services and functions.

System Control	Description	Required Setting
OSR public access authority	Prevent update by general user	*USE or *EXCLUDE *RX, *R or *X
OSR object auditing authority	Capture all successful and unsuccessful update accesses	*CHANGE
OSR exceptions	Can be updated by the general user	List must be maintained by the provider of service
		Object auditing parameter not required to be set
OSRs that must not have read/execute public access (public access authority of *EXCLUDE)	Those OSRs that may allow users to bypass security controls	List must be maintained by the provider of service
		Object auditing parameter set to *ALL
QSPL	Excessive number of audit records would be written if set	Object auditing parameter not required to be set

If the public access authority parameter on the OSR is set to:	The Provider of Service must specifically document the exception?	And Provider of Service must set the Object Auditing Value (OBJAUD) parameter on the OSR to:
AUT = *ALL	Yes	*NONE
AUT = *CHANGE	Yes	*NONE
AUT = *USE	No	*CHANGE
AUT = *EXCLUDE	Yes	*ALL
DTAAUT = *RWX	Yes	*NONE
DTAAUT = *RW	Yes	*NONE
DTAAUT = *RX	No	*CHANGE
DTAAUT = *R	No	*CHANGE
DTAAUT = *WX	Yes	*NONE
DTAAUT = *W	Yes	*NONE
DTAAUT = *X	No	*CHANGE
DTAAUT = *EXCLUDE	Yes	*ALL
DTAAUT = *NONE	Yes	*ALL

1.7.5.2 Security & System Administrative Authority

System and security administrative authority (privileged user) include those user profiles that have **use of the command line** (Limit Capabilities is set to *PARTIAL or *NO), **and also** either have been assigned **specific special authorities or have use of special authorities via a group profile.**

Special Authority	Allows a user:	System Authority	Security Administrative Authority
*ALLOBJ	To perform all operations on objects	X	X
*AUDIT	To define the auditing characteristics of the system		X
*IOSYSCFG	To configure input and output devices on the system	X	X
*JOBCTL	To control batch jobs and printing on the system	X	X
*SAVSYS	To save and restore objects	X	X
*SECADM	To work with user profiles on the system	X	X
*SERVICE	To perform software service functions on the system	X	X
*SPLCTL	Unrestricted control of batch jobs and output queues on the system	X	X

1.7.5.3 Harmful Code Detection

Not applicable.

1.7.5.4 Systematic Logon Attacks

System Value	Description	Required Setting
Sign-on Attempts - minimum required settings		
QMAXSIGN	Maximum number of sign-on attempts	5
QMAXSGNACN	Action when sign-on attempts reached	2

1.7.6 Elemento de Seguridad Interna – Auditoría Activa

System Value/Parameter	Description	Required Setting
Auditing Controls - minimum required settings		
System value QAUDCTL	System value for auditing control	*AUDLVL *OBJAUD
System value QAUDLVL	System value for auditing level	*AUTFAIL *JOBDTA *SAVRST *SECURITY
Privileged User Profile's AUDLVL Parameter	Privileged user's action auditing parameter	*CMD *CREATE *DELETE *OBJMGT *OFCSRV *OPTICAL *PGMADP *SERVICE *SPLFDTA *SYSMGT

1.7.7 Elemento de Seguridad Interna – Verificación

1.7.7.1 Health Checking

Requirement	Description
Confirm that mandatory access control system options are as specified	Validate: • System value settings in Section 5 • Auditing Control settings in Section 6 • Password settings in Section 2.1 • Sign-on attempt settings in Section 5.4 • Default settings for user resources in Section 3.2
Validate that only approved users hold system and security administrative authority (privileges)	System and security administrative authority (privileged user) include those user profiles that have **use of the command line** (Limit Capabilities is set to *PARTIAL or *NO), **and also** either have been assigned **specific special authorities or have use of special authorities via a group profile.** Special authorities are: *ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL, *SAVSYS, *SECADM, *SERVICE and *SPLCTL
Check that all OSR access controls are set	Validate settings in Section 5.1
Verify that only approved users are included in the access lists of OSRs beyond that allowed to general users	Reference Section 5.1
Ensure harmful code detection programs are installed and operational	Not applicable to OS/400 environment
Check that the required access and activity logs data do exist	Ensure the security audit journal (QAUDJRN) exists

1.7.8 Elemento de Seguridad Interna – Red

System Settings	Required Setting
TCP/IP Anonymous FTP	
ANONYMOUS user profile	PASSWORD(*NONE) and PWDEXPINT(*NOMAX)
Permissions for FTP exit program or library containing FTP exit program.	PUBLIC *EXCLUDE must be specified
Access permissions for directories accessible via Anonymous FTP	Each directory may allow read access or write access to anonymous users, but not both.
Directories enabled for anonymous FTP access	READ access via anonymous FTP must not be granted to directories containing classified data
Process Control: Anonymous FTP, Process for Receiving Files from Anonymous Users	Files that have been stored into a writeable directory must be examined (scanned for viruses, checked for IBM Confidential information, checked for inappropriate material, etc.) before being moved to a readable directory.
Trivial File Transfer Protocol (TFTP)	

System Settings	Required Setting
Directories enabled for TFTP (Trivial File Transfer Protocol) access	Access via TFTP may be granted only to directories containing unclassified data. IBM Confidential data is not permitted in directories accessible via TFTP or any subdirectories of the directory.
TCP/IP Network File System (NFS)	
/etc/exports	The /etc IFS directory must not be exported.
/etc/exports	Directories that are permitted to contain IBM confidential data may not be exported unless the requirements specified in Process Control: Network File System are met.
Process Control: Network File System (NFS), Process for Exporting IBM Confidential Data Without Strong Authentication	Access to data classified IBM Confidential may be granted through NFS on an exception basis under the following conditions: • Anonymous user access may not be granted to IBM Confidential data. • The -hosts option is specified in /etc/exports for all directories that may contain IBM Confidential files. • A process is established to ensure that all hosts specified in -hosts options in */etc/exports* at least quarterly, for all directories that may contain IBM Confidential files, share common userid/UID# and groupid/GID#/mapping. • A process is established to validate all hosts in */etc/exports* at least quarterly, for all directories that may contain IBM Confidential files. If access to directories that may contain IBM Confidential files is provided to netgroups, the hosts in the netgroups must be validated at least quarterly.
X-Window	
X-server access control	Must not be disabled.
Denial of Service Prevention	
Internet Servers: services to be disabled	ECHO, CHARGEN, FINGER, DISCARD, SYSTAT, DAYTIME, NETSTAT, WHO
Services to be disabled if not required to support an application	ECHO, CHARGEN, RSTAT, TFTP, RWALL, RUSER, DISCARD, DAYTIME, BOOTPS, FINGER, SPRAYD, PCNFSD, NETSTAT, WHO
SNMP service	Community names of 'public' and 'private' are not permitted if the SNMP service is active.

APÉNDICE II

Código de Ética en los Sistemas

I. Introducción

Para efectos del presente Código de Ética en los Sistemas, se entiende dentro del mismo ámbito a las profesiones relacionadas con la informática, la computación y los sistemas computacionales, sea cual fuere su denominación en lo sucesivo se utilizará el término profesional de sistemas para definirlo. La lista de normas no es necesariamente exhaustiva y la intención es ilustrar y explicar con detalle el Código de Ética en los Sistemas referente al comportamiento ideal que se espera encontrar en el profesional de sistemas.

II. Alcance del Código de Ética en los Sistemas

Aplicación Universal del Código

Este Código de Ética en los Sistemas ha sido creado y actualizado por la Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información, o ISACA por sus siglas en inglés). ISACA es una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de sistemas de información. Sus normas de auditoría y control de sistemas de información son respetados por profesionales de todo el mundo. Sus investigaciones resaltan temas profesionales que desafían a sus constituyentes y han dado pauta a la creación de este Código de Ética en los Sistemas, el cual es aplicable a toda persona que tenga una profesión asociada con la informática, la computación o los sistemas computacionales, sin importar la índole de su actividad o la especialidad que cultive tanto en el ejercicio independiente o cuando actúe como funcionario o empleado de instituciones públicas o privadas.

Actuación Profesional

El futuro de la profesión de sistemas, depende de la excelencia técnica y ética. Es por eso que se vuelve indispensable que todos los profesionales en esta área se adhieran a los principios ya expresados en este código, así como promover su difusión y práctica.

Los profesionales de sistemas tienen la ineludible obligación de regir su conducta de acuerdo a las reglas contenidas en este código, las cuales deben considerarse mínimas pues se reconoce la existencia de otras normas de carácter legal y moral cuyo espíritu amplía el de las presentes.

Este código rige la conducta del profesional de sistemas en sus relaciones con el público en general, con quien patrocina sus servicios (cliente o patrón) y con sus compañeros de profesión y le será aplicable cualquiera que sea la forma que revista su actividad, la especialidad que cultive o la naturaleza de la retribución que perciba por sus servicios.

Los profesionales de sistemas que además ejerzan otra profesión deben acatar las reglas de conducta incluidas en este código, independientemente de las que la organización señale a la que pertenezca o preste servicio.

Los profesionales de sistemas deben abstenerse de hacer comentarios sobre sus colegas cuando dichos comentarios perjudiquen su reputación o el prestigio de la profesión en general, a menos que se soliciten por quien tenga un interés legítimo de ellos.

Actitud Personal

El profesional de sistemas debe respeto a sus semejantes y su comportamiento en lo personal y social debe atender la práctica de buenas costumbres y seguir un objetivo útil.

El profesional de sistemas debe tener la costumbre de cumplir los compromisos adquiridos, no por el hecho de estar escritos, sino por convicción propia.

El profesional de sistemas debe ser capaz de comprometer su palabra y cumplirla aún en situaciones desfavorables.

El profesional de sistemas debe de respetar y hacer respetar su tiempo y el de los demás, predicar con el ejemplo, poseer espíritu de servicio y habilidad para comunicarse con los demás.

El profesional de sistemas actuará siempre cuidando el no afectar la integridad física, emocional ni económica de las personas.

Independencia de Criterio

Al realizar cualquier proyecto el profesional de sistemas acepta la obligación de sostener un criterio libre e imparcial, sin aceptar ni permitir presiones de terceros involucrados en la situación, que pudieran verse beneficiados por la decisión o actitud adoptada.

Rechazar Tareas que NO cumplan con la Moral del Profesional de Sistemas

El profesional de sistemas faltará al honor y dignidad cuando directa o indirectamente intervenga en arreglos o asuntos que no cumplan con las normas establecidas en el "Código de Ética del Profesional de Sistemas".

El profesional de sistemas hará uso y aplicación de sus conocimientos profesionales sólo en tareas que cumplan con las normas establecidas en el "Código de Ética del Profesional de Sistemas".

Calidad Profesional de los Trabajos

En la prestación de cualquier servicio se espera del profesional de sistemas un verdadero trabajo de calidad, por lo que se tendrán presentes las disposiciones normativas de la profesión que sean aplicables al trabajo específico que esté desempeñando y de ser posible sujetarse a lo más altos estándares de calidad mundial existentes.

Preparación y Calidad Profesional

El profesional de sistemas no debe aceptar tareas para las que no esté capacitado. Por ser la información un recurso difícil de manejar en las empresas, se requiere de profesionales de sistemas que definan estrategias para su generación, administración y difusión, por lo que ninguna persona podrá aceptar un trabajo relacionado con la informática, computación o sistemas computacionales, sin contar con el entrenamiento técnico y la capacidad comprobada necesaria para realizar éstas actividades de manera satisfactoria y profesional. El profesional de sistemas vigilará que su propia actualización y capacitación profesional sea de crecimiento permanente.

Ejercicio de la Profesión

El profesional de sistemas debe tener presente que la retribución económica por sus servicios no constituye el único objetivo ni la razón de ser del ejercicio de su profesión sino que él mismo se ajustará a los principios humanos en la utilización de la tecnología en bien del avance y desarrollo de la sociedad. El profesional de sistemas debe analizar cuidadosamente las verdaderas necesidades que puedan tenerse de

sus servicios, para proponer aquellos que más convengan dentro de las circunstancias.

III. Responsabilidades hacia el Cliente o Patrocinador del Servicio

La Importancia del Cliente

El profesional de sistemas debe ubicarse como una entidad de servicio, por lo que su objetivo principal es la atención adecuada al cliente. El profesional de sistemas debe brindar todo el respeto al cliente y entender que la única diferencia con él es la formación y habilidad al desarrollar herramientas informáticas. El profesional de sistemas debe evitar hacer comentarios alabadores al cliente con el objetivo de obtener beneficios, así como evitar hacer comentarios que deterioren la imagen de su cliente por el simple hecho de hacerlo.

Proteger el Interés del Cliente o Patrón

El profesional de sistemas independientemente de cual sea su relación contractual, debe vigilar por el interés del cliente o patrón y evitar en todo momento crear una situación de dependencia tecnológica, hacia sus servicios. Debe alertar al cliente o patrón sobre los riesgos de utilizar cada plataforma de equipos y programas con respecto a la continuidad de operaciones y servicios sin la presencia del profesional de sistemas.

El profesional de sistemas debe aprovechar y explotar al máximo las herramientas y aplicaciones adquiridas por la empresa, para el beneficio propio de la organización, así mismo debe indicar cualquier desperdicio de recursos computacionales del cual tenga conocimiento y evitar que la empresa haga gastos innecesarios mediante la utilización adecuada de todos los recursos.

El profesional de sistemas debe enterar al cliente o patrón cuando un proyecto propuesto no cumpla con los intereses propios de la organización.

El profesional de sistemas debe enterar al cliente o patrón de cualquier riesgo asociado con el desarrollo de un proyecto que pudiera impactar el costo, tiempo de entrega o calidad, para documentar las acciones requeridas para minimizar su impacto en caso de que ocurra.

El profesional de sistemas no debe aceptar trabajos en los que no se sienta competente para realizarlos a un nivel razonable de satisfacción del cliente. No olvidar en ningún momento que la satisfacción del cliente es lo más importante.

Asegurarse del buen uso de los recursos informáticos, evitando desperdiciarlos y gastarlos en formas para las que no fueron planeadas y autorizadas.

La actitud del profesional de sistemas siempre debe ser en forma proactiva para ver más allá de los proyectos que estén a su cargo y buscar mejores soluciones.

Responsabilidad Profesional

El profesional de sistemas expresará su opinión en los asuntos que se le hayan encomendado, teniendo en cuenta los lineamientos expresados en éste código y una vez que haya dado cumplimiento a las normas profesionales emitidas por la organización, que sean aplicables para la realización del trabajo.

Ningún profesional de sistemas que actúe independientemente permitirá que se utilice su nombre en relación con proyectos de información o estimaciones de cualquier índole, cuya realización dependa de hechos futuros, en tal forma que induzcan a creer que el profesional de sistemas asume la responsabilidad de que se realicen dichas estimaciones o proyectos.

El profesional de sistemas deberá puntualizar en qué consistirán sus servicios y cuáles serán sus limitaciones. Cuando en el desempeño de su trabajo el profesional se encuentre en alguna circunstancia que no le permita seguir desarrollando su labor en la forma originalmente propuesta, deberá comunicar ésa circunstancia a su cliente de manera inmediata.

Deberá ser objetivo e imparcial en la emisión de sus opiniones o juicios, buscando siempre el beneficio de sus clientes.

Derechos de Autor

El profesional de sistemas respetará el reconocimiento que hace el estado a favor de todo creador o desarrollador de programas de cómputo, en virtud del cual otorga su protección para el autor.

Cuando se presten los servicios en modo independiente, el profesional de sistemas deberá establecer en el contrato de servicios, quien será el poseedor de los derechos de autor sobre los programas desarrollados.

Cuando se trabaje de planta para un patrón, éste último tendrá los derechos de autor sobre todo el software que se desarrolle para su empresa, quedando el profesional de sistemas imposibilitado a comercializar dichos programas.

Cuando el profesional de sistemas sea el titular de los derechos de autor sobre un programa de computación, tendrá el derecho de autorizar o prohibir el arrendamiento o la venta de sus ejemplares.

El profesional de sistemas podrá tener acceso a la información de carácter privado relativa a las personas, contenida en las bases de datos, previa autorización de las personas de que se trate, excepto cuando se requiera una investigación de carácter legal.

Discreción Profesional

El profesional de sistemas tiene la obligación de guardar discreción en el manejo de la información que la empresa para la cual trabaje le proporcione al momento de prestar sus servicios. Considerar como confidencial toda la información acerca del negocio de su cliente o patrón. Asegurarse de que se guarde la confidencialidad de la información que le ha sido confiada.

El profesional de sistemas no debe permitir el acceso a la información a personal no autorizado, ni utilizar para beneficio propio la información confidencial de la empresa.

El profesional de sistemas podrá consultar o cambiar opiniones con otros colegas en cuestiones de criterio o de doctrina, pero nunca deberá proporcionar datos que identifiquen a las personas o negocios de que se trate, a menos que sea con consentimiento de los interesados.

Honestidad Profesional

El profesional de sistemas no debe cambiar, modificar o alterar la información de la empresa, para beneficio propio o de terceros, ni con fines de encubrir anomalías, fraudes o corrupción de otros

funcionarios cuando sean afectados directamente los intereses de la empresa.

El profesional de sistemas no debe participar en la planeación o ejecución de actos que puedan calificarse de deshonestos, o que originen o fomenten la corrupción en cualquiera de sus formas.

El profesional de sistemas no aceptará comisiones ni obtendrá ventajas económicas directas o indirectas por la recomendación que haga de servicios profesionales o de productos a la empresa, institución o dependencia a la que presta el servicio.

Lealtad hacia la Empresa a la que se le da Servicio

El profesional de sistemas se abstendrá de aprovecharse de situaciones que puedan perjudicar a quien haya contratado sus servicios y observará el principio del secreto profesional.

Siempre que el profesional de sistemas trabaje para un cliente o patrón y que tenga la oportunidad de realizar trabajos profesionales con otros clientes deberá informar a su patrón original. En caso de tener contrato de planta deberá además cuidarse de no apoyar profesionalmente directa ni indirectamente a los competidores de su patrón.

El profesional de sistemas no deberá ofrecer trabajos directa o indirectamente a funcionarios o empleados de sus clientes, si no es con previo consentimiento del mismo.

El profesional de sistemas en el desarrollo independiente de la profesión se abstendrá de ofrecer sus servicios a clientes de otro colega. Sin embargo, tiene derecho a realizar propaganda y competencia por los distintos medios de difusión expresando los servicios que ofrece y si algún cliente que solicita sus servicios esta siendo atendido por otro colega, se debe de sugerir la continuación con el colega o la ruptura de ésa relación, de tal manera que el cliente solo sea atendido por uno de ellos sobre una misma tarea.

Tratándose de asociaciones profesionales, no podrán los socios contraer o hacer trabajos profesionales por su cuenta, sin el consentimiento de los demás socios.

No Beneficiarse de las Compras del Patrón

El profesional de sistemas no debe obtener beneficio económico alguno directo o indirectamente cuando lleve a cabo la realización de actividades propias de su profesión dentro de la organización para la que presta sus servicios.

Cuando el profesional de sistemas preste sus servicios a una empresa o institución como empleado de planta no podrá buscar su beneficio personal en las compras de equipo y programas realizadas bajo su responsabilidad.

El profesional de sistemas no debe ceder a estrategias de soborno por parte de proveedores. No debe realizar o dar consejo al cliente o patrón para desarrollar una compra en la cual se pueda ver beneficiado económicamente algún familiar, a menos que sea con el conocimiento expreso del cliente o patrón.

No Usar Equipo ni Programas del Cliente o Patrón para Beneficio Personal

Cuando el profesional de sistemas requiera utilizar los equipos de cómputo o programas, propiedad del cliente o patrón para el que se prestan los servicios, para uso personal o de beneficio propio, debe consultar primeramente al propio cliente o patrón y obtener su autorización expresa para tal fin.

El profesional de sistemas no debe usar el equipo propiedad del cliente o patrón para fines de esparcimiento, aún cuando tenga autorización para utilizar el equipo. Ni fomentar que personas ajenas a la organización ingresen a las instalaciones y utilicen el equipo y los programas del software.

Trato Adecuado y Manejo del Lenguaje Apropiado

El profesional de sistemas debe tratar a todas las personas justamente sin tener en cuenta raza, religión, sexo, orientación sexual, edad o nacionalidad.

El profesional de sistemas debe dar a sus colaboradores el trato que les corresponde como profesionales y vigilará su adecuado entrenamiento, superación y justa retribución.

El profesional de sistemas no debe intentar confundir o engañar al cliente con comentarios técnicos mal fundamentados respecto a los sistemas computacionales, para lograr beneficio propio o enmendar fallas o errores propios.

Finalización de Servicios

Al finalizar un proyecto de sistemas, el profesional de sistemas debe cumplir con todos los requisitos de funcionalidad, calidad y documentación pactados inicialmente, a fin de que el cliente pueda obtener el mayor beneficio en la utilización de los mismos.

Al dejar la empresa para la cual se prestaban los servicios, el profesional de sistemas debe cuidar que el equipo de cómputo y los programas propiedad de la empresa se conserven en buen estado para su uso y aprovechamiento.

Al concluir el trabajo para el cual fue contratado, el profesional de sistemas debe implantar los mecanismos necesarios, para que el cliente este en posibilidad de continuar haciendo uso de los programas de aplicación, modificaciones o novedades que hubiere realizado a los mismos, a pesar de la ausencia del profesional de sistemas.

Dependencia Tecnológica

El profesional de sistemas debe evitar en todo momento generar una dependencia tecnológica con el cliente o patrón siguiendo estándares de desarrollo de software adecuados al cliente u organización para la cual se prestan los servicios.

Se debe apegar a unos estándares de análisis, diseño y programación de sistemas, para facilitar en todo momento la comprensión por parte de terceros, de su participación en el desarrollo de un sistema.

Desarrollo de Sistemas

El profesional de sistemas debe determinar perfectamente el alcance del proyecto y los requerimientos necesarios para su desarrollo.

El profesional de sistemas debe comunicar en tiempo los procedimientos a seguir para evaluar los requerimientos del cliente.

El profesional de sistemas debe utilizar estándares de desarrollo que garanticen en todo momento un desarrollo de software con la más alta calidad de software, para reforzar la calidad de vida del cliente u organización.

El profesional de sistemas debe determinar de manera clara los entregables de las diferentes etapas de desarrollo y establecer las fechas y compromisos formales de entrega, tanto por su parte como por la de los responsables involucrados del cliente.

El profesional de sistemas debe llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado que permita tomar decisiones.

El profesional de sistemas debe dejar siempre documentado todo sistema desarrollado para una empresa, con todo detalle necesario de tal manera que con su consulta se conozca el funcionamiento de cualquier procedimiento o programa El profesional de sistemas no debe realizar cambios en los procesos o programas sin antes obtener la autorización del cliente o los responsables designados por parte del cliente para el desarrollo del sistema.

El profesional de sistemas debe estar dispuesto a escuchar las peticiones de los usuarios y atender sus requerimientos sin menos preciar su falta de conocimientos en el ámbito de sistemas computacionales.

El profesional de sistemas debe observar los preceptos generales de calidad y las normas establecidas por la propia organización al respecto, en el desempeño de sus actividades y tenderá a la búsqueda continua por la excelencia en la aplicación de sus conocimientos profesionales.

El profesional de sistemas debe de tener la capacidad suficiente para reconocer sus fallas en las revisiones, hacer correcciones y aclarar las dudas del cliente, así como hacerle ver al cliente de manera cortés sus fallas, errores y proporcionar posibles alternativas de solución.

El profesional de sistemas debe comunicar los problemas que se le vayan presentando con los empleados del cliente que intervengan en el proyecto, a los directivos de la institución con la finalidad de evitar problemas a tiempo.

El profesional de sistemas debe utilizar una metodología de software para el desarrollo de su proyecto y generar la documentación con la más alta calidad que facilite al cliente o patrón el mantenimiento de los mismos.

IV. Responsabilidad hacia la Profesión

Respeto a los Colegas y a la Profesión

Todo profesional de sistemas cuidará las relaciones que sostenga con sus colaboradores, colegas e instituciones buscando el enaltecimiento de la profesión, actuando con espíritu de grupo y trabajo en equipo.

El profesional de sistemas deberá cimentar su reputación en la honestidad, honradez, lealtad, respeto, laboriosidad y capacidad profesional, observando las reglas de ética más elevadas en sus actos y evitando toda publicidad con fines de lucro o auto-elogio.

Buscará pertenecer a un Organismo Colegiado que cuente con un Código de Ética que se haga respetar y cumplir; en caso de no existir cuerpos colegiados de informática en su localidad, fomentar su creación y posteriormente la adopción de un código de ética.

Imagen de Calidad

El profesional de sistemas debe esforzarse por mantener una imagen positiva y de prestigio para quien lo patrocine y ante la sociedad en general, fundamentada en su calidad profesional e individual.

Difusión y Enseñanza de Conocimientos

Todo profesional de sistemas debe mantener altas normas profesionales y de conducta al momento y especialmente al transmitir sus conocimientos; así como contribuir al desarrollo y difusión de los conocimientos de la profesión.

Respeto a los Derechos de Autor

El profesional de sistemas reconoce los derechos de autor sobre todos los programas de aplicación, desarrollados por colegas o

empresas afines y se compromete a protegerlos y evitar que otros hagan uso de los mismos sin antes haber pagado por tales derechos.

Especialización Profesional

El profesional de sistemas debe tener una orientación hacia cierta rama de la informática, computación o sistemas computacionales, debiéndose mantener a la vanguardia en esa área del conocimiento de su particular interés.

Competencia Profesional

Es obligatorio para el profesional de sistemas mantener actualizados todos los conocimientos inherentes a las áreas de su profesión así como participar en la difusión de estos conocimientos a otros miembros de la profesión.

El profesional de sistemas debe informarse permanentemente sobre los avances de la informática, la computación y los sistemas computacionales además de invertir los recursos necesarios para su capacitación y formación profesional y personal.

Evaluación de Capacidades

El profesional de sistemas debe autoevaluarse periódicamente con la finalidad de determinar si cuenta con los conocimientos, tiempo y recursos que requiere su cliente.

En caso de que el profesional de sistemas tenga empleados a su cargo deberá asegurarse de que las capacidades técnicas de sus empleados o subordinados sean evaluadas periódicamente, al mismo tiempo que se debe asegurar de que cuentan con un código de ética como el presente.

Reconocimiento a la Colaboración Profesional

El profesional de sistemas al consultar a otro colega estará consciente del esfuerzo, trabajo y recursos que su colega ha dedicado al dominio de los diferentes programas y equipos de cómputo, estando dispuesto en todo momento a retribuir los honorarios adecuados por la asesoría solicitada.

Honorarios

El profesional de sistemas debe ser capaz de practicar un procedimiento para costear sus proyectos que le permitan con seguridad establecer sus honorarios sin necesidad de hacer cambios posteriores.

El profesional de sistemas debe establecer cuotas justas al fijar sus honorarios y debe respetarlos una vez que fueron acordados con sus clientes. Debe de establecer perfectamente el tiempo y la forma de pago.

El profesional de sistemas debe evitar establecer honorarios por debajo de los costos reales por el simple hecho de ganar un proyecto con conocimiento personal de que no es factible su cumplimiento.

Personal a sus Servicios

El profesional de sistemas debe realizar una supervisión del desempeño del personal que colabore con él en el desarrollo de proyectos.

El profesional de sistemas debe hacerse totalmente responsable del personal que colabore con él en el desarrollo de proyectos, cuando tal personal no sea del cliente.

Conflicto de Intereses en la Profesión

El profesional de sistemas debe evitar el recibir favores de los clientes a cambio de beneficiarlos en forma personal con tratos preferenciales a futuro.

El profesional de sistemas debe evitar cualquiera de las acciones siguientes: establecer relaciones sentimentales con los clientes, influir en los clientes para que tomen decisiones que posteriormente lo beneficien personalmente, el acoso hacia él o hacia el cliente, influir en crear u otorgar puestos que puedan ser ocupados por sus familiares o amigos dentro de la organización del cliente.

V. Del Profesional de Sistemas como Catedrático

Práctica Docente

El profesional de sistemas debe considerar al alumno como su cliente y considerarlo como su objetivo principal en su práctica docente. El profesional de sistemas que imparte cátedra debe orientar a sus alumnos para que en un futuro ejercicio profesional actúen con estricto apego a las normas de ética profesional.

Es obligación del profesional de sistemas catedrático mantenerse actualizado en las áreas de su ejercicio, a fin de transmitir al alumno los conocimientos más avanzados de las materias existentes en teoría y práctica.

El profesional de sistemas debe fomentar el estudio y la investigación así como la integración del alumno en grupos de trabajo que le permita el crecimiento y desarrollo personal, social y profesional.

El profesional de sistemas debe hacer público el temario que se va a desarrollar durante el tiempo que dure la enseñanza así como los procedimientos de evaluación.

Relación con los Alumnos

El profesional de sistemas debe dar a sus alumnos un trato digno y respetuoso, instándolos permanentemente a su constante superación personal y profesional.

El profesional de sistemas debe entender que la única diferencia con él es la formación y habilidad en determinadas áreas para lo cual el educando acude a capacitarse.

El profesional de sistemas debe abstenerse de hacer comentarios que perjudiquen la reputación o prestigio de alumnos, catedráticos, otros profesionales de sistemas y profesionistas en general.

El profesional de sistemas debe evitar hacer comentarios alabadores a los alumnos sobresalientes con el objetivo de agredir o hacer sentir mal al resto de los alumnos.

Es necesario que el profesional de sistemas maneje una conducta de respeto hacia el alumno y de esta manera pueda exigir respeto también de éste.

El profesional de sistemas debe evitar hacer comentarios que deterioren la autoestima del alumno con problemas de aprendizaje. Debe de evitar la intimidación del alumno.

El profesional de sistemas debe buscar procedimientos para comunicarse con los alumnos cuando no pueda asistir a clases.

Relación con la Institución Educativa

En sus relaciones con la administración o autoridades de la institución en la que ejerza como catedrático, deberá ser respetuoso de la disciplina prescrita, así como mantener una posición de independencia mental y espíritu crítico en cuanto a la problemática que plantea el desarrollo de la informática, la computación y los sistemas computacionales.

El profesional de sistemas debe comunicar los problemas que se le vayan presentando con los alumnos a los directivos de la institución con la finalidad de evitar los problemas a tiempo.

Discreción como Catedrático

El profesional de sistemas podrá referirse en sus clases a casos reales para ilustrar los conocimientos que imparta, pero se abstendrá de proporcionar información que identifique a personas, empresas o instituciones relacionadas con dichos casos, salvo que los mismos sean del dominio público.

Evaluación de Capacidades Docentes

El profesional de sistemas debe evaluarse periódicamente con la finalidad de determinar si cuenta con los conocimientos y habilidades que requiere la práctica docente.

Cumplimiento de Obligaciones

Es responsabilidad del profesional de sistemas cumplir con el tiempo convenido para asistir oportunamente y con la frecuencia requerida a desarrollar su práctica docente.

El profesional de sistemas debe predicar con el ejemplo y cumplir con su responsabilidad en asistencia, puntualidad en el salón de clases y tiempo establecido de clase diario.

El profesional de sistemas debe contar, si es permitido por la Institución educativa, con un profesor adjunto con la misma capacidad para que lo sustituya cuando sea inevitable la inasistencia.

Evaluaciones a los Alumnos

El profesional de sistemas debe comunicar en tiempo los procedimientos de evaluación y la conducta a seguir durante el tiempo que dure la enseñanza.

El profesional de sistemas debe exigir la asistencia continua del alumno en la misma forma que a él se le exige.

El profesional de sistemas debe llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado, así como también hacer una revisión total del examen y aclarar todas las dudas que resulten derivadas de su aplicación.

El profesional de sistemas debe tener la capacidad suficiente para reconocer sus fallas en las revisiones, hacer correcciones y aclarar las dudas del alumno si es posible hasta en forma personal pero siempre dentro del salón y con conocimiento de los presentes o de las autoridades educativas.

El profesional de sistemas debe evitar hacer convenios particulares en los que se vean favorecidos solo unos cuantos alumnos.

El profesional de sistemas debe llevar una supervisión del desempeño del alumno en forma personal preocupándose por establecer si los bajos resultados son producto del desempeño del alumno o del maestro.

Conflicto de Intereses en la Práctica Docente

El profesional de sistemas debe evitar el recibir favores de los alumnos a cambio de beneficiarlos en forma personal con calificaciones, justificaciones de faltas de asistencia y omisión de trabajos.

El profesional de sistemas debe evitar el establecimiento de relaciones sentimentales con los alumnos.

El profesional de sistemas debe evitar influir en los alumnos para que tomen decisiones que posteriormente lo beneficien personalmente.

El profesional de sistemas debe evitar el acoso hacia los alumnos. En el caso de que se encuentren familiares o amigos entre los alumnos, el profesional de sistemas debe tratarlos como si la afinidad no existiera ya que como alumnos todos deberán de disfrutar de los mismos derechos y obligaciones.

VI. Uso de Internet

Normas Generales para su Uso

Es obligación imperativa e ineludible del profesional en sistemas, proceder en todas las ocasiones que navegue en Internet portarse con honor y dignidad, ajustándose a la más estricta moralidad, velando por el prestigio personal y decoro profesional y actuando con decencia en todos los casos.

Por el prestigio y buen uso de Internet, el profesional de sistemas debe observar las reglas de este Código de Ética cuyas infracciones, por considerarse actos indignos y punibles, serán actos reprobatorios. Es obligación del profesional de sistemas fomentar y hacer que los usuarios de la red cumplan estas mismas normas, para evitar que la Internet pierda prestigio.

Creación y Uso de Páginas en Internet

El profesional de sistemas entiende que son actos contrarios a este Código de Ética los siguientes:

Navegar en Internet en páginas contrarias a las buenas costumbres, como son páginas pornográficas y páginas con contenido insano, entre otras.

Crear páginas de Internet sabiendo que contienen mentiras, falsedades, que se realizan con dolo y hacer creer a los usuarios que lo que contienen en verídico.

Dejar páginas en Internet abandonadas sin cumplir con lo que se promete en ellas.

Crear páginas con mala promoción a terceras personas ya sean físicas o morales, con el fin de perjudicarlos.

Ofrecerse para el desempeño de especialidades y funciones para las cuales no se tenga capacidad, preparación y experiencia razonables.

Crear páginas con virus para que al momento de bajar algún archivo éste sea enviado al usuario.

Comercializar el software libre en Internet.

Leer, modificar, borrar o dañar información de otros usuarios con dolo o en forma accidental.

Establecer ligas a páginas sin estar debidamente autorizado a hacerlo y cumpliendo con los derechos de autor involucrados en dichas ligas.

Correo Electrónico

El profesional de sistemas entiende que son actos contrarios a este Código de Ética los siguientes:

Enviar correos electrónicos conteniendo injurias, falsedades y malas palabras aunque el usuario sea de mucha confianza.

Enviar correos electrónicos sin remitente y sin asuntos.

Enviar por correos electrónicos virus, archivos o información que vaya en contra de las buenas costumbres.

Enviar correos electrónicos SPAM a los usuarios.

Enviar a través de correo electrónico publicidad no solicitada por el usuario.

Enviar correos electrónicos haciéndose pasar por otra persona.

Solicitar el correo electrónico de una persona con la finalidad de enviarle por una sola vez información solicitada y posteriormente enviarle información no solicitada.

Enviar correos electrónicos a los contactos de otros usuarios sin su autorización expresa.

Usar el correo electrónico de la empresa en la que labore para asuntos personales sin contar con previa autorización de hacerlo.

APÉNDICE III

Reporte Final del Caso Práctico

A continuación se presenta el contenido del reporte final por parte de los auditores en donde se indican los hallazgos encontrados y las recomendaciones hechas a las revisiones de los sistemas de información

Agenda

- Objectives
- Scope
- Review Team
- Summary
- Executive Overview

Objectives

- To confirm compliance with ITCS104 Corporate Standards requirements.
- To identify process deficiencies.
- To recommend solutions.
- To ensure that root cause analysis is done, investigated and determined.
- To implement the improvements defined

Scope

The review is based on:

- **ITCS104:** Information Technology Security Standards in Distribuited Services
- **Corporate Audit Program:** 42-00-00

Review Team

- Team Leader Auditor

- Team Member Auditor 1

- Team Member Auditor 2

- Team Member Auditor 3

- Team Member Auditor 4

Summary

Item	Comments
Distributed Services	Annual Revalidation of Continuos Business Need (affirmative confirmation concept), Quarterly Employment Review, Userid Administration process must be improved in order to reflect the new ITCS104 version. Systematic Attack Detection process must be reviewed and improved.

Executive Overview

Distributed Environment

DS - Process Documentation and Implementation

- 1.1 Identification
  - *1.1.1 Identification*
    - *Userids are being shared*
      - *159 of 278 userids on server 1 are shared*
  - *1.1.2 Employment Verification*
    - *Compliant (in the scope reviewed)*
  - *1.1.3 Registration*
    - *Divergences were detected between MAD and CEP registers.*
    - *Servers are classified as ITCS104 Departmental and development Susytems however are applied ITCS104 Business Unit Production System controls:*
      - *Server 2*
      - *Server 3*
      - *Server 4*
      - *Server 5*
- 1.2 Authentication
  - *Compliant (in the scope reviewed)*

DS - Process Documentation and Implementation

- 1.3 Authorization
  - *1.3.1 Access Authorization*
    - *Applications system owner are not informed when a new userid is created and the access is through operational system*
    - *The user's manager does not confirm the access removal of his employees*
    - *The Annual Revalidation of Continued Business Need process could be improved*
      - *Wrong "affirmative confirmation" concept is being applied.*
      - *If manager no answer until target date the userid is revalidated, however it must be cancelled.*
  - *1.3.2 Remote Access for Employees*
    - *Compliant (in the scope reviewed)*
  - *1.3.3 Business Use Notice*
    - *Compliant (in the scope reviewed)*
  - *1.3.4 User Resources*
    - *Compliant (in the scope reviewed)*

DS - Process Documentation and Implementation

- 1.4 Information Protection and Confidentiality
  - *1.4.1 Information Protection*
    - *Compliant (on the scope reviewed)*
  - *1.4.2 Residual Information*
    - *Compliant (on the scope reviewed)*
  - *1.4.3 Encryption*
    - *Compliant (in the scope reviewed)*
- 1.5 Service Integrity and Availability
  - *1.5.1 Operating System Resource Management*
    - *Compliant (in the scope reviewed)*
  - *1.5.2 System and Security Administrative Authority*
    - *A process must be in place for changing all passwords when system administrator is changed.*
  - *1.5.3 Harmful Code*
    - *Compliant (in the scope reviewed)*
  - *1.5.4 Vulnerability Scanning*
    - *Compliant (in the scope reviewed)*
  - *1.5.5 Security Advisory Patch Management*
    - *If an APAR will be not applied in the timeframe required, uncomplete information is delivery to Business Process Owner*
      - *Only delay is informed. Risk is not informed.*

DS - Process Documentation and Implementation

- *1.5.6 Software Modification*
  - *Compliant (in the scope reviewed)*
- *1.5.7 Service Availability Management*
  - *Denial of Services*
    - *Compliant (in the scope reviewed)*
  - *Systematic Logon Attacks*
    - *The current "Systematic Attacks" definition must be improved.*
    - *Only Invalid Logon Attempts are analized and controlled*
    - *There is not a clear definition for analyzing Invalid Logon Attempts regarding*
      - *network environment*
      - *site environment*
      - *So, potential Systematic Logon Attack are not inmediately detected and reported*
    - *Adequated threshold must be defined for access attempts not authorized*
  - *Server and Services Activation*
    - *The process of migration/upgrade of operating system of a server is not defined/documented.*
      - *server 6 has a cirats and evidences of vulnerability scan, health checking, change record.*
      - *server 7 has not a cirats or evidences of vulnerability scan, health checking, change record.*
  - *Client and Server Services*
    - *server 8 allow unrestricted access to intranet*

DS - Process Documentation and Implementation

- 1.6 Activity Auditing
  - *Compliant (in the scope reviewed)*
- 1.7 Assurance
  - *1.7.1 Health Checking*
    - *Security Health Checking template for OS/400 does not cover all items in OS/400 Technical Specifications .*
  - *1.7.2 Security Technical Testing*
    - *Compliant (in the scope reviewed).*
    - *Are performed from Brazil by Auditor 5.*
  - *1.7.3 Security Process Review*
    - *Corresponding to this review.*

DS - Process Documentation and Implementation

- 1.8 Security Incidents
  - *1.8.1 Reporting Security Incidents*
    - *Review the process in order to be aligned with Systematic Attack process.*
  - *1.8.2 Report Access Violations - Invalid Logons*
    - *No exaustive analysis is made when invalid logon are detected (See SAD process)*
  - *1.8.3 Misuse of Authority*
    - *Compliant (on the scope reviewed).*

DS - Process Documentation and Implementation

- 1.9 Physical Access Controls of Storage Media
  - *1.9.1 Physical Protection of Storage Media*
    - *Compliant (in the scope reviewed).*
  - *1.9.2 Physical Protection and Inventory Control of Storage Media*
    - *Compliant (in the scope reviewed).*

GLOSARIO DE TÉRMINOS

- A -

Address (dirección)

El término "address" se utiliza en Internet para referirse a la serie de caracteres numéricos o alfanuméricos, que identifican un determinado recurso de forma única y permiten acceder a él. En la red existen varios tipos de dirección de uso común: "dirección de correo electrónico" (e-mail address); "dirección IP" (internet address).

ADSL (Asymmetrical Digital Subscriber Line – Línea de Suscripción Asimétrica Digital)

Tecnología de transmisión que permite a los hilos telefónicos de cobre convencionales transportar hasta 9 Mbps (megabits por segundo) mediante técnicas de compresión.

Agent (agente)

En el modelo cliente-servidor, el agente es la parte del sistema que realiza la preparación e intercambio de información por cuenta de una aplicación del cliente o del servidor.

Ancho de banda (bandwith)

Es la propiedad fundamental de los canales de transmisión de datos y determina la velocidad con la que estos viajan por la red. Técnicamente es la diferencia en hertz (Hz) entre la frecuencia más alta y la más baja de un canal de transmisión. Habitualmente se usa para definir la cantidad máxima de datos que puede ser enviada en un período de tiempo (segundo) a través de un circuito de comunicación dado. En este caso en bps (bits por segundo) u otra unidad similar.

Anonymous FTP (FTP anónimo)

El FTP anónimo permite a un usuario de Internet la captura de documentos, ficheros, programas y otros datos contenidos en archivos existentes en numerosos servidores de información sin tener que proporcionar su nombre de usuario y una contraseña (password). Utilizando el nombre especial de usuario "anonymous", o a veces "ftp", el usuario de la red podrá superar los controles locales de seguridad y acceder a ficheros situados en un sistema remoto.

Applet (aplicación, aplique)

Pequeña aplicación (programa) escrita en Java, asociada normalmente a una página web, que se difunde a través de la red y se ejecuta en el navegador cliente.

Application (aplicación)

Un programa que lleva a cabo una función directamente para un usuario. WWW, FTP, correo electrónico y Telnet son ejemplos de aplicaciones en el ámbito de Internet.

Archive site (sitio de archivo)

Ordenador conectado a Internet que permite el acceso de los usuarios a una colección de ficheros en él almacenados. Un "anonymous FTP archive site", por ejemplo, permite el acceso a dicho material mediante el protocolo FTP. Los servidores WWW pueden también actuar como lugares de archivo.

Archivo (fichero, file)

Unidad significativa de información que puede ser manipulada por el sistema operativo de un computador. Un fichero tiene una identificación única formada por un "nombre" y una "extensión", en el que el nombre suele ser de libre elección del usuario y la extensión suele identificar el contenido o el tipo de fichero (usualmente viene dado por la aplicación que se utilizó para crear el archivo). Así, en el fichero prueba.txt el apellido "txt" señala que se trata de un fichero que contiene texto plano. En la estructura arborescente con la que se estructuran los contenidos de un computador, los archivos se ubican dentro de directorios.

ARPA (Advanced Research Projects Agency – Agencia de Proyectos de Investigación Avanzada)

Nombre actual del organismo militar norteamericano anteriormente llamado DARPA. Dicha agencia creó la red ARPANET, origen de Internet.

ARPANET (Advanced Research Projects Agency Network – Red de la Agencia de Proyectos de Investigación Avanzada)

Red pionera de larga distancia financiada por ARPA (antigua DARPA). Fue desarrollada a principios de la década de los sesenta y se convirtió en la base de la investigación sobre redes y el eje central de éstas durante el desarrollo de Internet. ARPANET estaba constituida por ordenadores de conmutación individual de paquetes, interconectados mediante líneas telefónicas.

ASCII (American Standard Code for Information Interchange – Estándar Americano de Codificación para el Intercambio de Información)

Conjunto de normas de codificación de caracteres mediante caracteres numéricos, de amplia utilización en informática y telecomunicaciones.

ASP (Active Server Pages – Páginas de Servidor Activo)

Ambiente de desarrollo en scripts creado por la empresa Microsoft, cuya particularidad es la de funcionar del lado del servidor, generando en forma dinámica las páginas HTML que sirve. Cuando un usuario solicita un archivo ".asp" en su browser, el servidor interpreta los comandos y genera la página que envía finalmente al usuario. Con este lenguaje, que permite además utilizar VBasic scripts, Javascripts y otros, se crean lo que se ha llamado "sitios dinámicos". Su sencillez de manejo, implementaciones de interactividad y comunicación con bases de datos lo han hecho muy apreciado para desarrollar websites y aplicaciones sobre web.

ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona)

Estándar que define la conmutación de paquetes (cells - celdas o células) de tamaño fijo con alta carga, alta velocidad (entre 1,544 Mbps. y 1,2 Gbps) y asignación dinámica de ancho de banda. ATM es conocido también como "paquete rápido" (fast packet).

Attachment (adjunto, anexo)

Dícese de un fichero o archivo de información digital que es adjuntado a un mensaje de correo electrónico. El fichero puede contener cualquier objeto digitalizado: texto, gráficos, planillas electrónicas, imágenes fijas o en movimiento, sonido. Para su transporte a través de Internet, el fichero debe ser codificado en un formato como el MIME, UUENCODE o Bin-Hex.

Autentificación (authentication)

Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad (por ejemplo: compras electrónicas). También se aplica a la verificación de identidad de origen de un mensaje de correo electrónico.

Autopistas de la información (data highway)

Con este término se denomina el conjunto de los servicios de información en línea, BBs y redes como Internet, Compuserve o America On Line. Acuñado en 1994 por el entonces vicepresidente de

los Estados Unidos, Al Gore, el término ha perdido parte de su fuerza para pasar a englobarse dentro de los que el G-7 ha denominado Infraestructura Global de Información (GII en terminología inglesa). Muchos analistas equiparan las autopistas de la información a Internet, la "red de redes", que conecta a 30 millones de usuarios en todo el mundo; a través de Internet empresas, organismos y particulares intercambian información en todo el mundo de manera rápida y sencilla.

- B -

Bajar (download)

Forma metafórica de aludir al traspaso de la información desde algún servidor de Internet hasta el computador propio. Pueden bajarse todo tipo de ficheros tales como programas, sonidos, videos, imágenes, etc.

Baudio (baud)

Del nombre de J.M.E. Baudot. En la transmisión de datos, un baudio es el número de veces que cambia el "estado" del medio de transmisión en un segundo. Por ejemplo, un módem de 14.400 baudios cambia 14.400 veces por segundo la señal que envía por la línea telefónica. Como cada cambio de estado puede afectar a más de un bit de datos, la tasa de bits de datos transferidos (por ejemplo: medida en bits por segundo) puede ser superior a la correspondiente tasa de baudios.

Bcc (copia oculta)

Es una de las líneas que componen la cabecera de un mensaje de correo electrónico y su finalidad es incluir uno o más destinatarios de dicho mensaje cuya identidad no aparecerá en el mensaje recibido por el destinatario o destinatarios principales. Es decir, se crea una "copia oculta" del mensaje. "Bcc" es un acrónimo de la frase inglesa "blind carbon copy" (copia ciega en papel carbón).

Bit (bit)

Del inglés binary digit, "dígito binario". Unidad mínima de información digital que puede ser tratada por un computador, equivalente a una elección binaria: 1 ó 0.

Bps (bits por segundo)

Unidad que mide la capacidad de transmisión de una línea de telecomunicación. Define el número de bits que se transmiten en un segundo.

Bug (error)

Término aplicado a los errores descubiertos al ejecutar un programa informático. Fue usado por primera vez en el año 1945 por Grace Murray Hooper, una de las pioneras de la programación moderna, al descubrir cómo un insecto (bug) había dañado un circuito del ordenador. Hoy en día, muchos programas son creados y puestos a disposición del público en las conocidas versiones beta, para que los propios usuarios detecten los errores.

Buscador (search engine)

Herramienta dedicada a recopilar y estructurar de manera sistemática la información de toda la red, facilitando así la búsqueda de datos por palabras clave. Hay dos tipos básicos: aquellos que entregan resultados a una búsqueda por palabra clave (Lycos o Infoseek) y los que organizan su información temáticamente, por directorios (Yahoo!), aunque muchos de ellos integran ambos tipos. Se presentan con una interfaz web, es decir; son accesibles a través de un navegador y sus resultados pueden seguirse mediante hiperenlaces.

Byte

Conjunto significativo de información digital equivalente a ocho bits que representan un caracter.

- C -

CGI (Common Gateway Interface - Interfaz Común de Intercomunicación)

Conjunto de medios y formatos que permite el intercambio de datos entre el navegador y otros programas residentes en servidores WWW. Por ejemplo, una cgi permite que los datos que un usuario envía a través de un formulario web se almacenen en una base de datos.

Cgi-bin (cgi-bin)

Directorio de un servidor web donde suelen almacenarse los programas CGI. "bin" es una contracción de "binario".

Ciberespacio

Término creado por William Gibson en su novela fantástica "Neuromancer" para describir el "mundo" de los ordenadores y la sociedad creada en torno a ellos. Hoy en día se ha convertido en un término genérico que designa el conjunto de servicios y utilidades que integra la red Internet.

Cliente (client)

Una aplicación cliente es aquella que funciona solicitando procesos o servicios a otra aplicación servidor. Un navegador, al solicita una URL a un servidor web, es un cliente. Los programas cliente se ejecutan siempre sobre una red, bien sea interna o externa.

Comercio electrónico (e-commerce)

Intercambio de bienes y servicios realizado a través de las Tecnologías de la Información y las Comunicaciones, habitualmente con el soporte de plataformas y protocolos estandarizados. Hoy por hoy, el comercio electrónico es una de las utilidades más extendidas de la Internet: de los aproximadamente 40 millones de sitios web existentes en 1998, se calcula que 27 millones son sitios comerciales.

Comunidad virtual

El conjunto de personas que comparten el ciberespacio.

Conmutación de paquetes

La conmutación de paquetes es un sistema de transmisión de datos mediante el cual toda la información que sale de un terminal para ser transmitida por la red es troceada en bloques de una determinada longitud llamados paquetes. A cada paquete se le añade la información necesaria al comienzo del mismo, de manera que cada uno se pueda mover por la red de forma independiente. Si en un momento dado una ruta o un nodo de comunicación queda fuera de servicio, los paquetes son enviados de forma automática por otras rutas, sin que quede interrumpida la comunicación.

Correo electrónico (e-mail)

Aplicación que permite enviar mensajes a otros usuarios de la red sobre la que está instalada. En Internet, el correo electrónico permite que todos los usuarios conectados a ella puedan intercambiarse mensajes. Los programas cliente de correo electrónico incluyen diversas utilidades, normalmente acceso integrado a los servidores de news, y posibilidad de adjuntar todo tipo de archivos a los mensajes.

- D -

Dialup (conexión por línea conmutada)

Conexión temporal, en oposición a conexión dedicada o permanente, establecida entre ordenadores por línea telefónica normal. Dícese también del hecho de marcar un número de teléfono.

Dirección internet (internet address)

Dirección IP que identifica de forma inequívoca un punto de conexión en una red internet. Una dirección Internet (con "I" mayúscula) identifica de forma inequívoca un nodo en Internet.

Dirección IP (IP address)

Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.245. Todo computador que se conecta a Internet posee una dirección IP que lo identifica de forma inequívoca. Esta IP puede ser fija (en el caso de los servidores) o variable (en el caso de los computadores de usuarios, que se conectan sólo temporalmente, su dirección IP es asignada aleatoriamente cada vez que se conecta a Internet). Las direcciones alfanuméricas que solicitamos por ejemplo al navegar (p.e. www.e.cl) son transformadas por el DNS en direcciones IP al transportarse por la red.

DNS (Domain Name System – Sistema de Nombres de Dominio)

El DNS es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP basándose en los nombres de dominio. De este modo, cuando se requiere un servicio de un host concreto (p.e. www.e.cl), el DNS traduce el nombre en la dirección IP asignada a ese servidor. La búsqueda de estas direcciones se realiza de manera jerarquizada, comenzando por los dominios territoriales o genéricos (.cl, .es, .au., .com, .net), y siguiendo por los dominios específicos que definen a cada sistema (por ejemplo, "e").

Dominio

Conjunto de páginas reagrupadas con un mismo nombre.

- E -

EDI (Electronic Data Interchange – Intercambio Electrónico de Datos)

Sistema y protocolos de intercambio de datos a través de la red utilizado sobre todo por empresas, que asegura una mayor privacidad en las transacciones de datos.

Encriptación (encryption)

La encriptación o cifrado es el tratamiento de un conjunto de datos mediante una clave, a fin de impedir que nadie excepto el

destinatario de los mismos pueda acceder a ellos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

Ethernet (Ethernet)

Sistema de red de área local de alta velocidad, que utiliza protocolos TCP/IP, por lo que los computadores conectados a estas redes acceden directamente a Internet a través de ellas. Se ha convertido en un estándar de red corporativa.

Extranet

Modelo de construcción de redes que utiliza la tecnología de Internet para conectar la red local (LAN) de una organización con otras redes (por ejemplo, proveedores y clientes), permitiendo así el intercambio de información y servicios.

- F -

FAQ (Frequently Asked Questions – Preguntas Frecuentes)

Estas siglas significan en español "Preguntas formuladas con frecuencia" o, como es más usado, "Preguntas frecuentes". Sitios web, grupos de noticias o listas de correo mantienen siempre accesible un documento de FAQs para la consulta de los usuarios principiantes, con el fin de ofrecer respuestas rápidas a dudas comunes. La recolección de este conjunto de cuestiones suele realizarse con las contribuciones de los propios usuarios. Son un buen punto de partida para iniciarse en el estudio de algún tema y una base común de conocimientos y discusión para todos sus usuarios.

Firewall (cortafuegos)

Sistema que se coloca entre una red local e Internet. Su función es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc., impidiendo la entrada a usuarios no autorizados.

Formulario (form)

El popular formulario requerido para todo tipo de transacciones burocráticas tiene su reflejo en los sitios web en los “forms”, páginas html con espacios que deben ser completados por el usuario. Cajas de texto, seleccionadores, botones para pulsar son sus componentes habituales, confeccionados normalmente para solicitar información, realizar una inscripción en un servicio o contestar una encuesta.

Freeware (programas de libre distribución)

Software que se distribuye a través de la red de forma gratuita. La eclosión del freeware está íntimamente relacionada con Internet: usualmente estos programas son creados por estudiantes o entidades universitarias, que ponen sus productos en manos de la comunidad informática.

FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos)

Protocolo que permite a un usuario de un sistema acceder a, y transferir desde, otro sistema de la red. A través del FTP se pueden bajar o subir archivos a través de Internet. FTP es también habitualmente el nombre del programa que el usuario invoca para ejecutar el protocolo.

- G -

Gateway (pasarela)

Una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que poseen implementaciones diferentes y son incompatibles entre sí. No debería confundirse con un convertidor de protocolos. Hoy se utiliza el término router (direccionador, encaminador, enrutador) en lugar de la definición original de gateway.

GNU (Gnu's not Unix - GNU no es Unix)

Proyecto creado en 1984 con el fin de desarrollar un sistema operativo tipo Unix según la filosofía del "software libre".

GUI (Graphical User Interface – Interfaz Gráfica de Usuario)

Componente de una aplicación informática que visualiza el usuario y a través de la cual opera con ella. Está formada por ventanas, botones, menús e íconos, entre otros elementos.

- H -

Hardware (equipo físico)

Componentes físicos de un computador o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.

Hiperenlace (hyperlink)

Marcador existente en un documento hipertexto que enlaza éste a otro archivo, que puede ser otro documento hipertexto u otro tipo de archivo (gráfico, video). Llamado también simplemente enlace.

Hipermedia (hypermedia)

Acrónimo de los términos "hipertexto" y "multimedia", que se refiere a las páginas web que integran información en distintos tipos de formato: texto, imágenes, sonidos y vídeo, principalmente.

Hipertexto (hypertext)

Concepto y término inventado por Ted Nelson en 1969. Nelson, un famoso visionario de la informática, investigó durante 25 años las posibilidades de interacción entre las computadoras y la literatura. El concepto alude a un tipo de texto que no posee la linealidad del texto escrito y que permite realizar conexiones creativas (enlaces), entre las distintas partes del mismo o con otros textos. El hipertexto es una forma diferente de organizar información y permite al usuario definir su propio patrón de lectura. Bajo ese concepto nació el lenguaje HTML y la WWW. También los libros electrónicos o enciclopedias multimedias están organizados como hipertextos.

Hop (salto)

Término utilizado para denominar cada uno de los pasos que es preciso dar para llegar de un punto de origen a otro de destino a lo largo de una red con la ayuda de direccionadores (routers).

Host (sistema anfitrión)

Ordenador que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP. La acepción verbal (to host) describe el hecho de almacenar algún tipo de información en un servidor ajeno. Los host son comúnmente llamados servidores.

Hostname (nombre de sistema anfitrión)

Denominación otorgada por el administrador a una computadora. El hostname es parte de la dirección electrónica de esa computadora, y debe ser único para cada máquina conectada a Internet.

HTML (HyperText Markup Language – Lenguaje de Marcado de Hipertexto)

Lenguaje de programación en el que se generan las páginas web, elemento base de la navegación WWW. Nacido como un lenguaje de formateo de texto para su visualización en los navegadores, con el tiempo se ha ido complicando y admitiendo componentes de otros lenguajes (javascript, por ejemplo). El HTML se estructura por medio de etiquetas o tags, que van definiendo los elementos de la página: texto, tablas, enlaces, formularios; o llamando desde el documento a otros archivos conexos (gráficos, audio, video, etc.). La definición del estándar HTML está a cargo del Web Consortium.

HTTP (Hypertext Transfer Protocol – Protocolo de Transferencia de Archivos de Hipertexto)

Protocolo que enlaza, a través de Hipervínculos, las páginas de Hipertexto (HTML) que forman el World Wide Web. El Protocolo HTTP consiste en un conjunto de reglas que se aplican a las peticiones que hace un cliente o navegador y a las respuestas que entrega un servidor. Típicamente se utiliza en la descripción de la dirección en la que se encuentra una página específica (ej: http:\\aquilahosting.com.mx).

- I -

ICANN (Internet Corporation for Assigned Names and Numbers - Corporación Internet para la Asignación de Nombres y Números)

Organismo independiente sin ánimo de lucro creado en 1998 con el objeto de gobernar, entre otras cosas, la asignación de espacio de direcciones IP y la gestión del sistema de asignación de nombres de dominio. Organismo sustituto del IANA.

Interfaz (interface)

Zona de contacto, conexión entre dos componentes de "hardware", entre dos aplicaciones o entre un usuario y una aplicación. En este último sentido, interfaz es la cara visible de los programas, con la cual los usuarios interactúan. Pantallas, íconos, mensajes y lenguajes utilizados forman parte de la interfaz.

Internet

Una internet (con "i" minúscula) es un conjunto de redes conectadas entre sí.

Internet Society (Sociedad Internet)

La Internet Society es una organización profesional sin ánimo de lucro que facilita y da soporte a la evolución técnica de Internet, estimula el interés y da formación a las comunidades científicas y docentes, a las empresas y a la opinión pública, acerca de la tecnología, usos y aplicaciones de Internet y promueve el desarrollo de nuevas aplicaciones para el sistema. Esta sociedad ofrece un foro para el debate y la colaboración en el funcionamiento y uso de la infraestructura global. La Internet Society pública un boletín trimestral (On The Net) y convoca una conferencia anual (INET). El desarrollo de los estándares técnicos de Internet tiene lugar bajo los auspicios de Internet Society con un importante apoyo de la Corporation for National Research Initiatives, mediante un acuerdo de cooperación con la Administración Federal de los Estados Unidos de América. Tiene también una estructura territorial formada por diversos capítulos a nivel nacional y regional.

Internet2

El proyecto Internet2 trata de crear una nueva Internet de mayores y mejores prestaciones en el ámbito de las Universidades Norteamericanas. Fue lanzado en 1996 por un grupo de dichas Universidades con la colaboración del Gobierno Federal y de importantes Empresas del sector de la Informática y las Telecomunicaciones.

Internet

Internet es la mayor red de interconexión de redes del mundo. Tiene una jerarquía de tres niveles formados por redes de eje central (backbones como, por ejemplo, NSFNET y MILNET), redes de nivel intermedio y redes aisladas (stub networks). Internet es una red multiprotocolo, que permite a todos sus usuarios la utilización de sus servicios (World Wide Web, correo electrónico, grupos de noticias, etc.), por medio de la simple conexión a uno de los millones de servidores que proporcionan acceso a la red.

Intranet

Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. La utilización de las tecnologías Internet en una red corporativa permite crear un sitio de intercambio de información y comunicación accesible a todos los usuarios con unos simples navegadores y programa de correo electrónico. Este sitio puede tener una parte pública y otra privada, exclusiva para el personal de la

organización. Cuando una Intranet se conecta a través de Internet con las redes de otras compañías, se conoce como Extranet.

IP (Internet Protocol - Protocolo Internet)

El IP, Protocolo de Internet, provee los procedimientos y reglas que definen la transmisión de paquetes de datos, es decir; la fragmentación y el ruteo (medio de encaminar los paquetes) de los datos a través de la red. La versión actual es IPv4 mientras que en Internet2 se intenta implementar la versión 6 (IPv6), que permite mejores prestaciones dentro del concepto QoS (Quality of Service -. Servicios de Calidad). Frecuentemente se usan las siglas IP para referirse al número o la dirección IP.

IP dinámica (dynamic IP)

Se llama IP dinámica al número IP que es asignado en forma aleatoria a un computador cuando se conecta a su proveedor ISP. Todo proveedor dispone de un rango de números IP que otorga dinámicamente a sus usuarios de servicio dial-up, mientras que los servidores de Internet disponen de IP fija.

ISP (Internet Service Provider - Proveedor de Servicios Internet)

Organización, habitualmente con carácter comercial, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece otros servicios relacionados, por ejemplo hospedaje de páginas web, consultoría de diseño e implantación de webs e Intranets.

- J -

Java

Lenguaje de programación desarrollado por Sun Microsystems, orientado a objetos y similar al C++, que se utiliza sobre todo para la elaboración de aplicaciones exportables a la red (applets). Estos programas se asocian a páginas web y se descargan automáticamente con la página para ejecutarse después en el computador local. Las características más reseñables de este lenguaje son las implementaciones de seguridad y su operabilidad sobre cualquier plataforma. Los programas de Java enriquecen las posibilidades de las páginas web y permiten agregar animación e interactividad.

JavaScript

Lenguaje de programación desarrollado por Netscape. Aunque es parecido a Java, se diferencia de él en que los programas están incorporados dentro del documento HTML. Por ello, la ejecución de los

programas (que la realiza el mismo navegador) es más rápida y menos segura.

- K -

KB

Abreviatura de kilobyte, unidad de medida equivalente a mil bytes.

- L -

LAN (Local Area Network - Red de Área Local)

Red de datos para interconectar los computadores de un área de trabajo reducida (una oficina, un edificio o, a lo máximo, varias sedes repartidas en unos pocos kilómetros cuadrados). Por ser redes de pequeña extensión, los protocolos de señal pueden optimizarse para llegar a velocidades de transmisión de hasta 100 Mbps (100 megabits por segundo).

Línea dedicada

Medio de conexión a Internet, con acceso las 24 horas, a través de un cable. Habitualmente se contrata una línea dedicada o en renta para conectar redes de área local (LAN) a un proveedor de servicios de Internet.

Linux

Sistema Operativo de libre distribución similar al UNIX, con la peculiaridad de que puede ser instalado en un computador personal. Fue desarrollado por Linus Torvald, y hoy es muy utilizado para la configuración de servidores de Internet.

Log

Archivo que registra movimientos y actividades de un determinado programa (log file). En un servidor web, se encarga de guardar todos los requerimientos (“requests”) y servicios entregados desde él, por lo que es la base del software de estadísticas de visitas.

- M -

Mbps (megabits por segundo)

Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por un millón de bits.

MIME (Multipurpose Internet Mail Extensions - Extensiones Multipropósito del Correo Internet)

Conjunto de especificaciones Internet de libre distribución que permiten tanto el intercambio de texto escrito en lenguajes con diferentes juegos de caracteres como el envío de ficheros adjuntos entre ordenadores y aplicaciones que sigan los estándares de correo Internet. Más moderno que su antecesor, UUEncoding, admite incluso el formateo del mensaje. Las especificaciones MIME se encuentran recogidas en numerosos RFCs, entre ellos los RFC1521 y 1848.

Mirror (réplica)

Servidor Internet cuyo contenido es una réplica exacta de otro servidor o de parte de él. Normalmente este tipo de servidores cuentan con la aprobación del servidor original y sirven para reducir el tiempo de acceso del usuario a servidores situados en lugares muy distantes.

Modelo cliente/servidor (client/server Model)

Modelo según el cual una aplicación está dividida en dos partes, un programa cliente y un programa servidor. El primero obtiene datos del segundo, sin necesidad de que ambos se estén ejecutando en el mismo ordenador. Es la tecnología que utilizan la mayor parte de las aplicaciones sobre Internet.

Módem (modem)

Acrónimo de modulador/demodulador. Designa al componente de hardware que convierte las señales digitales en analógicas y viceversa, para su transmisión de computador a computador a través de una línea telefónica. La velocidad del módem se mide en una unidad llamada baudios (bits por segundo), por ejemplo 28,800 baudios, que define la cantidad de datos capaz de transmitir en una fracción de tiempo.

Modulación

Proceso de tratamiento de la información que realizan los módems para transformarla en señal analógica, con el fin de poder ser transmitida a través de líneas telefónicas.

Multimedia

Se llama multimedia a la capacidad de un equipo o un programa de combinar información digitalizada de varios formatos, tales como texto, gráficos, imagen fija y en movimiento y audio. A partir del nacimiento de las interfaces gráficas de usuario, la multimedia pudo

desarrollarse y convertirse en el medio de comunicación entre personas y equipos, aumentando la variedad de información disponible.

- N -

Negocio electrónico (e-business)

Cualquier tipo de actividad empresarial realizada a través de las Tecnologías de la Información y las Comunicaciones.

NIC (Network Information Center – Centro de Información de la Red)

NIC se llama a cualquier organización responsable de proporcionar información acerca de una red. Se llama habitualmente NIC a las entidades existentes en cada país responsable de administrar los dominios dentro del mismo.

- P -

Packet (paquete)

En Internet la información transmitida es dividida en paquetes que se reagrupan para ser recibidos en su destino. Paquete se llama a la unidad de datos que se envía a través de una red.

Petición (request)

Dícese de cualquiera de las "órdenes" que se envían a un servidor por medio de una aplicación cliente: solicitar una URL en un navegador, consultar los mensajes en una casilla de correo electrónico o descargar un archivo por ftp son acciones que suponen "peticiones" a los servidores. Éstos funcionan registrándolas y sirviéndolas.

PGP (Pretty Good Privacy - Privacidad Bastante Buena)

Conocido programa de libre distribución, escrito por Phil Zimmermann, que impide, mediante técnicas de criptografía, que ficheros y mensajes de correo electrónico puedan ser leídos por otros. Puede también utilizarse para firmar electrónicamente un documento o un mensaje, realizando así la autentificación del autor.

Plug-in

Pequeño programa que se "adhiere" a otro para poder ejecutar cierto tipo de archivos. Son plug-ins, por ejemplo, Flash o Real Audio, requeridos para visualizar animaciones o escuchar música a través de un navegador.

POP3 (Post Office Protocol – Protocolo de Oficina de Correos)

Protocolo diseñado para permitir a sistemas de usuario individual leer correo electrónico almacenado en un servidor. La Versión 3, la más reciente y más utilizada, llamada POP3, está definida en RFC 1725.

Portal (portal)

Sitio web cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios, entre los que suelen encontrarse buscadores, foros, compra electrónica, etc.

Protocol (protocolo)

Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina-a-máquina o intercambios de alto nivel entre programas de asignación de recursos.

Protocolo Internet (Internet Protocol)

Conjunto de reglas que estandarizan y regulan la transmisión de paquetes de datos a través de la red, mediante las cuales todos los computadores conectados pueden intercambiar información.

Proxy (apoderado)

Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

- Q -

Queue (cola)

Conjunto de paquetes que se encuentran en espera de ser procesados y/o transmitidos.

- R -

RDSI – ISDN (Red Digital de Servicios Integrados – Integrated Services Digital Network)

Tecnología en plena evolución que es ofrecida por las compañías telefónicas más importantes. ISDN combina servicios de voz y digitales

a través de la red en un solo medio, haciendo posible ofrecer a los clientes servicios de transmisión de datos así como conexiones de voz a través de un solo "cable". Los estándares de la ISDN los especifica la ITU-TSS.

Router (enrutador)

Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza sobre información, previamente introducida en el sistema, de nivel de red y tablas de direccionamiento.

- S -

Server (servidor)

Sistema que proporciona recursos a un número variable de usuarios; por ejemplo: servidor de ficheros, servidor de nombres o servidor de correo electrónico, ya sea en una red interna o externa. En Internet este término se utiliza muy a menudo para designar a aquellos sistemas que proporcionan información a los usuarios de la red.

SMTP (Simple Mail Transfer Protocol - Protocolo Simple de Transferencia de Correo)

Protocolo definido en STD 10, RFC 821, que se usa para transferir correo electrónico entre ordenadores. Es un protocolo de servidor a servidor, de tal manera que para acceder a los mensajes es preciso utilizar otros protocolos.

Spam (bombardeo publicitario)

Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir "torreja de mortadela".

- T -

TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de Control de Transmisión/Protocolo Internet)

Sistema de protocolos, definidos en RFC 793, en los que se basa buena parte de Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red.

Telnet

Telnet es el protocolo estándar de Internet que permite realizar un servicio de conexión desde un terminal remoto. Esta definido en STD 8, RFC 854 y tiene opciones adicionales descritas en muchos otros RFC's.

Transferencia de archivos (file transfer)

Copia de un fichero desde un ordenador a otro a través de una red de ordenadores.

- U -

UNIX

Sistema operativo interactivo y de tiempo compartido creado en 1969 por Ken Thompson. Reescrito a mitad de la década de los '70 por ATT alcanzó enorme popularidad en los ambientes académicos y más tarde en los empresariales, como un sistema portátil robusto y flexible, muy utilizado en los ambientes Internet.

URL (Uniform Resource Locutor – Localizador Uniforme de Recursos/Identificador)

Universal de Recursos. Sistema unificado de identificación y localización de recursos en la red. El URL define las direcciones de Internet, que se componen de protocolo, nombre de dominio y dirección local del documento dentro del servidor. Este tipo de direcciones permite identificar objetos WWW, Gopher, FTP, News, etc. Ejemplos de URL son: http://www.e.cl o ftp://ftp.e.cl/

URN (Uniform Resource Name –Nombre Uniforme de Recurso)

Sistema de identificación de recursos cuya intención es sustituir al sistema URI/URL. El sistema URN esta basado más en el recurso en sí que en el lugar en el que se halla el recurso.

- W -

Web

El término se utiliza para definir el universo del World Wide Web, los sitios, la información y los servicios de la "telaraña". Han existido diversos intentos de imponer una traducción adecuada al español, pero continúa utilizándose, sin más, "web".

WWW (World Wide Web)

Sistema de información distribuido, basado en hipertexto, creado a principios de los años 90 por Tim Berners Lee, investigador en el CERN, Suiza. La información puede ser de cualquier formato (texto, gráfico, audio, imagen fija o en movimiento) y es fácilmente accesible a los usuarios mediante los programas navegadores. La popularización del WWW facilitó en gran medida el acceso masivo del público a Internet.

- Z -

ZIP

Tipo de archivo muy utilizado para agrupar y comprimir otros archivos, con el fin de ponerlos a disposición de los usuarios por ftp o enviarlos por correo electrónico. Por este medio podemos enviar todo un sitio web, por ejemplo, en un solo archivo, haciendo su transporte por la red más cómodo y más seguro. Zip es además un formato de almacenamiento, de tamaño similar al disquete, con capacidad para 100 Mb.

BIBLIOGRAFÍA

No.	Nombre de Bibliografía
1	Computers under attack. ACM Press, 1990. P. Denning.
2	Vulnerabilidad y Seguridad de los Sistemas Informáticos. Fundación Citema, 1982. Valentin Sanz Caja.
3	A Structured Approach to Computer Security. Technical Report 122, Chalmers University of Technology, 1992. Tomas Olovsson.
4	Computer Crime. A Crimefighter's Handbook. O'Reilly & Associates, 1995. David Icove, Karl Seger, and William VonStorch.
5	The Social Organization of the Computer Underground. PhD thesis, Northern Illinois University, 1989. Gordon R. Meyer.
6	A Taxonomy of Computer Program Security Flaws, with Examples. ACM Computing Surveys, 1994. Carl E. Landwher, Alan R. Bull, John P. McDermott, and William S. Choi.
7	Use of a Taxonomy of Security Faults. Technical Report TR-96-051, Purdue University Department of Computer Science, 1996. Taimur Aslam, Ivan Krsul, and Eugene H. Spafford.
8	The Cuckoo's Egg. Doubleday, 1989. Cliff Stoll.
9	Practical Unix & Internet Security. O'Reilly & Associates, 2nd edition, 1996. Simson Garfinkel and Eugene H. Spafford.
10	Computer Security Management. Prentice Hall, 1981. Donn B. Parker.
11	Department of Defense Trusted Computer System Evaluation Criteria. Technical Report DOD 5200.28-STD, Department of Defense, 1985. Sheila L. Brand Et Al.
12	Glossary of Computer Security Terms. Technical Report NCSC-TG-004, National Computer Security Center, 1988. Sue Berg Et Al.
13	VAX Security: Protecting the System and the Data. John Wiley and Sons, 1990. Corey Sandler, Tom Badgett, and Larry Lefkowitz.
14	Glosario de Términos de Criptología. Centro Superior de Información de la Defensa, 1991. CESID.

15	Why Cryptosystems Fail. Communications of the ACM, 37:32-40, 1994. Ross J. Anderson.
16	National Research Council Committee on Information Systems Trustworthiness. Trust in Cyberspace. National Academy Press, 1999.
17	The Human Side of Computer Security. SunWorld, 1999. Carole Fennelly.
18	MrMean the Hacker; login: 1997. Peter V. Radatti.
19	Information Security Technology?. Don't rely on it. A Case Study in Social Engineering. In Proceedings of the 5th USENIX Unix Security Symposium. The USENIX Association, 1995. Ira S. Winkler and Brian Dealy.
20	Physical Security. In Keith M. Jackson and Jan Hruska, editors, Computer Security Reference Book. Butterworth-Heinemann, 1992. Randle Cowcher.
21	Techniques of Neutralization. A Theory of Delinquency. In Marvin E. Wolfgang Et Al., editors, The Sociology of Crime and Delinquency. John Wiley and Sons, 2nd edition, 1970. Gresham Sykes and David Matza.
22	The Reasoning Criminal: Rational Choice Perspectives on Offending. Springer-Verlag, 1986. D.B. Cornish and R. V. Clarke.
23	Theft by Employees. Lexington Books, 1983. Richard C. Hollinger and John P. Clark.
24	Seductions of Crime: Moral and Sensual Attractions in Doing Evil. Basic Books, 1988. J. Katz.
25	Breaking Confidences: Organizational Influences on Insider Trading. The Sociological Quarterly, 1989. N. Reichman.
26	Personnel Security. In Keith M. Jackson and Jan Hruska, editors, Computer Security Reference Book. Butterworth-Heinemann, 1992. Martin Smith.
27	La Pratique del audit informatique. Eyrolles, 1983. José Plans.

28	Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer. John Wiley and Sons, New York, 1984. D. W. Davies and W. L. Price.
29	Identity Verification and Biometrics. In Keith M. Jackson and Jan Hruska, editors, Computer Security Reference Book. Butterworth-Heinemann, 1992. David Everett.
30	The Smart Card – A Standardized Security Device Dedicated to Public Cryptology. In Contemporary Cryptology - The Science of Information Integrity. IEEE Press, 1992. Louis Claude Guillou, Michel Ugon, and Jean-Jacques Quisquater.
31	Biometric Identification. In Seminar on Network Security: Authorization and Access Control in Open Network Environment, 1998. Simo Huopio.
32	Biometric Identification Comparison Chart. PC Week, 1997. Ken Phillips.
33	Using your Body as a Key: Legal Aspects of Biometrics, 1997. Robert van Kralingen, Corien Prins, and Jan Grijpink.
34	Laboratory Evaluation of the IriScan Prototype Biometric Identifier. Technical Report SAND96-1033, Sandia National Laboratories, 1996. F. Bouchier, J.S. Ahrens, and G. Wells.
35	Iris Recognition for Personal Identification, 1997. John Daugman.
36	Texture Analysis of the Human Iris for High Security Authentication. Technical Report Image Processing 304-529, Department of Electrical Engineering, McGill University, 1997. Dave McMordie.
37	Recognizing Persons by their Iris Patterns. In Biometrics: Personal Identification in Networked Society. Kluwer, 1998. John Daugman.