UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

UNIVERSIDAD DE SOTAVENTO, A.C.

“MODELO DE LA AUDITORIA INFORMÁTICA PARA LA SEGURIDAD FÍSICA”

PRESENTA:

GRISSET ISELA MARQUEZ CRUZ

ASESOR DE TESIS:

LIC:

M.A. RAUL DE JESUS OCAMPO COLIN

COATZACOALCOS, VERACRUZ. 2011

Modelo de la Auditoria Informática para la Seguridad Física

Índice

Capítulo III Marco Aplicativo

Índice de Tablas y Figuras

Capítulo II Marco Teórico

Capítulo III Marco Aplicativo

Capítulo IV Concreción del Modelo de Auditoria Informática para la Seguridad Física

Dedicatoria

Esta Tesis está dedicada con mucho cariño a mi familia por hacer sido motivación y apoyo para lograr una meta constructiva en mi vida. Esta dedicada con mucho cariño a mi madre por apoyarme en cada objetivo que planeo en mi vida y darme la confianza para llevarlos a cabo.

Especialmente está dedicada a mi padre para que te sientas orgulloso de mí, espero no defraudarte y te agradezco por haberme ofrecido estudios.

A mis hermanos gracias por estar conmigo y apoyarme siempre, los quiero mucho. Y a mis tíos por estar siempre conmigo y consentirme tanto, los quiero. Sobrinos, sobrinas y sobrinitos, quisiera nombrarlos a cada uno de ustedes pero son mucho, pero eso no quiere decir que no me acuerde de cada uno, a todos los quiero mucho y mas que sobrinos son como mis amigos.

Le agradezco con mucho cariño a todas las personas que intervinieron directa e indirectamente en el desarrollo, aceptación y presentación de mi tesis, les estoy muy agradecido.

Le agradezco a Dios por darme la oportunidad de vivir y de regalarme una familia maravillosa la razón para pensar y la inteligencia para aprender y así haber logrado este sueño.

Y a mis profesores por confiar en mí, por tenerme la paciencia necesaria, por apoyarme en momentos difíciles. Agradezco el haber tenido unos profesores tan buenas personas como lo son ustedes. Nunca los olvidare.

Y no me puedo ir sin antes decirles, que sin ustedes a mi lado no lo hubiera logrado, tantas desveladas sirvieron de algo y aquí está el futuro.

Definición del Problema

Situación Actual

Actualmente “la mayoría de las empresas usa algún tipo de sistemas de la información (salvo caso particulares de pequeñas empresas). Las nuevas tecnologías han “invadido” las sociedad en cuestiones de diez años, imponiendo a muchas personas el uso de herramientas que desconocen” GSII, 2007.

Se suele oír en medios de comunicación, información de atentados y destrozos a infraestructuras públicas, privadas y la destrucción de información y otros activos que se encuentran en ellas, mediante el análisis de esta información se puede ver que existen debilidades en la seguridad física de las instituciones.

Las instituciones y sus unidades de sistemas de igual forma se encuentran expuestas a diversas amenazas y riesgos como incendios, inundaciones, sabotaje, atentados, robos y otros; aspectos que afectan el normal funcionamiento de la misma, es por eso que se debe tomar una serie de medidas de seguridad.

Muchas instituciones públicas y privadas no toman medidas de precaución, se observa que una gran mayoría comienzan con lo que consideran indispensable y esencial para su funcionamiento. A medida que crecen las instituciones y por problemas que atraviesan con frecuencia, estas adquieren medidas de precaución y seguridad que en muchos casos no es adecuado ni suficiente, esto debido también al continuo incremento y avance de la tecnología.

En otros casos las instituciones cumplen con las medidas de seguridad de acuerdo a las normas existentes en un determinado periodo, pero debido a constantes mejoras y actualizaciones de las normas, estándares y metodologías de evaluación, que no son tomados en cuenta en la institución, estas quedan nuevamente desactualizadas.

Otro factor, es que con frecuencia los responsables del área de Informática o Sistemas, no toman en cuenta o ignoran las normas al momento de implementar medidas de seguridad física, que prevengan la materialización de amenazas y estén en base a normas como la NB-ISO-IEC 27002, NB-ISO-IEC 27001 y otras relacionadas a Seguridad Física de la información.

Planteamiento del Problema

Varias instituciones no ven la necesidad de someter a evaluación de Auditoria Informática las unidades de sistemas, y desconocen los beneficios de aplicar normas y estándares, por lo que las medidas de protección que toman para la seguridad física, no siempre son adecuadas, haciendo que estas se encuentren expuestas a amenazas y riesgos.

Las Normas y Metodologías son amplias y generales, lo que dificulta su uso, aplicación e implementación, a los profesionales interesados en realizar una evaluación específicamente a la Seguridad Física.

Los instrumentos de Auditoria como cuestionarios, entrevistas, Checklist y otros, requieren la adecuación por parte de los profesionales y personal interesado, en hacer una evaluación de la Seguridad Física a través de una Auditoria Informática.

Muchas de las evaluaciones realizadas a las instituciones públicas y privadas, no siempre responden a las exigencias de la Seguridad Física, debido a que no se tiene definido cuales van a ser los criterios de auditoría contra los que se evaluara el cumplimiento.

Problema Principal.

Por lo que podemos decir:

Los activos de las unidades de sistemas de las instituciones, están expuestas a amenazas y riesgos físicos, debido a inadecuadas evaluaciones de Auditoria Informática en la Seguridad Física.

Hipótesis

El Modelo de Auditoria Informática para la Seguridad Física, permita evaluar de forma completa los recursos de información y activos físicos de las unidades de sistema, en base a la norma NB-ISO-IEC 27002.

Identificación de Variables

Variable Dependiente: Evaluar de forma completa los recursos de información y activos físicos en instituciones.
Variable Independiente: El Modelo de Auditoria Informática para la Seguridad Física.
Variable Interviniente: Norma NB-ISO-IEC 27002.

Variable Independiente-Causa	Variables Dependiente- Efecto
El Modelo de Auditoria Informática para la Seguridad Física.	Evaluar de forma completa los recursos de información y activos físicos en instituciones.

Objetivo General

- Elaborar un Modelo de Auditoria Informática para la Seguridad Física de la Informacion[9] y recursos fisicos[10], en base a la Norma NB-ISO-IEC 27002 y COBIT, que permita evaluar e identificar las amenazas y riesgos existentes en las unidades de sistemas de las instituciones.

Objetivo Específico

- Especificar normas para la Seguridad Física de los recursos de información y activos físicos, en base a la Norma NB-ISO-IEC 27002.
- Determinar Objetivos de Control para la Seguridad Física, en base a la norma NB-ISO-IEC 27002 y COBIT.
- Clasificar la información según los activos a evaluar en la Seguridad Física.
- Elaborar herramientas para la implementación de Auditoria Informática que permita evaluar el área de Seguridad Física en base a los objetivos de control determinados.
- Seleccionar y Clasificar los instrumentos para el área de Seguridad Física.

[9]Informacion (Contratos y acuerdos, documentación de Sistemas, manuales de usuarios, material de capacitación, planes de continuidad e información archivada).

[10]Recursos físicos: Equipos de computación, medios removibles, relacionados con el almacenamiento de información.

Justificación

Justificación Teoría

Se tiene información de Metodologías de Auditoria Informática a nivel Internacional, los cuales están enfocados a diversas áreas donde también se toma en cuenta la Seguridad Física, este hecho dificulta la comprensión, aplicación e implementación de la Metodología; a los profesionales y miembros de instituciones públicas o privadas interesadas en realizar este tipo de evaluación.

Es por eso que el presente trabajo de Auditoria Informática, aporta con información para evaluar específicamente la Seguridad Física de la información y recursos físicos de las unidades de sistemas de instituciones, lo cual facilita su comprensión, aplicación e implementación.

Justificación Social

La presente tesis es de beneficio social porque expresa de manera comprensible las medidas de Seguridad Física que deben considerarse para la información y recursos físicos de las instituciones, va en beneficio de estudiantes profesionales y personas miembros de instituciones públicas o privadas interesadas en la Auditoria Informática a la Seguridad Física, permite la comprensión y aplicación de medidas de Seguridad Física, y la evaluación de la misma a través de las herramientas propuestas.

Justificación Práctica

La investigación es importante porque proporciona información sobre las medidas de la Seguridad Física para la información y recursos físicos de las unidades de sistemas de instituciones, otorga información de procesos, procedimientos y herramientas de evaluación para llevar a cabo una Auditoria Informática a la Seguridad Física.

Justificación Económica

Con respecto a lo económico, es sabido que recuperar algún activo perdido es más costoso que implementar medidas de Seguridad Física. Por lo que, la aplicación de la presente tesis es importante, ya que permite a las unidades de sistemas de las instituciones, conocer el nivel de seguridad física y partiendo de esa información puede implementar y mejorar las medidas de protección para su información y recursos físicos.

Introducción

Debido al incremento de tecnologías de información, las Auditorias Informáticas se han incrementado en los últimos años considerablemente en todo el mundo, porque se hace necesaria la realización de evaluaciones en las distintas áreas de la informática para optimizar su funcionamiento.

En el capítulo I se analiza como el continuo avance de las tecnologías, la poca e inadecuada práctica de evaluaciones de auditoría informática en las instituciones, deja las unidades de sistemas expuestas a amenazas y riesgos físicos, por lo que se plantea el objetivo de elaborar un Modelo de Auditoria Informática para la Seguridad Física. Para el logro de este objetivo se selecciona normas, se especifica objetivos de control para la seguridad física basado en la norma NB- ISO – IEC 27002 y la metodología COBIT, además se plantea, la construcción de herramientas de evaluación de acuerdo a los objetivos de control especificados.

La presente tesis evalúa la seguridad física de los recursos de información y activos físicos relacionados con el almacenamiento de la información, sin considerar aspectos de seguridad lógica para los mismos.

La respuesta tentativa de la investigación es: el Modelo de Auditoria Informática para la Seguridad Física permite evaluar de forma completa los recursos de información y activos fijos de las unidades de sistemas, en base a la norma NB-ISO-IEC 27002.

En el Capítulo II se encuentra las teorías e información sobre auditoria informática, normas y metodologías de auditoría que son utilizadas en la etapa de construcción del modelo proyecto.

En el Capítulo III se encuentra el Marco Aplicativo, en ella se describe la construcción de objetivos de control y herramientas (relevamiento de información y evaluación) que son utilizadas a lo largo de las etapas de la auditoria informática.

En el Capítulo IV se encuentra la concreción del Modelo de Auditoria Informática para la Seguridad Física y las pruebas realizadas en instituciones, describe el modo de empleo de las herramientas, además de probar la hipótesis planteada.

Tras el análisis del trabajo se tiene conclusiones puntuales según los objetivos propuestos y las recomendaciones en base a la experimentación del trabajo de investigación, expuestas en el capitulo V.

En la penúltima parte de este documento, se encuentras las referencias bibliográficas de los textos consultados en la realización, en algunos casos se cita los textos con los códigos de consulta de las bibliotecas.

Al final del documento se encuentras los anexos, que contiene información sobre el trabajo de investigación como: (1) Documentación de la Aplicación del Modelo propuesto y (2) otros documentos.

Capítulo I. Marco Contextual

Capítulo I. Marco Contextual

En el presente capítulo se muestra un panorama general de la Tesis de Grado, describe los antecedentes, el planteamiento del problema, los objetivos propuestos y los aportes en el desarrollo de la presente investigación.

1. Introducción

Con frecuencia se utiliza el término de: Auditoria de Sistemas, Auditoria de Sistemas Informáticos o Auditoria Informática para referirse a la actividad de evaluar y verificar el funcionamiento correcto, eficaz, eficiente de los sistemas y el entorno informático, el presente trabajo utiliza el término de Auditoria Informática.

La Auditoria Informática, comprende diferentes áreas como el desarrollo, mantenimiento, dirección, seguridad, redes, ofirmatica, exploración, bases de datos, aplicaciones y otros, que son evaluados de forma independiente a través de Auditorias Informáticas a casa una de estas áreas, de acuerdo al requerimiento de las instituciones[1].

Para realizar evaluaciones de Auditoria Informática, existe la metodología Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT) reconocida en varios países del mundo. La metodología COBIT[2] proporciona los denominados Objetivos de Control, presenta las actividades en una estructura manejable y lógica, brinda buenas prácticas a través de un marco de trabajo de dominios y procesos. Las buenas prácticas de COBIT; son un consenso de expertos, están enfocadas fuertemente en el control de actividades, ayudan a optimizar las inversiones, aseguran la entrega del servicio y brindan medidas para juzgar cuando las cosas no van bien.

[1]Auditoria Informática, Plattini Mario, Del Peso Emilio, Segunda Edición [AIEP, 2001].

[2] [COBIT 4.0, 2005].

La presente tesis aporta información sobre medidas de protección de Seguridad Física con las que debe contar para los activos[3] de una institución, sea esta de carácter público o privado, estas medidas de protección están en base a la Norma de Seguridad NB-ISO-IEC 27002 y COBIT reconocida en Bolivia y a nivel Internacional. Del mismo modo provee información para la identificación, aplicación, implementación y herramientas para una Auditoria Informática dedicada específicamente a la Seguridad Física de los recursos de información y activos institucionales. Esta información facilita la realización de una Auditoria Informática a la Seguridad Física de los recursos de información y activos físicos, ya que se proporciona un Modelo para realizar la Auditoria Informática.

1. 1. Antecedentes

La informática ha sido un área que ha cambiado en los últimos años debido a la proliferación de las tecnologías de información. "A partir de 1950 la Informática se convierte en una herramienta muy importante en las labores de Auditoría Financiera, ya que permite llevar a cabo de forma rápida precisa operaciones, que manualmente consumirían demasiados recursos[4]." Al convertirse los sistemas de información de las empresas cada vez más dependientes de los computadores y descubrir varios casos de fraude cometidos con ayuda del computador, seguir con la Auditoria alrededor del computador[5] ya no es viable. Por lo que surge la necesidad de una nueva especialidad dentro de la Auditoria, que verifique el funcionamiento correcto, eficaz y eficiente de los sistemas informáticos; esta nueva especialidad es denominada Auditoria Informática.

[3]Se considera un activo a: Recursos de Información, Activos Físicos, Recurso de Software y los Servicios. [ISO/ IEC 17799]. Este trabajo contempla: Recursos de Información (Documentación de Sistemas, manuales de usuario, material de capacitación, planes de continuidad e información archivada) y Activos Físicos: Equipamiento Informático (procesadores, monitores, computadoras portátiles), medios magnéticos (cintas y discos).

[4]Recursos económico, humano y de tiempo. [AIEP, 2001].

[5]Considerado también como una Caja Negra [AIEP, 2001].

La tendencia a la realización de Auditorías Informáticas en distintas áreas como ser: “Sistemas informáticos, bases de datos, ofirmatica, seguridad, redes, física y otros”[6], se ha incrementado en los últimos años considerablemente en todo el mundo, por que permite identificar las falencias en las instituciones lo cual ayuda a mejorar el área que es auditada.

En el transcurso de los últimos años, la utilización de normas como las de Tecnologías de información, Técnicas de seguridad y requisitos (NB-ISO-IEC 27001), Tecnología de información y Código de práctica para la gestión de seguridad de la información (NB-ISO-IEC 27002) y la realización de evaluaciones, también ha cobrado mayor importancia en nuestro medio, aunque todavía existen instituciones con personal que desconoce o no utiliza las normas existentes y metodologías de evaluación como ser COBIT u otras.

COBIT (Objetivos de Control para la Información y las Tecnologías Relacionadas) es considerado principalmente como un recurso educativo para los profesionales dedicados a las actividades de control. Es una metodología que maneja cuatro Dominios[7], está constituido por 34 objetivos de Control de alto nivel y 318 objetivos de control detallados[8].

ISACA (Information Systems Audit and Control Association), es una organización global líder de profesionales que representa a individuos en más de 100 países y comprende todos los niveles de la tecnología de información. Sus normas de Auditoría y control de Sistemas de Información son respetados por profesionales de diversos países, ISACA ofrece la posibilidad de obtener certificaciones como “Certified Information System Auditor” (CISA) y “Certified Information Security Manager” (CISM).

[6][AIEP, 2001] Auditoria Informática un Enfoque Practico, Mario Piattini.

[7]Planeacion y Organización, Adquisición e Implementación, Entrega de Servicios y Soportes, Monitoreo [COBIT].

[8]Objetivos de Control para la Información y las Tecnologías Relacionadas [COBIT].

En comparación con años anteriores son más los profesionales Informáticos y Auditores que se interesan, informan, conocen, capacitan y actualizan sobre la Auditoria Informática, toman cursos de especialización para llegar a ser Auditoria Informática, toman cursos de especialización para llegar a ser Auditor Certificado de Sistemas de Información (CISA) reconocido a nivel internacional y es otorgado por ISACA.

1.2. Antecedentes de Instituciones Auditoras en Informática

En Bolivia existen instituciones que trabajan en el área de Auditoria Informática como ser: BDO BERTHIN AMENGUAL & ASOCIADOS es una firma reconocida en Bolivia, trabaja con consultorías y auditorias. Existe una división que se dedica a la Auditoria Informática o de Sistemas, realizan evaluaciones de riesgos a los sistemas, redes, gestión de seguridad de la información y otros. Los consultores aplican y utilizan distintas metodologías y Normas como las Normas de Auditoria Gubernamentales, Cobit, ISO 17799 y otras.

PRICEWATERHOUSECOOPERS S.R.L. es una institución que opera en Bolivia y es miembro de la organización mundial PricewaterhouseCoopers. Entre las actividades que realizan en el área de informática, se encuentran: evaluaciones de sistemas de control interno, asistencia a los departamentos de Auditoría interna; revisión de gestión de la seguridad, normas de seguridad, configuración de seguridad de plataformas tecnológicas, configuración de seguridad de dispositivos de comunicación, evaluación de planes de contingencia.

1.3. Antecedentes del Proyecto

En la Carrera de Informática de la Universidad Mayor de San Andrés se tiene trabajos relacionados con Auditoria Informática y Normas, dentro de ellos se puede citar a: AUDITORIA INFORMATICA DE REDES de Ascarrunz Martínez Henoch, el cual propone una metodología para la Auditoria a redes de computadoras a nivel del área local que evalúa las redes, verifique el diseño adecuado de la red de comunicación, tiene cuestionarios para la evaluación física y lógica con puntajes de donde obtiene un promedio, así determina el nivel en que se encuentra la red, clasificándolo como pésima, deficiente, aceptable, adecuada, buena y sobresaliente.

AUDITORIA EN CALIDAD DE SOFTWARE de Aspiazu Castro, Virginia propone un modelo de Auditoria de calidad de software para los sistemas informáticos. Este modelo detecta los puntos débiles de los sistemas y evalúa de acuerdo al tipo de sistema que se considera, planeta 3 etapas para la Auditoria en la calidad del software: la planificación donde se hará una investigación a fin de conocer las áreas auditadas, diagnostico de Auditoria y dictamen final donde se da a conocer las debilidades encontradas y el nivel de calidad. Todo este proceso es realizado para determinar si el software cumple con las normas de calidad que existe y si está de acuerdo a las métricas del software.

GUIA DE AUDITORIA INFORMATICA de Perales & Paredes quienes elaboran una guía y proponen un algoritmo de evaluación automatizado que permite identificar riesgos en 8 áreas de la unidad informática, realizaron cuestionarios de acuerdo a las áreas consideradas, proponen un software que permite reducir el tiempo de procesamiento de los datos constituyéndose en una herramienta para el auditor.

GUIA DE AUDITORIA DE SEGURIDAD DE LA INFORMACION de Zenteno Flores Lorena, plantea la elaboración de una guía de Auditoria de seguridad de la información, tomando como base la norma ISO 17799, para esto determina puntos débiles de la seguridad de la información según esta norma, el proyecto concluye de manera satisfactoria logrando diseñar y elaborar una guía o manual técnico que considera aspectos prácticos y legales.

AUDITORIA INFORMATICA DE CALIDAD BASADA EN LA NORMA ISO 9000 de Aliaga Moruno Ivert en la tesis propone la hipótesis "Es posible ajustar las metodologías de Auditoria de Sistemas o informática a las normas ISO 9000", para obtener Auditorias de sistemas con calidad. Para esto realiza estudios sobre metodologías y norma ISO 9000, el cual hace referencia y define conceptos para lograr sistemas de Calidad de Software, cumpliendo plenamente con el ajuste, se obtuvo un modelo con los lineamientos necesarios para auditar.

Si bien existe en la Carrera de Informática de la Universidad Mayor de San Andrés, Tesis y Proyectos de Grado relacionados a Auditoria Informática contemplando aspectos de seguridad, no se ha encontrado investigaciones, ni propuestas orientadas a la Seguridad Física de manera específica, para efectuar una Auditoria Informática a la Seguridad Física de las unidades de sistemas de instituciones.

Capítulo II Marco Teórico

Capítulo II. Marco Teórico

2. Amenaza, Vulnerabilidad y Riesgo

Dentro del campo de la auditoria informática existen riesgos, amenazas y vulnerabilidades que son diferentes.

2.1. Amenaza

La amenaza se define como la causa potencial de un incidente no deseado, que causa daño a un sistema o a la organización[11].

Es una persona o cosa vista como posible fuente de peligro o catástrofe. Las amenazas se presentan de forma compleja y son de difícil pronostico[12].

2.1.1. Tipos de Amenazas[13]

Las amenazas se clasifican en: naturales, involuntarias e intencionadas.

2.1.1.1. Amenazas Naturales o Física

Son las que ponen en peligro los componentes físicos del sistema. En ellas se distingue por un lado los desastres naturales, como las inundaciones, rayos o terremotos, y las condiciones medioambientales, tales como la temperatura, fuego, inundación, humedad, presencia del polvo.

[11][ISO 27002, 2007] Términos y Definiciones Pag. 6.

[12][PIATTINI, 2001] Capitulo 3 Pag. 48.

[13][SYPDI, 2008] TEMA 2 Seguridad en Sistemas Operativos [PIATTINI, 2001] Capitulo 3 Pag. 48.

2.1.1.2. Amenazas Involuntarias

Son aquellas relacionadas con el uso descuidado del equipo por falta de entrenamiento o de concienciación sobre la seguridad. Entre las más comunes se cita: borrar sin querer parte de la información sin desearlo, dejar sin protección determinados ficheros básicos del sistema, divulgación de datos por dejar pegado a la pantalla un post-it con nuestra contraseña u olvidar salir del sistema.

2.1.1.3. Amenazas Intencionadas

Son aquellas procedentes de personas que pretenden acceder para borrar, modificar o robar la información; para bloquearlo o por simple diversión.

Los causantes del daño son de dos tipos: externos e internos.

- Los causantes externos ingresan al sistema de múltiples formas como: (1) entrando al edificio o accediendo físicamente al ordenador, (2) entrando al sistema a través de la red aprovechando las vulnerabilidades, (3) accediendo a través de personas autorizadas.
- Los causantes internos son de tres tipos: (1) empleados despedidos o descontentos, (2) empleados coaccionados y (3) empleados que obtienen beneficios personales.

2.2. Vulnerabilidad

La vulnerabilidad es la debilidad de un recurso o grupo de recursos que son aprovechados por una o varias amenazas[14].
Es una situación creada por la falta de uno o varios controles que eviten la amenaza, que afecta al entorno informatico[15].

[14][ISO 27002, 2007] Términos y Definiciones Pag. 6.

[15][PIATTINI, 2001] Capitulo 3 Pag. 49.

2.2.1. Tipos de Vulnerabilidad[16]

Entre los tipos de vulnerabilidad se tiene; físicas, naturales, hardware y software, medios o dispositivos, por emanación, y vulnerabilidad de la comunicación.

2.2.1.1. Vulnerabilidad Física

La vulnerabilidad física es la posibilidad de entrar o acceder físicamente para robar, modificar o destruir el ambiente del edificio o el entorno físico del sistema.

2.2.1.2. Vulnerabilidad Natural

Se refiere al grado en que los activos de la institución son afectados por desastres naturales o ambientales como el fuego, inundaciones, rayos, terremotos, o fallas eléctricas. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

2.2.1.3. Vulnerabilidad del Hardware y del Software

La vulnerabilidad del hardware es la facilidad del acceso a los dispositivos.

La vulnerabilidad del software son las fallas o debilidades del sistema que hacen fácil su acceso y lo hacen menos fiable.

2.2.1.4. Vulnerabilidad de los Medios o Dispositivos

Son las posibilidades de robar o dañar los discos, cintas y otros dispositivos de la computadora.

[16][SYPDI, 2008] TEMA 2 Seguridad en Sistemas Operativos.

2.2.1.5. Vulnerabilidad por Emanación

Se refiere a la intercepción de las radiaciones de los dispositivos eléctricos y electrónicos para descifrar o reconstruir la información almacenada o transmitida.

2.2.1.6. Vulnerabilidad de las Comunicaciones

La vulnerabilidad de las comunicaciones es el riesgo de intercepción cuando los ordenadores están conectados a la red.

2.2.1.7. Vulnerabilidad Humana

La vulnerabilidad humana es el riesgo que representan los usuarios o personas que administran y utilizan los sistemas tanto física o mediante conexión, ya que toda la seguridad descansa sobre ellos.

2.3. Riesgo[17]

El Riesgo es la posibilidad de que una amenaza llegue a acaecer[18] por una vulnerabilidad. El riesgo se cuantifica como el resultado de multiplicar la probabilidad de que la amenaza se produzca, por el daño potencial de esta, se expresa en forma de ecuación:

Riesgo = Probabilidad * Daño potencial.

Una amenaza con un riesgo alto, debe ser paliada de forma rápida. Una amenaza con un riesgo medio, aunque importante, es de menor urgencia y por último las de riesgo bajo, se puede llegar a ignorar dependiendo del costo y del esfuerzo necesario.

[17][PIATTINI, 2001] Capitulo 3 Pag. 49.

[18]Acaecer sinónimo de acontecer, suceder, ocurrir.

Por estas razones es necesario tomar medidas de protección para la seguridad de las instituciones u organizaciones sin importar si son grandes o pequeñas.

2.4. Seguridad[19]

Cuando se habla de seguridad se suele oír varias expresiones como: seguridad de las infraestructuras, seguridad informática, seguridad de los sistemas, seguridad de tecnologías de información o protección de la información.

La seguridad son medidas de protección y preservación, que se toman para garantizar la confidencialidad, integridad, disponibilidad, autenticación, autorización y confiabilidad que son consideradas para los activos estratégicos y valiosos relacionados con los sistemas y la institución. Cada institución define que activos consideran importantes.

2.4.1. Clasificación de la Seguridad[20]

La seguridad se clasifica en Seguridad Lógica y Seguridad Física.

- La seguridad Lógica, son medidas para la protección de acceso lógicos, cubre requerimientos que van más allá de aspectos físicos a través del uso de barreras y procedimientos que permita el almacenamiento y acceso a los datos solo para personas autorizadas.
- La Seguridad Física, es la "Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial".

[19][PIATTINI, 2001].
[20][PIATTINI, 2001].

La seguridad física suministra protección ante accesos no autorizados, los cuales son prevenidos en una institución, para evitar daños, perdidas e interferencias a los activos de la institución y sobre todo la perdida de la información. La Seguridad Física es aplicada a nivel general, como controlar entradas físicas a la empresa, asegurar áreas e implantar equipos de seguridad.

2.5. Seguridad Física[21]

La seguridad física suministra protección ante accesos no autorizados, datos e interferencias a las instituciones de la organización y a la información.

Los requisitos sobre seguridad física varían considerablemente según las instituciones y dependen de la escala de organización de los sistemas de información. Pero son aplicables a nivel general los conceptos de asegurar áreas, controlar perímetros, controlar las entradas físicas e implantar equipamiento de seguridad.

Esto deriva en que para un atacante es fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

2.5.1. Amenazas a la Seguridad Física[22]

Consiste en analizar qué aspectos del ambiente constituyen una amenaza a la infraestructura.

Las amenazas a la seguridad física son:

- Las emergencias.
- El fuego y Smok.

[21][CISSP, 2004].
[22][CISSP, 2004].

- Derrumbamiento o explosión.

- La pérdida de utilidad (corriente eléctrica, el aire acondicionado, que calienta).
- El daño de agua (la rotura de la cañería).
- El descargo de los materiales toxico.
- Los desastres naturales.
- El movimiento de tierra (como los terremotos).
- El daño de una tormenta (como la nieve, hielo y diluvios).
- La intervención humana.
- El sabotaje.
- El vandalismo.
- La guerra y las huelgas.

2.6. Evaluacion[23]

La evaluación es el proceso de análisis y valoración continua, mediante el cual se juzga o prueba algo.

Es el proceso de planificación, obtención y análisis para una adecuada toma de decisiones sobre el proceso desarrollado.

2.6.1. Evaluación de Riesgo

Es el proceso total de análisis de riesgo y valoración de riesgo.

2.7. Estándar, Política y Normas de Seguridad

A través del tiempo se ha formulado estándares, normas y políticas que son el fruto de la experiencia de los profesionales en los diversos campos que existen.

[23][ISO 27002, 2007] Términos y Definiciones Pag. 6.
[ANDER-EGG, 2000].

2.7.1. Estándar

Es una publicación que recoge el trabajo en común de los comités de fabricantes, usuarios, organizaciones, departamentos de gobierno, consumidores y contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional con el objeto de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.

Los estándares ayudan a aumentar la fiabilidad y efectividad de materiales, productos, procesos o servicios que utilizan las partes interesadas como los productores, vendedores, compradores, usuarios reguladores y otros.
Aunque la legislación y las reglamentaciones nacionales hacen referencia a los estándares, estos son de uso voluntario.

2.8. Política

Las políticas son formas de comunicarse con los usuarios, establecen un canal formal de actuación del personal, en relación con los recursos y servicios.

Consideran principalmente el alcance, objetivos, responsabilidades, requerimientos mínimos, definición de violaciones y sanciones.

Ofrecen explicaciones comprensibles sobre por qué se toma ciertas decisiones y explica la importancia de los recursos, establecer las expectativas de la organización y especifica la autoridad responsable de aplicar los correctivos o sanciones.

2.9. Norma

Son reglas, guías de actuación a seguir o son patrones de referencia.

Las normas de seguridad son de carácter general y de carácter especifico:

a) Normas de carácter general: son universalmente aceptadas.
b) Normas de carácter específico: regulan una función, trabajo u operación específica.

Entre las ventajas de las normas se tiene:

- ✓ Ofrecen un lenguaje común de comunicación entre fabricantes, usuarios y/o consumidores.
- ✓ Establece un equilibrio entre los distintos agentes.
- ✓ Es un patrón necesario de confianza entre el cliente y el proveedor.
- ✓ Representa un elemento de sistematización de seguridad.
- ✓ Facilita la comprensión y ejecución de las tareas de seguridad de forma clara y precisa.
- ✓ Permite la dirección eficaz del sistema de seguridad.
- ✓ Impide que exista vacios acerca de la seguridad.
- ✓ Facilita la rápida formación y concientización del personal
- ✓ Permite un manejo excelente de las instalaciones y equipo.
- ✓ Homogeniza medios y procedimientos, además de facilitar la comunicación y la seguridad.
- ✓ Aumenta el sentido de seguridad en el usuario.

En Bolivia como en otros países existen normas, como ser la Norma Boliviana NB-ISO-IEC 27002 (antiguamente Norma Boliviana NB-ISO-IEC 17799:2005), y la Norma Boliviana NB-ISO-IEC 27001, ambas se dedican a la Seguridad de la Información.

2.10. Norma Boliviana NB-ISO-IEC 27002

Norma Boliviana sobre Tecnologías de la Información- Técnicas de Seguridad- Código de prácticas para la gestión de seguridad de la información (NB-ISO-IEC 27002); es publicada en Bolivia en noviembre del 2007 por el Instituto Boliviano de Normalización y Calidad (IBNORCA).

La Norma NB-ISO-IEC 27002 es un compendio de recomendaciones y buenas prácticas para la seguridad de toda institución, se aplica independientemente de sus características. Las recomendaciones de la norma son neutrales en cuanto a la tecnología, ayudan a evaluar y entender las medidas de seguridad existentes.

2.10.1. Evolución de la Norma BS7799 a la actual ISO 27001 y 27002[24]

La Norma BS7799 aparece en 1995, con el objetivo de preparar a cualquier empresa y sobre todo a las británicas en la certificación de la seguridad de la información, por medio de auditorías realizadas por auditores certificados y externos. El gobierno del Reino Unido recomendó como parte de su Ley de Protección de la Información, que las compañías británicas utilicen la BS7799 como método de cumplimiento de la Ley.

1. La primera parte de la norma BS7799-1 es una guía de buenas prácticas, la que no establece un modelo de certificación.
2. La segunda parte de la norma BS7799-2 audita y certifica a empresas solicitantes que hayan desarrollado un Sistema de Gestión de Seguridad de la Información (SGSI), asegura la adaptación continua de la seguridad a los requisitos cambiantes de la empresa y su entorno.

[24][ISOHIS, 2008].

Las dos partes de la norma BS7799 se revisan en 1999 y la primera parte se adopta por ISO, sin cambios sustanciales con la denominación de ISO 17799 en el año 2000.

El 2005 la ISO publica la segunda parte de la norma con la denominación ISO 27001, junto a la primera revisión formal realizada en ese mismo año de la ISO 17799.

Estas normas son traducidas y adaptadas en Bolivia por un Comité Técnico de Normalización, luego de aprobar el trabajo son publicadas por el Instituto Boliviano de Normalización y Calidad (IBNORCA).

Las normas ISO 27001 son publicadas en Bolivia el 2007 bajo la denominación de NB-ISO-IEC 27001 y NB-ISO-IEC 27002.

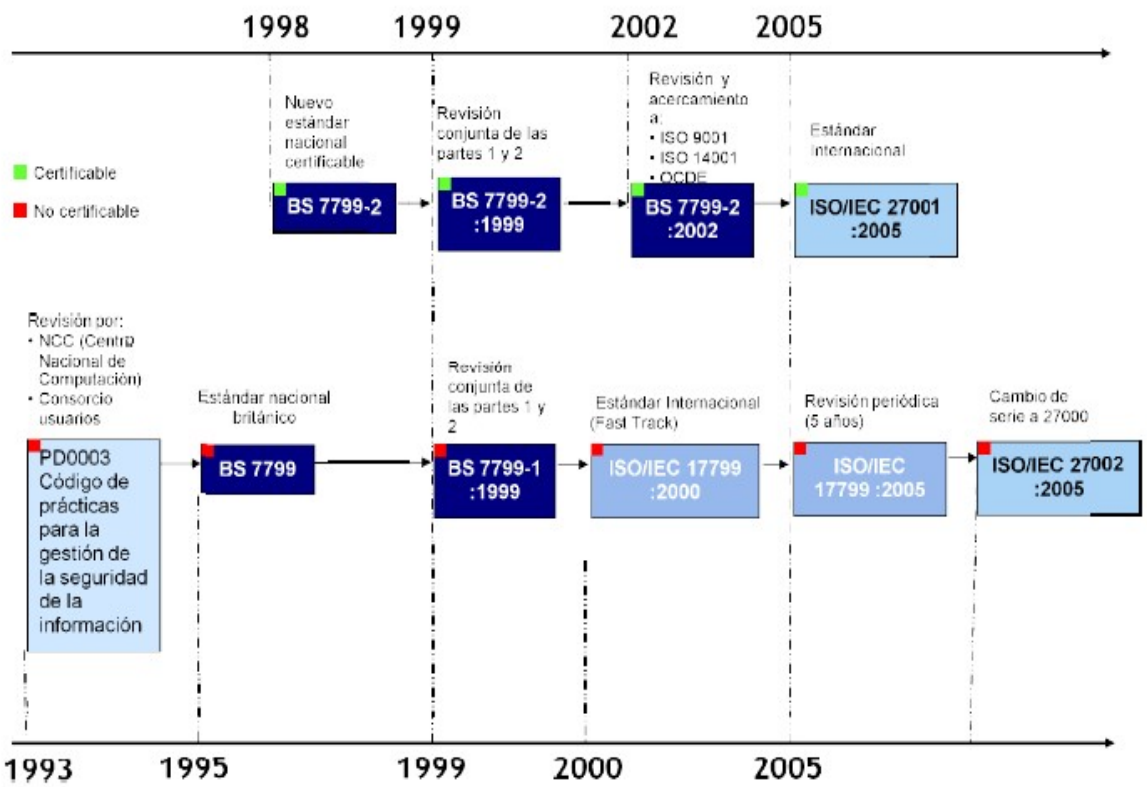
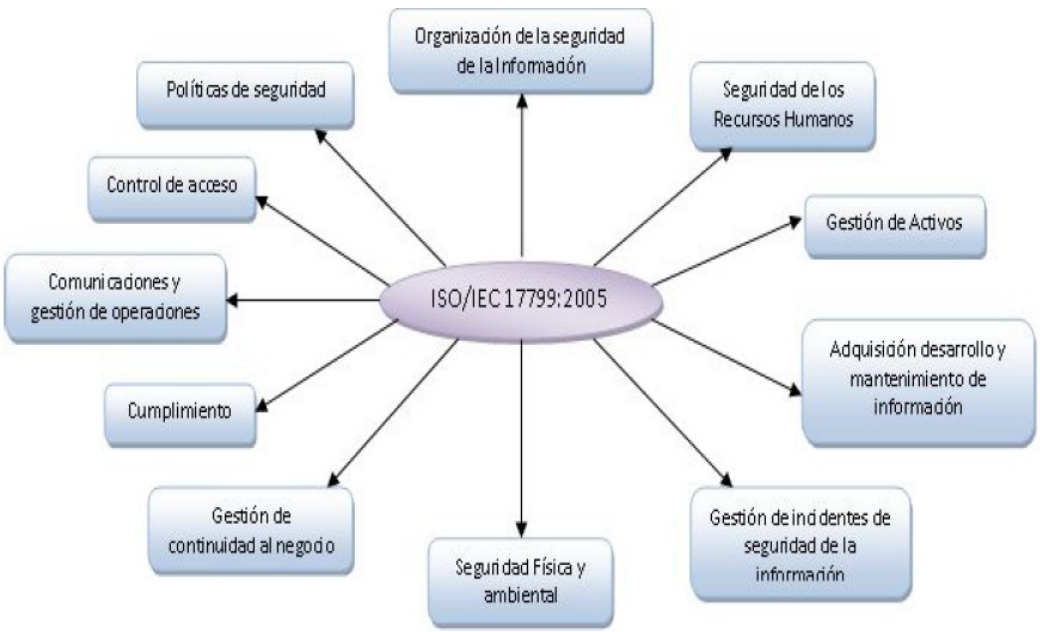


Figura 2.10.1. Historia Norma NB-ISO-IEC 27001 y 27002

2.11. Estructura de la Norma NB-ISO-IEC 27002[25]

La norma NB-ISO-IEC 27002 se compone por once clausulas de control, y treinta y seis categorías principales de seguridad dentro de sus clausulas.



2.1 …. Política de Seguridad

Esta clausula tiene un control principal que es la política de seguridad de la información.

2.11.1.1. Política de Seguridad de la Información

Su objetivo es proporcionar soporte y orientación a la dirección para la seguridad de la información conforme a requisitos del negocio, leyes y regulaciones relevantes.

[25][ISO 27002,2007] Norma Boliviana NB-ISO-IEC 27002.

La alta dirección debe establecer una clara dirección de la política de acuerdo con los objetivos del negocio, demostrar el apoyo y el compromiso para y con la seguridad de la información a través de la publicación y

mantenimiento de una política de seguridad de la información de la institución.

2.11.2. Organización de la Seguridad de la Información

Esta clausula tiene dos controles principales que son: (1) Organización interna y (2) partes externas.

2.11.2.1. Organización Interna

Tiene como objetivo Gestionar la seguridad de la información dentro del la institución.

2.11.2.2. Partes Externas

El objetivo es mantener la seguridad de la información y de las instalaciones de procesamiento de informaciones de la institución que son accedidas, procesadas, comunicadas a, o dirigidas por partes externas.

2.11.3. Gestión de Recursos

La gestión de recursos comprende dos controles principales que son: (1) responsabilidad por los recursos y (2) clasificación de la información.

2.11.3.1. Responsabilidad por los Recursos

El objetivo es alcanzar y mantener la protección apropiada de los recursos institucionales.

2.11.3.2. Clasificación de la Información

Tiene como objetivo asegurar que la información recibe un apropiado nivel de protección.

2.11.4. Seguridad de los Recursos Humanos

Los controles de esta clausula son: (1) previo a la contratación, (2) durante el empleo y (3) finalización o cambio de empleo.

2.11.4.1. Previo a la Contratación

Asegura que los empleados, contratistas y terceras partes usuarias[26] entiendan sus responsabilidades y sean adecuados para los roles que han sido considerados, y reducir el riesgo de robo, fraude o mal uso de las instalaciones.

2.11.4.2. Durante el Empleo

Asegura que todos los empleados contratistas y terceras partes usuarias estén consientes de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, son equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

2.11.4.3. Finalización o cambio de empleo

Asegura que los empleados, contratistas y terceras partes usuarias salgan de una institución o cambien de empleo de manera ordenada.

[26]Terceras partes usuarias, se refiere a personas ajenas a la instituciones, que vienen a prestar un servicio o a consultar y solicitar uno.

2.11.5. Seguridad Física y Ambiental

Los controles principales para la seguridad física y ambiental son: (1) áreas seguras y (2) seguridad del equipamiento.

2.11.5.1. Áreas Seguras

El objetivo es prevenir el acceso físico no autorizado, daño o interferencia a los predios e información de la organización.

Las instalaciones de procedimiento de información critica o sensible de la organización deben estar ubicadas en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada, debe estar físicamente protegidas contra accesos no autorizados, daño e interferencia.

2.11.5.2. Seguridad del Equipamiento

El objetivo es prevenir perdida, daños, robos o exposiciones al riesgo de los recursos e interrupción a las actividades de la institución.

2.11.6. Gestión de Comunicaciones y Operaciones

La gestión de comunicaciones y operaciones tiene diez controles principales cada uno cumple un objetivo y son:

2.11.6.1. Procedimiento y Responsabilidades Operacionales

Asegura la correcta y segura operación de las instalaciones de procesamiento de la información.

2.11.6.2. Gestión de la prestación del servicio por terceras partes

Implementa y mantiene el nivel apropiado de seguridad de la información y de prestación de servicio conforme con los acuerdos de prestación de servicio de terceras partes.

2.11.6.3. Planificación y aceptación del sistema

Minimiza el riesgo de fallas de los sistemas.

2.11.6.4 Protección contra código malicioso y móvil

Protege la integración del software y de la información.

2.11.6.5. Respaldo

Mantiene la integridad y disponibilidad de información e instalaciones de procesamiento de información.

2.11.6.6. Gestión de seguridad de las redes

Asegura la protección de la información en las redes y la protección de la infraestructura de soporte.

2.11.6.7. Manejo de los Medios

Previene la divulgación, modificación retiro o destrucción de recursos no autorizado y la interrupción de las actividades del negocio.

2.11.6.8. Intercambio de Información

Mantiene la seguridad de la información y el software intercambiado dentro de una organización y con cualquier organización externa.

2.11.6.9. Servicios de Comercio Electrónico

Garantiza la seguridad de los servicios de comercio electrónico y su empleo seguro.

2.11.6.10. Supervisión

Detecta actividades de procesos de información no autorizados.

2.11.7. Control de Accesos

El control de accesos tiene siete controles enfocados a objetivos, son:

2.11.7.1. Requisitos del negocio para el control de accesos

Controla el acceso de información.

2.11.7.2. Gestión de Accesos a Usuarios

Asegura que el usuario autorizado tenga acceso y prevenir el acceso no autorizado a sistemas de información.

2.11.7.3. Responsabilidad de los Usuarios

Previene el acceso de usuarios no autorizados que comprometan o roben información e instalaciones de proceso de información.

2.11.7.4. Control de acceso a la red

Previene el acceso no autorizado a servicios conectados a una red.

2.11.7.5. Control de acceso al sistema operativo

Previene el acceso no autorizado a los sistemas operativos.

2.11.7.6. Control de acceso a la aplicación e información

Previene el acceso no autorizado a la información guardada en los sistemas de aplicación.

7.11.7.7. Computación móvil y trabajo remoto

Garantiza la seguridad de la información cuando se utilizan dispositivos de computación móvil e instalaciones de trabajo remoto.

2.11.8. Adquisición, desarrollo y mantenimiento de Sistemas de Información

Considera seis controles principales los cuales son:

2.11.8.1. Requisitos de seguridad de los sistemas de información

Garantiza que la seguridad es una parte integral de los sistemas de información.

2.11.8.2. Procesamiento correcto en las aplicaciones

Previene errores, pérdidas, modificaciones no autorizadas o uso indebido de la información en las aplicaciones.

2.11.8.3. Controles Criptográficos

Protege la confidencialidad, autenticidad e integridad de la información por medios criptográficos.

2.11.8.4. Seguridad de archivos de sistema

Garantiza la seguridad de los archivos de sistemas.

2.11.8.5. Seguridad en procesos de desarrollo y soporte

Mantiene la seguridad del software de aplicación del sistema y de la información. Los ambientes de soporte de proyectos son estrictamente controlados.

2.11.8.6. Gestión de vulnerabilidad técnica

Reduce riesgos resultantes de la exploración de vulnerabilidades de técnicas publicadas.

2.11.9. Gestión de incidentes de seguridad de la información

Los controles de la gestión de incidentes de seguridad de la información son: (1) reporte de los eventos y debilidades en la seguridad de la información y (2) gestión de incidentes y mejora de seguridad de la información.

2.11.9.1. Reporte de los eventos y debilidades en la seguridad de la información

Asegura que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de manera que permita tomar la acción correctiva a tiempo.

2.11.9.2. Gestión de los incidentes y mejora de seguridad de la información

Asegura que un consistente y efectivo acercamiento sea aplicado a la gestión de incidentes de seguridad de la información.

2.11.10. Gestión de Continuidad del Negocio

La gestión de continuidad del negocio tiene como control a los aspectos de seguridad de la información en la gestión de continuidad del negocio.

2.11.10.1. Aspectos de seguridad de la información en la gestión de continuidad del negocio

Cuyo objetivo es contrarrestar las interrupciones de las actividades del negocio y para proteger los procesos críticos del negocio de los efectos de las principales fallas de sistemas de información o de desastre y para asegurar su oportuna reanudación.

2.11.11 Cumplimiento

Considera los controles: (1) cumplimiento de requisitos legales, (2) cumplimiento con las políticas y normas de seguridad y cumplimiento técnico, y (3) consideraciones de la Auditoria de los sistemas de información.

2.11.11.1. Cumplimiento de Requisitos Legales

Su objetivo es evitar la violación de cualquier ley, de obligaciones estatuarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

2.11.11.2. Cumplimiento con las políticas y normas de seguridad y cumplimiento técnico

Asegura que los sistemas cumplen con las políticas y normas de seguridad de la organización.

2.11.11.3. Consideraciones de la auditoria de los sistemas de información

Maximiza su efectividad y minimizar las interferencias al/del proceso de auditoría de sistemas de información.

2.12. Norma Boliviana NB-ISO-IEC 27001[27]

Tecnología de la información- Técnicas de seguridad- Sistemas de Gestión de seguridad de la información- Requisitos (NB-ISO-IEC 27001).

Esta norma adopta un enfoque de procesos para establecer, implementar, realizar, hacer, seguimiento, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) de una institución.

Este "enfoque de proceso" es la identificación e interacciones de estos procesos.
La norma NB-ISO-IEC 27001 adopta el modelo Planear-Hacer- Verificar-Actuar (PHVA), que se aplica para estructurar todos los procesos.

[27][ISO 27001, 2007] Norma Boliviana.

Planificar (Establecer el SGSI)	Establecer la política, los objetivos, los procesos y los procedimientos relacionados a la gestión de riesgo y la mejora de la seguridad de la información para

	entregar resultados.
Hacer (Implementar y realizar el SGSI)	Implementar y realizar la política, los controles, procesos y procedimientos.
Verificar (Hacer el seguimiento y revisar el SGSI)	Evaluar y, cuando sea aplicable, medir el desempeño del proceso frente a la política, objetivos y experiencia práctica del SGSI, e informar de los resultados para la revisión por la dirección.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la Auditoría interna del SGSI y la revisión de la dirección u otra información relevante, para alcanzar la mejora continua del SGSI.

Tabla 2.12 Procesos Normas NB-ISO-IEC 27001

2.13. Auditoria

2.13.1. Definición

El termino de Auditoria empleada en el área Financiera, con frecuencia solo se la considerada como una evaluación, cuyo único fin era detectar errores y señalar fallas[28].
Pero la auditoria y el control van más allá de detectar fallas.

La auditoria no solo detecta errores: “es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar acciones alternativas para mejorar la organización y lograr los objetivos propuestos”[29].

[28]Las fallas pueden ser en manejo de la información, controles, etc.

[29][Montgo, 1997].

Según la Norma Gubernamental Boliviana, la auditoria es “la acumulación y evaluación objetiva de evidencia para establecer e informar sobre el grado de correspondencia entre la información examinada y criterios establecidos”[30].

Algo importante de la auditoria es que “se evaluar para mejorar lo existente, corregir y proponer alternativas de solucion”[31].

Por lo que la auditoria no se reduce a la simple evaluación y señalamiento de errores, actualmente la auditoria se realiza a distintas áreas y desde distintos puntos de vista.

2.13.2. Clases de Auditoria[32]

La Auditoria se clasifica desde diversos puntos de vista, (1) por su amplitud, (2) por su frecuencia, (3) según el sujeto, (4) según el contenido y fines.

2.13.2.1. Por su amplitud son:

- Auditoria total: Afecta a todos los elementos de la empresa.
- Auditoria parcial: Se concentra en determinados elementos de la empresa.

2.13.2.2. Por su frecuencia, la auditoria es permanente u ocasional

- Auditoria permanente: Se realiza periódicamente a lo largo del ejercicio económico.
- Auditoria ocasional: Se realiza de forma esporádica.

[30][NGAG, 2005] Normas Generales de Auditoria Gubernamental, Contraloría General de la República de Bolivia.

[31][ECHENI, 2001] *Auditoría en Informática, Echenique García José Antonio.*

[32][JNAVA, 2007] Apuntes de Auditoria Informática.

2.13.2.3. Según el sujeto que la efectúa, la auditoria es interna y externa

- Auditoría interna: Está a cargo de empleados de la propia empresa, encuadrados en un departamento directamente dependiente de la dirección general.
- Auditoría externa: está a cargo de auditores profesionales, ajenos a la empresa y totalmente independientes.

2.13.2.4. Por su contenido y fines

- Auditoría de gestión: Afecta a la situación global de la empresa
- Auditoría financiera: Examen y verificación de los estados financieros de la empresa, para emitir una opinión fundada sobre el grado de la fiabilidad de dichos estados.
- Auditoría contable: Analiza la adecuación de los criterios empleados para recoger los hechos derivados de la actividad de la empresa y su representación, mediante apuntes contables, en los estados financieros.
- Auditoria operacional: Determina hasta que punto una organización, una unidad o función dentro de una organización, cumple los objetivos establecidos por la gerencia; así como identificar las condiciones que necesiten mejora.

Se extiende a todas las áreas o campos de trabajo como ser:

- Auditoria organizativa: Analiza si la estructura organizativa de la empresa es la adecuada, según las necesidades y problemas de la misma.
- Auditoria informática: Examen y verificación del correcto funcionamiento y control del sistema informático de la empresa

En otras palabras, se acepta el término de auditoría para cualquier actividad que implique revisión, evaluación, análisis, estudio, exposición de deficiencias y propuesta de medidas para solucionar o eliminar las mismas.

En muchos casos, las fronteras entre los tipos de auditoría no están bien definidas.

2.14. Auditoria Informática

Según Ron Weber en Auditing Conceptual Foundations and Practice, la auditoria informática "es la revisión y evaluación de los controles, sistemas y procedimientos de la información de los equipos de computo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que sirva para una adecuada toma de decisiones" [33].

"La Auditoria Informática es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente"[34].

2.14.1. Tipos de Auditoria dentro de la Auditoria Informática

Dentro de la Auditoria Informática existen varios tipos de auditoría, entre ellas la auditoria física, auditoria de dirección, auditoria del desarrollo, auditoria de mantenimiento, auditoria de seguridad y otros.

[33][ECHENI, 2001].

[34][ECHENI, 2001] *Auditoría en Informática, Echenique García José Antonio.*

a) La Auditoria Física verifica, evalúa y comprueba la funcionalidad, racionalidad y seguridad de los medios físicos.

b) Auditoria de Dirección auditor examina el proceso de planificación de sistema de información y evalúa si razonablemente se cumplen los objetivos.
c) Auditoria del Desarrollo verifica y evalúa todo el ciclo de vida del software excepto: la exploración, el mantenimiento y el retiro del servicio o aplicación cuando esta tenga lugar.
d) Auditoria de Mantenimiento (Hardware y Software) es la evaluación de la protección y continuidad del normal funcionamiento de los soportes físicos y lógicos existentes en la organización, comprobación de la existencia de las políticas y procedimientos formales relativos al mantenimiento preventivo y correctivo del hardware, sistemas de información y red de comunicaciones dentro de la institución.
e) Auditoria de seguridad, Evalúa las medidas de protección de datos y de los sistemas computarizados, involucrando en forma global Hardware y Software, las medidas de protección a ser utilizadas y los planes de contingencia preparados para enfrentar problemas con o sin conocimiento de causa.

Al finalizar el trabajo de auditoría se obtiene un informe del estado de la institución o unidad auditada, en el desarrollo de la auditoria el auditor obtiene los papeles de trabajo o documentación que son parte de la evidencia que ayuda a sustentar su opinión.

2.15. Informe de Auditoria

El Informe de Auditoría es el objetivo de la Auditoria Informática en sí.
El auditor define los objetivos del trabajo a realizar basado en un diagnostico previo que incluya tanto a la institución, como a las tecnologías involucradas en la satisfacción de necesidades de información automatizada para su gestión.

La información recopilada le sirve para obtener un entendimiento de las debilidades de control y/o situaciones de interés que se presentan. Tanto el trabajo deber ser documentado.

- Documentación o papeles de trabajo, que conserva la información de cada auditoria y puede ser organizada de la siguiente manera:
  - Archivo permanente, se almacena la información que es útil para conocer la empresa en sus aspectos generales y sirve de orientación para cualquier contacto con ella.
  - Archivo de auditoría en curso, para cada auditoria se abre uno, cuando acaba la auditoria se ve la documentación que tiene aspecto permanente y pasa a otra carpeta o archivo.
- Evidencia, es la base razonable de la opinión del Auditor Informático.

2.15.1. Tipos de Dictamen de Informe[35]

En todos los casos en que un auditor realiza una revisión, debe expresar una opinión. La opinión, diagnostico o dictamen es la expresión emitida acerca del resultado del proceso de auditoría.
Existen cuatro formas de dictaminar:

2.15.1.1. Dictamen favorable o limpio

La opinión calificada como favorable, sin salvedades o limpia deber manifestarse de forma clara y precisa, es el resultado de un trabajo realizado sin limitaciones de alcance y sin incertidumbre, de acuerdo con la normativa legal y profesional.
Si existen circunstancias que afectan de alguna manera, y no son lo suficientemente importantes como para generar una opinión adversa, se debe incluir un párrafo explicativo y establecer una opinión con salvedades.

[35][PIATTINI, 2001] Capitulo 4: “El informe de Auditoría” y [PROFAGER, 2007].

2.15.1.2. Opinión con salvedad

Se reitera lo dicho en la opinión favorable, al respecto de las salvedades cuando sean significativas en relación con los objetivos de auditoría, describiéndose con presión la naturaleza y razones, se realiza según las circunstancias siguientes:

- ✓ Limitaciones al alcance del trabajo realizado, restricciones por parte del auditado.
- ✓ Incertidumbres cuyo resultado no permita una previsión razonable.
- ✓ Irregularidades significativas.
- ✓ No hay suficiente evidencia comprobatoria.
- ✓ No hay notas aclaratorias.

2.15.1.3. Opinión desfavorable o adversa

Establece que no presenta razonablemente los resultados de las operaciones de la entidad, de conformidad con principios generalmente aceptados.

Las excepciones son más importantes que no le permite emitir una opinión con salvedades, por lo que se incluye los motivos o razones técnicas que le orientan a emitir este tipo de dictámenes y los efectos que significan.

La opinión desfavorable o adversa es aplicable en el caso de:

- Identificación de irregularidades.
- Incumplimiento de la normativa legal y profesional que afecten significativamente a los objetivos de auditoría informática estipulados, incluso con incertidumbre; todo ello en la evaluación de conjunto y reseñando detalladamente las razones correspondientes

2.15.1.4. Opinión denegada o abstención de opinión

Establece que el auditor no expresa una opinión, normalmente por los siguientes motivos:

- Incertidumbres significativas de un modo tal que impida al auditor formarse una opinión.
- Irregularidades.
- Limitación en el alcance de la auditoria.
- La existencia de incertidumbre cuando su importancia es significativa.
- La trascendencia que tiene el riesgo de que la empresa no pueda seguir en operación.
- Falta de información.
- Incumplimiento de normativa legal y profesional.

Para realizar la auditoria, se desarrolla un plan de trabajo el cual es revisado y desarrollado de acuerdo a la experiencia y habilidad del auditor. También requiere de una Metodología de evaluación, que permita realizar el trabajo de evaluación del área de informática.

2.16. Metodologías de Evaluación en Informatica[36]

Para lograr un nivel alto de seguridad" se utilizan las metodologías necesarias para realizar un plan de seguridad" y las dos Metodologías de Evaluación por antonomasia son de Análisis de Riesgos y de Auditoria Informática.

2.16.1. Metodologías de Análisis de Riesgos

El análisis de riesgos es un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una institución.

[36][PIATTINI, 2001] Capitulo 3 Pag. 49.

La metodología de Análisis de Riesgos, es una herramienta de gestión o de toma de decisiones, antes de desplegar un servicio o cuando está en funcionamiento, es deseable hacerlo antes, de forma que las medidas se incorporen en el diseño del servicio, en la elección de componentes, en el desarrollo de aplicaciones y en manuales de usuario.

Todo lo que sea corregir riesgos imprevistos es costoso en tiempo propio y ajeno, lo que va en detrimento de la imagen prestada por la institución y supone, en último extremo, la pérdida de confianza en su capacidad. Un representante de esta metodología es:

12.16.1.1. Magerit[37]

El Consejo Superior de Administración Electrónica (CSAE) ha elaborado y promueve la "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" (MAGERIT); esta metodología permite conocer, evaluar y valorar el riesgo al que están sometidos y así poder gestionarlos ayudando a protegerlos, trabaja con un esquema repetitivo donde a través del análisis de riesgos, los objetivos y estrategias permite elaborar un plan de seguridad que implantado y operado, satisface los objetivos propuestos con un nivel de riesgos aceptable para la Dirección.

2.17. Metodología de Auditoria Informática

La metodología de Auditoria informática consiste en la recolección de pruebas suficientes para que el auditor emita un dictamen acerca del objeto de evaluación. Una metodología de Auditoria informática es:

[37][MAGERIT, 2006].

2.17.1. Cobit[38]

La Asociación de Control de Sistemas de Información y Auditoria (ISACA[39]) propone la metodología de Control de Objetivos de Información y Tecnologías Relacionadas (COBIT) como un recurso educacional para los profesionales, el cual brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, tiene como objetivos de control[40] la efectividad y eficiencia de las operaciones; confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones. COBIT es una metodología realizada a nivel internacional que permite a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes, permite el desarrollo de políticas claras y de buenas prácticas para control de Tecnologías de Información (TI) a través de las empresas.

2.18. Metodología Cobit

2.18.1. Estructura de la Metodología Cobit[41]

Cobit define las actividades de Tecnología de Información (TI) es un modelo genérico de procesos, estos son cuatro dominios fundamentales de la metodología y tiene distribuidos treinta y cuatro Objetivos de control generales:

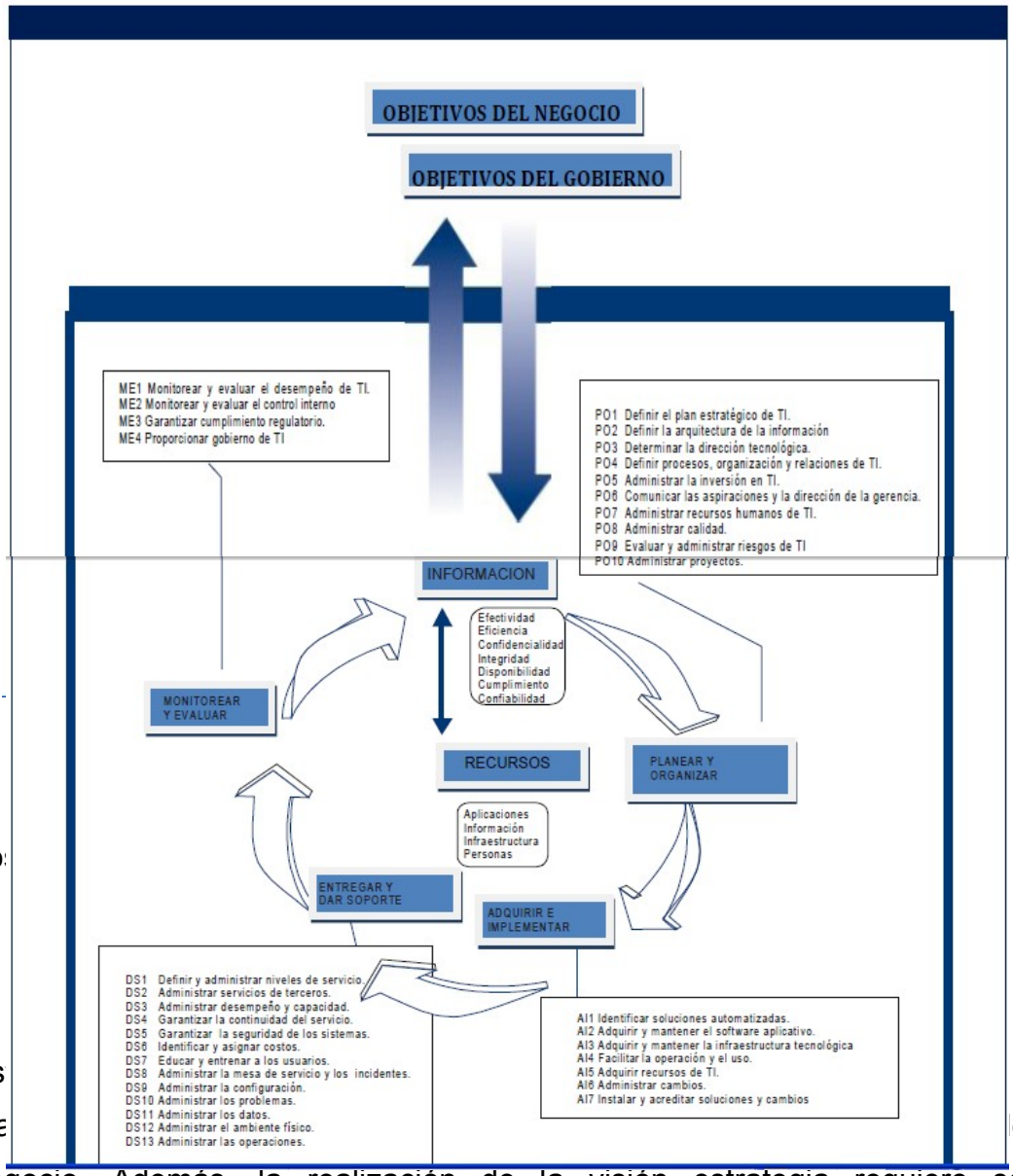
- Planear y Organizar.
- Adquirir e Implementar.
- Entregar y Dar Soporte.
- Monitorear y Evaluar.

[38][COBIT, 2002] y [COBIT 4.0, 2005].

[39]ISACA en ingles “Information Systems Audit and Control Association” es una organización líder de profesionales que presenta a individuos en más de 100 países.

[40]Un objetivo de control es un estatuto del resultado o propósito que se desea alcanzar al implantar procedimientos de control es un proceso en particular.

[41][COBIT 4, 2005].



Lo

Es la

ma el

negocio. Además, la realización de la visión estrategia requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se implementa una estructura organizacional y una estructura tecnológica apropiada.

Los Objetivos de control de este dominio son:

- PO1 Definir un plan estratégico de TI.
- PO2 Definir la arquitectura de la información.
- PO3 Determinar la dirección tecnológica.
- PO4 Definir los procesos, organización y relaciones de TI.

- PO5 Administrar la inversión de TI.
- PO6 Comunicar las aspiraciones y la dirección de la gerencia.
- PO7 Administrar recursos humanos de TI.
- PO8 Administrar la calidad.
- PO9 Evaluar y administrar los riesgos de TI.
- PO10 Administrar proyectos.

2.18.1.2. Adquirir e Implementar (AI)

Las soluciones de Tecnologías de Información necesitan ser identificadas, desarrolladas o adquiridas, así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones satisfacen los objetivos del negocio.

Los Objetivos de control de este dominio son:

- AI1 Identificar soluciones automatizadas.
- AI2 Adquirir y mantener software aplicativo.
- AI3 Adquirir y mantener infraestructura tecnológica.
- AI4 Facilitar la operación y el uso.
- AI5 Adquirir recursos de TI.
- AI6 Administrar cambios.
- AI7 Instalar y acreditar soluciones y cambios.

2.18.1.3. Entregar y dar Soporte (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye en la prestación del servicio, la administración de seguridad y continuidad, el soporte del servicio a los usuarios, la administración de datos e instalaciones operacionales.

Los Objetivos de Control de este dominio son:

- DS1 Definir y administrar los niveles de servicio.
- DS2 Administrar los servicios de terceros.
- DS3 Administrar el desempeño y la capacidad.
- DS4 Garantizar la continuidad del servicio.
- DS5 Garantizar la seguridad de los sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar a los usuarios.
- DS8 Administrar la mesa de servicio y los incidentes.
- DS9 Administrar la configuración.
- DS10 Administrar los problemas.
- DS11 Administrar los datos.
- DS12 Administrar el ambiente físico.
- DS13 Administrar las operaciones.

2.18.1.4. Monitorear y Evaluar (ME)

Todos los procesos de TI se evalúan de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Los Objetivos de control de este dominio son:

- ME1 Monitorear y evaluar el desempeño de TI.
- ME2 Monitorear y evaluar el control interno.
- ME3 Garantizar el cumplimiento regulatorio.
- ME4 Proporcionar gobierno de TI.

2.19. Modelos de Madurez[42]

El modelo de madurez facilita la evaluación por medio de la identificación de mejoras necesarias en la capacidad, permite la evaluación desde un nivel de (0) no existente, hasta un nivel (5) equivalente a optimizado. La ventaja del modelo de madurez, es su fácil de uso para la dirección porque permite evaluar y ubicarse a sí misma en la escala.

[42][COBIT 4.0, 2005].

Escala	Descripción
0 **No existente.**	Carencia completa de proceso reconocible. La empresa no reconoce que existe un problema a resolver.
1 **Inicial**	Existe evidencia que la empresa reconoce que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar, en su lugar existen enfoques que son aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible	Se han desarrollado procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No existe entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos y es poco probable que se detecten desviaciones. Los procedimientos en si no son sofisticados pero formalizan las prácticas existentes.
4 Administrado	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizado	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en resultados de mejoras continuas y en modelos de madurez de otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, hace que la empresa se adapte de manera rápida.

Tabla 2.19. Escala de Valores

2.20. Metodología

La Metodología de trabajo para la construcción del modelo de Auditoria Informática para la seguridad física, consta de cuatro etapas: (1) Análisis, (2)

Diseño, (3) Desarrollo y (4) Prueba, en cada una de ellas se describe el objetivo, la entrada y salida, para la comprensión de la metodología.

Etapa	Objetivo	Entrada	Resultado
Análisis Análisis de modelos, normas y estándares	Obtener un panorama general de modelo, establecer su importancia.	Modelos base para la construcción del nuevo modelo: Norma ISO 27001 Norma ISO 27002 Modelo COBIT	Síntesis del modelo conocimiento de los modelos.
Análisis Delimitación del campo.	Definir el alcance y límites para el campo de trabajo.	Modelos en estudio	Delimitación del área de trabajo.
Diseño Identificación de procesos y controles.	Identificar procesos y controles para el nuevo modelo.	Delimitación del área del trabajo, con la selección de controles y procesos del nuevo modelo.	Obtención de los Controles y Procesos relevantes para el modelo en seguridad física.
Desarrollo Desglose de los lineamientos.	Desglosar y detallar (Lineamientos) los modelos en estudio.	Modelos en estudio y modelos complementarios referentes al área de trabajo.	Obtención de las especificaciones de lineamientos para el modelo propuesto
Desarrollo Estructuración de controles y procesos.	Estructurar, construir los controles y procesos.	Lineamientos desglosados	Estructuración Objetivos de Control del nuevo Modelo
Desarrollo Elaboración de escalas de evaluación	Elaborar escalas de evaluación	Objetivos de Control del nuevo Modelo Propuesto	Herramientas de evaluación del Modelo propuesto.
Prueba Revisión del Modelo.	Validar las herramientas del modelo, a través de pruebas.	Herramientas de evaluación del Modelo propuesto.	Validación de Herramientas de evaluación y del modelo.
Concreción del Modelo	Obtener el Modelo Final	Objetivos de control y herramientas de evaluación validadas.	Modelo Final de Auditoría Informática para la seguridad Física

Capítulo III Marco Aplicativo

Capítulo III Marco Aplicativo

3. Diseño y Construcción del Modelo de Auditoria Informática para la Seguridad Física

El Modelo de Auditoria Informática para la Seguridad Física que se propone en la tesis es una estructura teórica que permite establecer, realizar, implementar medidas de protección física, para la información y los recursos físicos que se encuentran directamente relacionados con el almacenamiento de la información.

El presente Modelo de Auditoria Informática para la Seguridad Física está basado en los conceptos de:

1) ISO 27001.
2) ISO 27002.
3) COBIT.
4) Norma de Auditoria Gubernamental.

3.1. Características del Modelo

El modelo propuesto tiene tres características que se detallan a continuación.

- Los requisitos establecidos en el Modelo de Auditoria Informática para la Seguridad Física son genéricos y están previstos a ser aplicables en toda institución independientemente del tipo, tamaño y su naturaleza.
- Está enfocada a las unidades de sistemas, la auditoria informática es amplia y se aplica en todas las áreas donde intervienen las tecnologías, el procesamiento de la información y los sistemas, sin embargo debido a las características de la seguridad física para la información se aplica normas y practicas exclusivamente para la seguridad física de la información.

- Adecuado a nuestra realidad, ya que el modelo considera las recomendaciones de las normas bolivianas e internacionales.

De acuerdo a estas consideraciones, el modelo propuesto evalúa de forma completa la seguridad física de acuerdo a los conceptos ya mencionados de los estándares internacionales y bolivianos.

El modelo propuesto requiere de la construcción de objetivos de control y herramientas propias que estén de acuerdo a los conceptos que maneja, para esto se realiza.

- ✓ El diseño y construcción de objetivos de control para la seguridad física.
- ✓ El diseño y construcción de herramientas del modelo.
- ✓ El diseño y construcción del modelo de seguridad física.
- ✓ El diseño y construcción de las etapas de la Auditoria Informática.

3.2. Diseño y Construcción de Objetivos de control para la Seguridad Física

Para el modelo propuesto en este punto se selecciona objetivos de control de los modelos COTIB y NB-ISO-IEC 27002, de forma que garantice la evaluación de la seguridad física de los recursos de información.

Del modelo internacional COBIT se hace el análisis y selección de objetivos de control de controles detallados que contemplan aspectos de seguridad física. Cabe aclarar que muchos aspectos de COBIT ya son contemplados en el modelo NB-ISO-IEC 27002, pero existen aspectos que no son tomados en cuenta, los cuales se adicionan a las clausulas y objetivos de control del modelo NB-ISO-IEC 27002.

El modelo NB-ISO-IEC 27002 es la norma dedicada a la seguridad de la información, lo que permite alinear de mejor manera el modelo propuesto a la seguridad física, de este modelo la clausula fundamental para garantizar la seguridad física es: Seguridad física y ambiental, pero no se debe dejar de lado aspectos organizacionales que cooperen con esta clausula.

En consecuencia para el modelo propuesto se selecciona 10 de las 11 clausulas que tiene la norma NB-ISO-IEC 27001 se excluye 1 clausula completa y los objetivos de control y sub controles que están dirigidos a la parte de seguridad lógica, teniendo así clausulas y controles exclusivamente para el apoyo de la seguridad física de los recursos de información.

Objetivos de control ISO 27002	
5	5.1. Política de seguridad de la información.
6	6.1. Organización Interna.
	6.2. Partes externas.
7	7.1. Responsabilidad por los recursos.
	7.2. Clasificación de la información.
8	8.1. Previo al empleo.
	8.2. Durante el empleo.
	8.3. Finalización o cambios de empleado.
9	9.1. Áreas Seguras.
	9.2. Seguridad del equipo.
10	10.1. Procedimientos y responsabilidades operacionales.
	10.2. Gestión de entrega de servicio de tercera parte (No tomado en cuenta).
	10.3. Planificación y aceptación del sistema (No tomado en cuenta).
	10.4. Protección contra código malicioso y móvil (No tomado en cuenta).
	10.5. Respaldo.
	10.6. Gestión de seguridad de redes (No tomado en cuenta).
	10.7. Manejo de medios.
	10.8. Intercambio de información (No tomado en cuenta).
	10.9. Servicios de comercio electrónico (No tomado en cuenta).
	10.10. Seguimiento (No tomado en cuenta).
11	11.1. Requisitos del negocio para el control de acceso.
	11.2. Gestión de accesos a usuarios.
	11.3. Responsabilidad de los usuarios.
	11.4. Control de acceso a redes (No tomado en cuenta).
	11.5. Control de acceso al sistema operativo (No tomado en cuenta).
	11.6. Control de acceso a las aplicaciones y a la información (No tomado en cuenta.
	11.7. Computación móvil y trabajo remoto (No tomado en cuenta).
12	12. Adquisición, desarrollo y mantenimiento de los sistemas de información.
13	13.1. Informe sobre los eventos y debilidades de seguridad de la información.
	13.2. Gestión de los incidentes y mejoras de seguridad de la información.
14	14. Gestión de continuidad del negocio.
15	15.1. Cumplimiento de requisitos legales.
	15.2. Cumplimiento con normas y políticas de seguridad y cumplimiento técnico.
	15.3. Consideraciones de la auditoria de sistemas.

Tabla 3.2. Objetivos de Control de COBIT

	COBIT
PO	PO1 Definir un plan estratégico de TI.
	PO2 Definir la arquitectura de la información.
	PO3 Determinar la dirección tecnológica.
	PO4 Definir los procesos, organización y relaciones de TI.
	PO5 Administrar la inversión de TI.
	PO6 Comunicar las aspiraciones y la dirección de la gerencia.
	PO7 Administrar recursos humanos de TI.
	PO8 Administrar la calidad.
	PO9 Evaluar y administrar los riesgos de TI.
	PO10 Administrar proyectos.
AI	AI1 Identificar soluciones automatizadas (No tomado en cuenta).
	AI2 Adquirir y mantener software aplicativo (No tomado en cuenta).
	AI3 Adquirir y mantener infraestructura tecnológica.
	AI4 Facilitar la operación y el uso (No tomado en cuenta).
	AI5 Adquirir recursos de TI (No tomado en cuenta).
	AI6 Administrar cambios (No tomado en cuenta).
	AI7 Instalar y acreditar soluciones y cambios (No tomado en cuenta)
DS	DS1Definir y administrar los niveles de servicio.

	DS2 Administrar los servicios de terceros.
	DS3 Administrar el desempeño y la capacidad
	DS4 Garantizar la continuidad del servicio.
	DS5 Garantizar la seguridad de los sistemas.
	DS6 Identificar y asignar costos.
	DS7 Educar y entrenar a los usuarios.
	DS8 Administrar la mesa de servicio y los incidentes.
	DS9 Administrar la configuración.
	DS10 Administrar los problemas.
	DS11 Administración de la información sí.
	DS12 Administrar el ambiente físico.
	DS13 Administrar las operaciones.
ME	ME1 Monitorear y evaluar el desempeño de TI.
	ME2 Monitorear y evaluar el control interno.
	ME3 Garantizar el cumplimiento regulatorio.
	ME4 Proporciona gobierno de TI.

Tabla 2.2.1 Objetivos de Control Norma ISO 27002

Según los modelos ISO 27002 y COBIT	Nº	Objetivos de Control Propuesto
ISO 27002 – 5 y COBIT - PO6	1	1.1 Política de seguridad de la información Comunicar las aspiraciones y la dirección de la gerencia. Definir un plan estratégico de TI Definir los procesos, organización y relaciones de TI
COBIT - PO1		
COBIT - PO4		
ISO 27002 – 6.1 es equivalente a COBIT - DS1	2	2.1 Organización Interna Definir y administrar los niveles de servicio
ISO 27002 - 6.2 es equivalente a COBIT - DS2		2.2 Partes externas Administrar los servicios de terceros

Tabla 3.2.2. Objetivos de Control Modelo Propuesto

En el Capitulo Concreción del Modelo, se detallada las clausulas y contenido de los objetivos de control obtenidos y descritos.

3.3. Diseño y Construcción de Herramientas del Modelo

Los instrumentos o herramientas para el relevamiento de información son diversos, entre ellas están la observación, cuestionario, entrevistas, checklist y otras.

Para el modelo propuesto se elabora instrumentos de evaluación y de relevamiento de información. Estos instrumentos están de acuerdo a las clausulas y objetivos de control diseñados.

Los instrumentos propuestos son:

- Hojas de evaluación.
- Hojas de relevamiento de información.

3.3.1. Escala de Evaluación

Los niveles de seguridad se establecen para clasificar a una institución, para ello se elabora una Tabla Escala de Clasificación.

Según los parámetros de evaluación tomados del modelo de madurez

0	1	2	3	4	5

Tabla 3.3.1. Escala de Evaluación

Los valores 0 y 1 representan los puntajes mínimos, 2 y 3 son puntajes intermedios, 4 y 5 puntajes altos, estos valores son llevados a escalas porcentuales, de donde resulta el nivel bajo 0-39, nivel medio 40-79 y nivel alto de 80-100.

Nivel porcentual	Nivel de seguridad
0-39	Nivel Bajo de seguridad
40-79	Nivel Medio de seguridad
80-100	Nivel Alto de seguridad

Tabla 3.3.2. Escala de Clasificación

Estas escalas se utilizan para identificar el nivel de seguridad física de una institución.

3.3.2. Hojas de Evaluación

Las Hojas de evaluación constituye el instrumento de evaluación, en ellas se llena toda la información recolectada.

Siguiendo las escalas de clasificación del Modelo de Madurez[43], en la hoja de evaluación se selecciona y marca la opinión que representa el comportamiento actual de la institución. Luego se coloca en la columna Total el valor que indique la X, al final se obtiene el resultado total de la evaluación.

Hoja de Evaluación								
	CLAÚSULA: Gestión de Comunicaciones y Operaciones							
	CONTROL PRINCIPAL: Respaldo							
Nº	SUB - CONTROL: Respaldo de información							
I		Evaluación						Total
		0	1	2	3	4	5	
1	Se hace copias de respaldo de la información y se pone a prueba regularmente.		X					1
2	Se realizan registros exactos y completos de las copias de respaldo y procedimiento documentado de restauración.	X						0
3	Los respaldos se almacenan a una distancia suficiente para evitar el daño o desastre que ocurra en el predio principal.			X				2
4	A la información de respaldo se le da un nivel apropiado de protección física y ambiental.		X					1
	RESULTADO TOTAL DE LA EVALUACIÓN							3

[43]Citado y

3

Obtenie ır el resultado en un valor porcentual con la siguiente ecuación:

$$X=\frac{\sum p_i = 100}{N}$$

Ecuación III.1.

Donde:

X= Nivel de objeto de control
i= al número de preguntas
p= puntaje
$p_{i=}$ puntaje de la pregunta i
n= valor de la tabla, se obtiene de la siguiente manera: n=5* i

La ecuación se aplica para encontrar el equivalente porcentual de todas las hojas evaluadas, posteriormente se saca el valor promedio de las hojas de evaluación (El promedio es igual a la sema de todos los valores dividido

entre en total d hojas de evaluación usadas), este valor final encontrado se identifica en la escala de clasificación e identifica el nivel en el que se encuentra la seguridad física de la institución.

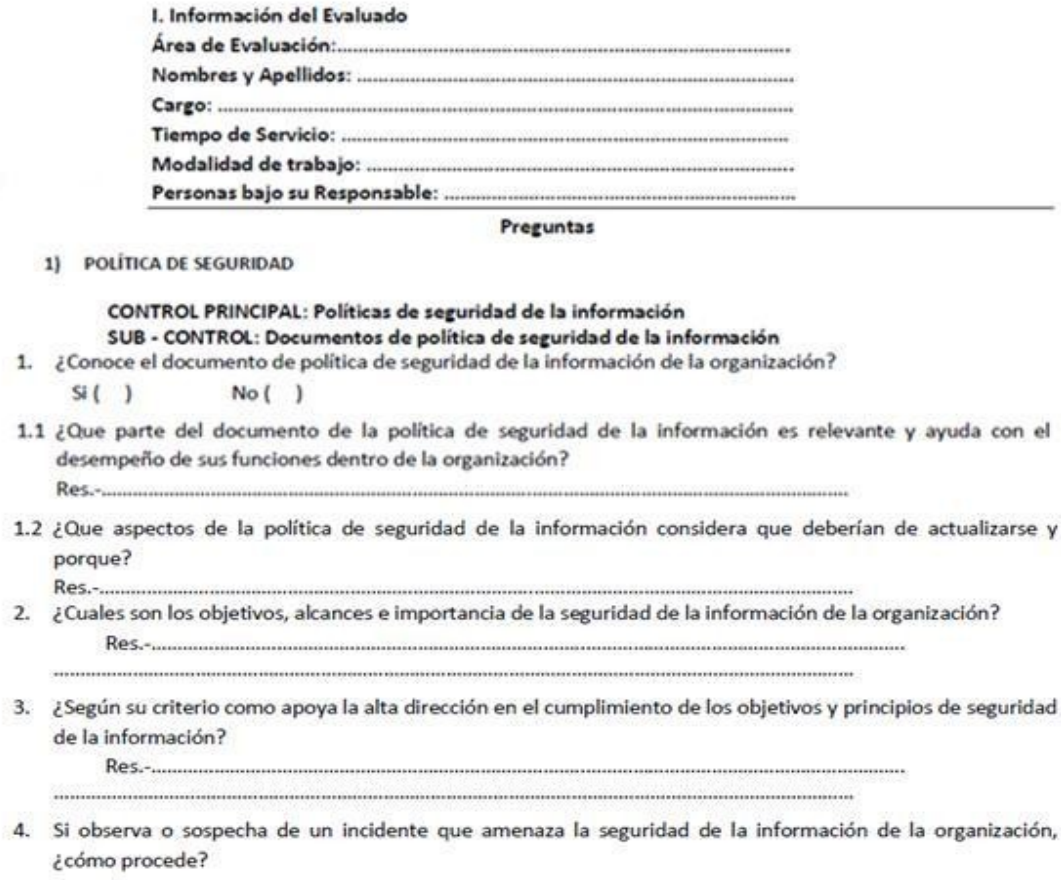
3.3.3. Hojas de relevamiento de información

Representan parte de los papeles de trabajo del auditor que le servirá para sustentar su opinión.

Las hojas de relevamiento de información son cuestionarios elaborados en base a los objetivos de control del modelo propuesto.

En las hojas de relevamiento de información existen preguntas abiertas y cerradas según el nivel de conocimiento que se desea evaluar.

Estas hojas de relevamiento de información sirven para llenar parte de las Hojas de evaluación, la otra parte son complementadas con la revisión de la documentación existente en la institución.



I. Información del Evaluado

Área de Evaluación:.....
Nombres y Apellidos: .....
Cargo: .....
Tiempo de Servicio: .....
Modalidad de trabajo: .....
Personas bajo su Responsable: .....

Preguntas

1) POLÍTICA DE SEGURIDAD

CONTROL PRINCIPAL: Políticas de seguridad de la información
SUB - CONTROL: Documentos de política de seguridad de la información

1. ¿Conoce el documento de política de seguridad de la información de la organización?
   Si ( ) No ( )

1.1 ¿Que parte del documento de la política de seguridad de la información es relevante y ayuda con el desempeño de sus funciones dentro de la organización?
Res.-.....

1.2 ¿Que aspectos de la política de seguridad de la información considera que deberían de actualizarse y porque?
Res.-.....

2. ¿Cuales son los objetivos, alcances e importancia de la seguridad de la información de la organización?
   Res.-.....
   .....

3. ¿Según su criterio como apoya la alta dirección en el cumplimiento de los objetivos y principios de seguridad de la información?
   Res.-.....
   .....

4. Si observa o sospecha de un incidente que amenaza la seguridad de la información de la organización, ¿cómo procede?
   Res.-

Figura 3.3.3. Hojas de Relevamiento de Información

La Figura 3.3.3. Es un ejemplo de las Hojas de relevamiento de información, existe un compendio completo que se mostrara en el siguiente Capitulo Concreción del Modelo.

Siguiendo con la construcción del Modelo de Auditoria Informática para la Seguridad Física, se construye el modelo de seguridad física.

3.4. Diseño y Construcción del Modelo de Seguridad Física

El modelo garantiza la seguridad física de la información y los activos físicos que están relacionados con su almacenamiento.

De acuerdo a la norma NB.ISO-IEC 27001 debe cumplir con cinco requisitos fundamentales que son:

- Sistema de Gestión de la seguridad de la información (SGSI): Es necesario establecer un sistema de gestión de seguridad de la información.
- Responsabilidad de la dirección.
- Auditorías Internas.

- Revisión por la dirección del SGSI
- Mejora del SGSI.

3.4.1. El Sistema de Gestión de la seguridad de la información

Es necesario establecer un sistema de gestión de seguridad de la información EL SGSI está basado en el modelo del procesos Planificar, Hacer, Verificar y Actuar (PHVA) [44] modelo similar manejado por COBIT que son sus dominios Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, Monitorear y Evaluar.

[44]La fundamentación se encuentra en el capítulo del Marco teórico

Estableciendo el SGSI según el modelo Planificar, Hacer, Verificar y Actuar se tiene cuatro procesos principales que son:

- Planificación o Establecimiento.
- Implementar.
- Seguimiento y Revisión.
- Mantenimiento y Mejora.

Independientemente en cada proceso se tiene las actividades a realizar para lograr el SGSI.

3.4.1.1. Proceso de Planificación o Establecimiento

El proceso de Planeación del modelo propuesto esta según los principios que considera la norma NB-ISO-IEC 27001, esta norma es fundamental, trabaja en un esquema similar a la metodología COBIT.

La organización debe:

1. Definir el alcance y límites.

2. Definir una política.
3. Definir un plan estratégico.

Se debe definir el plan estratégico que es el conjunto de planes, acciones a realizar y el tiempo que requiere para lograr el objetivo propuesto.

4. Definir el enfoque de valoración del riesgo de la organización.
5. Identificar los riesgos.
6. Analizar y evaluar los riesgos.
7. Identificar y evaluar las opciones para el tratamiento de riego.
8. Seleccionar e implementar los objetivos de control y controles.

Este punto se establece controles detallados que dependen de la norma NB-ISO-IEC 27002 del cual se selecciona los objetivos de control y controles para la seguridad física de la información.

9. Obtener aprobación de la dirección sobre los riesgos residuales.
10. Obtener automatización de la dirección.
11. Preparar una declaración de aplicabilidad.

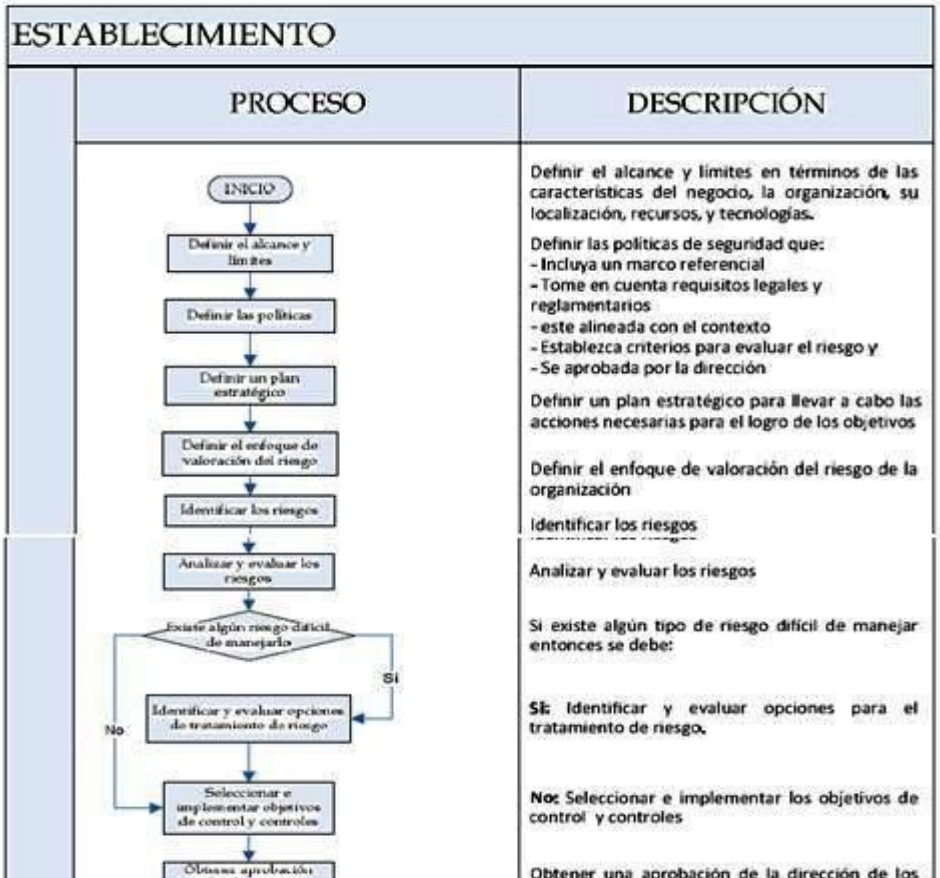


Figura 3.4.1.1. Proceso de Planificación o Establecimiento

3.4.1.2. Proceso Implementar

Según norma NB-ISO-IEC 27001 se debe:

1. Formular un plan de tratamiento de riesgo que identifique la acción de gestión apropiada los recursos, responsabilidades y prioridades para gestionar los riesgos de seguridad de la información.
2. Implementar el plan de tratamiento de riesgos para alcanzar los objetivos de control identificados, los cuales incluyen consideraciones a consolidar y asignar roles y responsabilidades.
3. Implementar los Objetivos de control diseñados (en el modelo propuesto), para alcanzar los objetivos de control.
4. Definir como medir la eficacia de los controles seleccionados o grupos de control y especificar como esas medidas se usan para valorar la eficacia del control para producir resultados comparables y reproducibles.
5. Implementar programas de formación y toma de conciencia.
6. Implementar procedimientos y otros controles capaces de permitir la detección rápida de eventos de seguridad y responder a incidentes de seguridad.

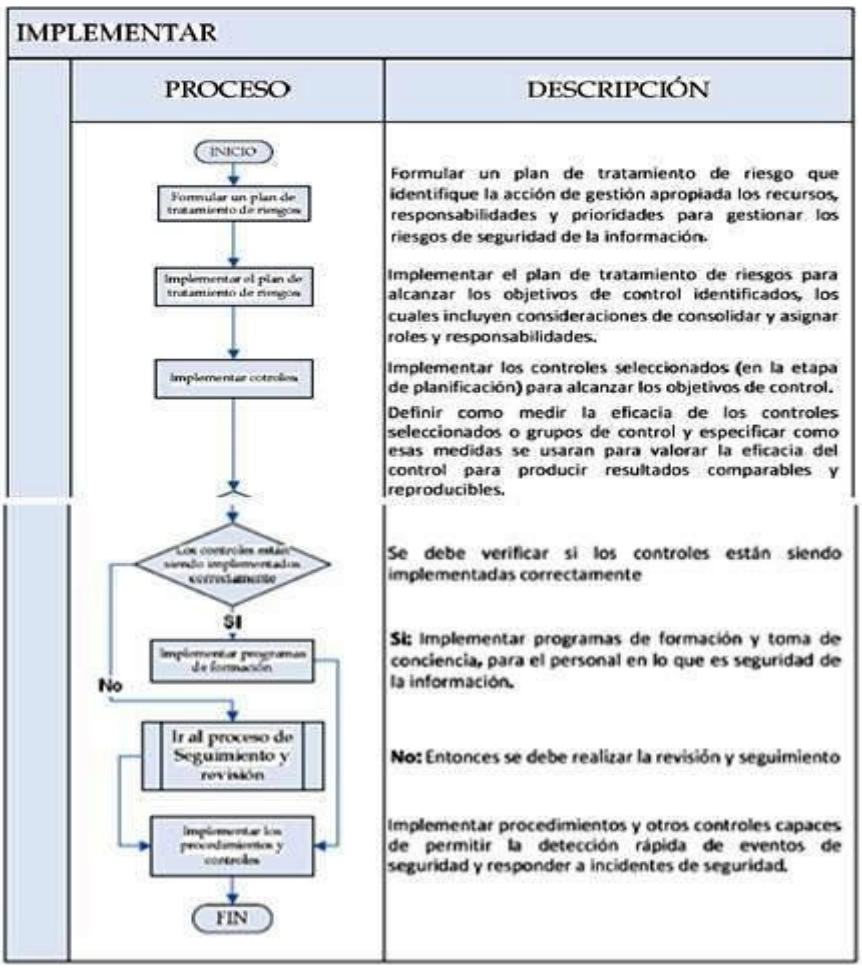


Figura 3.4.1.2. Proceso de Implementación

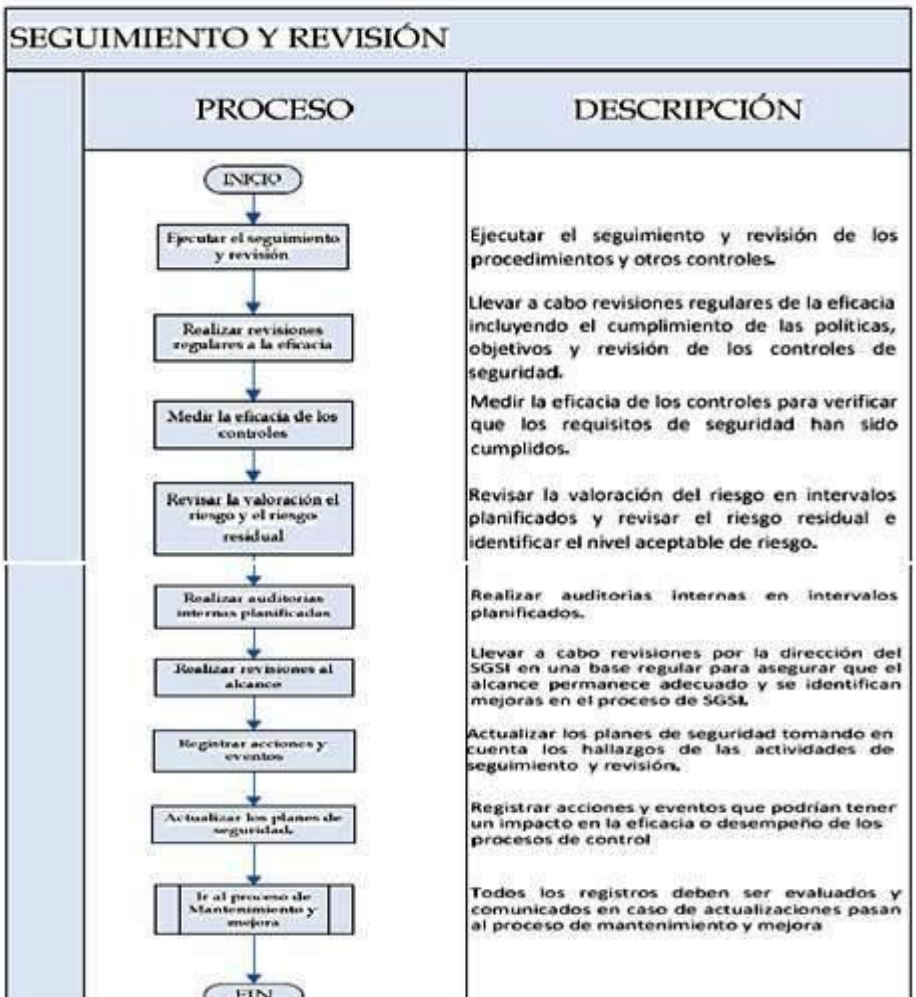
3.4.1.3. Proceso de Seguimiento y Revisión

1. Ejecutar el seguimiento y revisión de los procedimientos y otros controles.
2. Llevar a cabo revisiones regulares de la eficacia del SGSI incluyendo el cumplimiento de la política y objetivos de SGSI y revisión de los controles de seguridad tomando en cuenta los resultados de auditorías de seguridad, los incidentes, los resultados de la eficiencia

de las medidas, las sugerencias y la retroalimentación de todas las partes interesadas.

3. Medir la eficacia de los controles para verificar que los requisitos de seguridad han sido cumplidos.

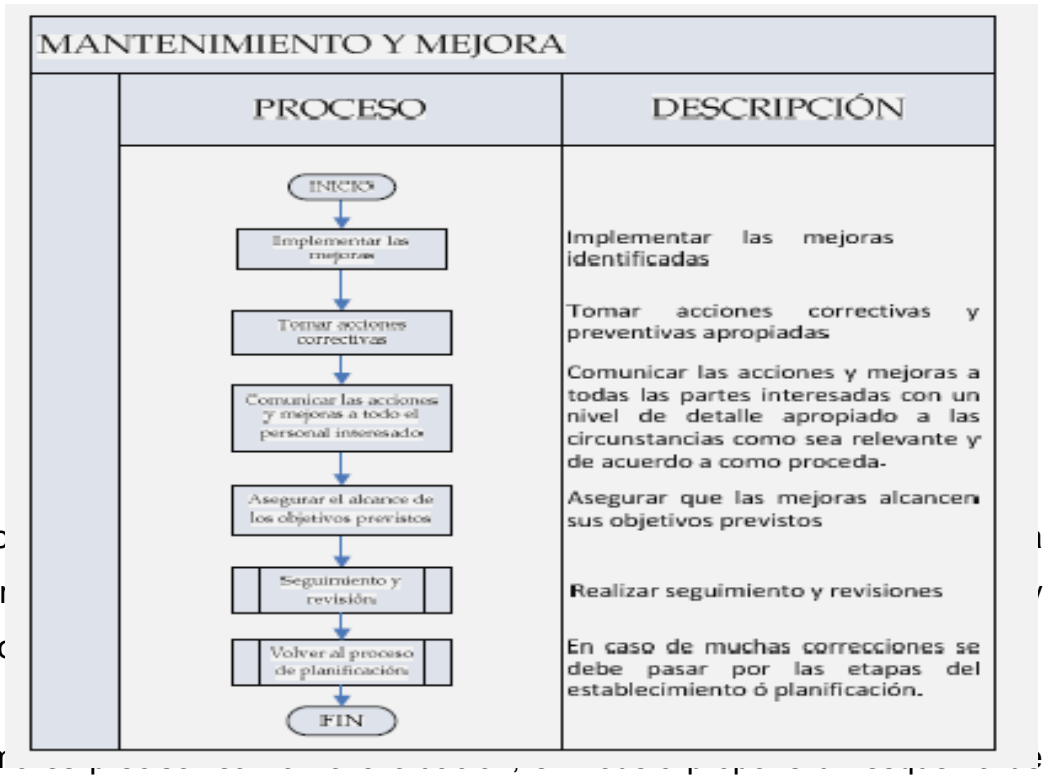
4. Revisar la valoración del riesgo en intervalos planificados y revisar el riesgo residual e identificar el nivel aceptable de riesgo tomando en cuenta cambios a la organización, la tecnología, objetivos y procesos de negocio.
5. Conducir auditorías internas al SGSI en intervalos planificados.
6. Llevar a cabo revisión por la dirección del SGSI en una base regular para asegurar que el alcance permanece adecuado y se identifican mejoras en el proceso de SGSI.
7. Actualizar los planes de seguridad tomando en cuenta los hallazgos de las actividades de seguimiento y revisión.
8. Registrar acciones y eventos que podrían tener un impacto en la eficacia o desempeño del SGSI.



3.4.1

1. In

2. Tomar acciones correctivas y preventivas apropiadas aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y de la propia organización.
3. Comunicar las acciones y mejoras a todas las partes interesadas con un nivel de detalle apropiado a las circunstancias como sea relevante y de acuerdo a como proceda.
4. Asegurar que las mejoras alcancen sus objetivos previstos.



Esto
Infor
mejo
Com

Trabajo para la ejecución de la Auditoria Informática.

3.5. Etapas de Auditoria Informática del Modelo de Auditoria Informática para la Seguridad Física

El modelo de auditoría es construido considerando los objetivos de la Norma de Auditoria Gubernamental.

El modelo presenta un esquema de trabajo en base a procesos, donde las actividades permiten la transformación de las entradas en salidas. Las salidas de un proceso forman parte de la entrada siguiente proceso directamente.

Por lo general se consideran tres procesos fundamentales que son: (1) Planificación, (2) Ejecución y (3) Revisiones e informe. Según los auditores y su metodología de trabajo existen otros procesos que adicionalmente pueden ser incorporados como: (4) Archivo y (5) Seguimiento.

El modelo propuesto considera cinco procesos, cada uno determinado de acuerdo a las actividades a desarrollar en cada etapa que son:

- ✓ Planificación.
- ✓ Ejecución o Implementación.
- ✓ Revisión.
- ✓ Comunicación Resultados.
- ✓ Seguimiento.

En cada una de estas etapas se identifica: (1) los elementos de entrada, (2) las actividades que se desarrollan durante la etapa y (3) los elementos de salida o resultados de la etapa.

3.5.1. Proceso de Planificación

3.5.1.1. Elementos de entrada del Proceso de Planificación

El inicio de una Auditoria Informática a la seguridad Física se da por:

- Que la Auditoria estaba planificada o
- Existe la demanda por parte de la Alta Dirección, quien aprueba de forma documentada de la realización de la Auditoria Informática en la Unidad de Sistemas.

Estos son los elementos que constituirán la entrada para la etapa de Planificación.

3.5.1.2. Proceso de la Planificación

Antes de iniciar la Auditoria Informática a la seguridad Física en la Unidad de Sistemas es necesario realizar una planificación y desarrollar un plan de trabajo para alcanzar satisfactoria y eficientemente los objetivos de la Auditoria Informática.

La planificación debe permitir un adecuado desarrollo de las etapas, se debe tomar conocimiento del sujeto y objeto a evaluar.

El auditor debe comprender el objeto de auditoría: las políticas, forma de registro, nivel de seguridad.

Se define el alcance y los objeticos de la auditoria, en esta investigación, se tiene definido la evaluación a la Seguridad Física de las Unidades de Sistemas.
Se diseña el plan de trabajo para el proceso de ejecución de la auditoria, para tal efecto se determina los procedimientos y pruebas que se ejecuta para la obtención de evidencias competente y suficiente.

En esta etapa el auditor debe solicitar los documentos de la organización.

3.5.1.3. Elementos de salida de la Planificación

Como resultado del proceso de planificación de la Auditoria Informática se tiene:

Un documento resumen el cual debe contener el o los objetivos del examen, el alcance y plan de trabajo el cual es usado durante la ejecución.

3.5.2. Proceso de Ejecución o Implementación

3.5.2.1. Elementos de entrada de la Ejecución o Implementación

El plan de trabajo de la Auditoria Informática, es la guía para la ejecución de la Auditoria Informática para la seguridad física de las unidades de sistemas de la organización.

3.5.2.2. Procesos de Ejecución o Implementación

Para iniciar con el desarrollo del proceso de ejecución de la Auditoria Informática previamente se debe revisar, si es necesario actualizar el programa de trabajo.

Esta etapa comprende el análisis detallado y la ejecución de una serie de pruebas, ya sea de cumplimiento o pruebas sustantivas de los objetivos de control determinados para la seguridad física.

En esta etapa se pone en práctica herramientas que tiene el auditor para recolectar la evidencia. Las herramientas son métodos de relevamiento de información para esto el auditor emplea:

Observación, que se realiza en el entorno para tener una idea objetiva del funcionamiento de la unidad de sistemas. Entrevistas, que son realizadas al/a los responsables(s) de la unidad de sistemas y al el auxiliar de sistemas o personal encargado del área. Checklist el cual es diseñado y rediseñado para brindar la mayor información posible.

En esta etapa se comprueba, si la organización trabaja de acuerdo a los procedimientos establecimientos, y/o verifica que procedimientos no están definidos.

Para esta etapa en el modelo propuesto tiene, Hojas de relevamiento de información física, el cual es aplicado al personal de la unidad de sistemas de la organización. Esta documentación constituirá parte de los papeles del trabajo de auditoría.

3.5.2.3. Elementos de salida de la Ejecución o Implementación

Los elementos de salida del proceso de Ejecución o implementación son los documentos o papeles de trabajo reunidos a lo largo del proceso (con encuestas, entrevistas y otras). Esta información constituye la evidencia del trabajo realizado.

Otro elemento de salida es la conclusión preliminar, sobre la situación de la organización, pues conforme se desarrolla el trabajo el auditor es capaz de ir obteniendo pequeñas conclusiones previas.

3.5.3. Proceso de Revisión

3.5.3.1. Elementos de entrada de la Revisión

La entrada a este proceso son los documentos o papeles de trabajo, la información reunida y procesada en la etapa de ejecución.

3.5.3.2. Proceso de Revisión

Se hace el análisis de los documentos recolectados y de las observaciones realizadas durante el desarrollo.

Se evalúa los niveles alcanzados en las pruebas realizadas, y tras un discernimiento objetivo, se obtiene una conclusión. Esta conclusión reafirma o corrige las conclusiones preliminares que el auditor formula en la etapa de revisión.

Las conclusiones son el resultado y la opinión del auditor respecto a la unidad auditada.

3.5.3.3. Elementos de Salida de la Revisión

El elemento de salida de la revisión, es la conclusión u opinión del auditor presentada a la institución.

3.5.4. Proceso de Comunicación de Resultados

3.5.4.1. Elementos de Entrada de Comunicación de Resultados

El elemento de entrada en la etapa de comunicación de resultados, es la conclusión u opinión del auditor presentado a la organización.

3.5.4.2. Procesos de Comunicación de Resultados

El auditor debe elaborar un informe de Auditoría Informática el cual es el medio de comunicación del resultado obtenido durante la auditoria, este informe debe ser oportuno, objetivo, claro y preciso, además debe ser emitido de forma escrita y debe contener eficiente información para ser entendido por los destinatarios, si corresponde debe facilitar la acción correctiva.

Una vez entregado y comunicado el resultado de forma escrita, si fuera necesario se debe realizar una reunión con el personal que considere oportuno la organización, para aclarar o explicar los resultados de la auditoria informática.

En caso de aclaraciones, se debe complementar esta información en el informe final que es presentado.

3.5.4.3. Elementos de salida de la Comunicación de Resultados

La salida del proceso de comunicación de resultados, es el informe final de la Auditoria Informática y las recomendaciones entregadas, a los directivos de la institución, quienes firmaran como constancia de la ejecución y conformidad con el trabajo realizado.

3.5.5. Proceso de Seguimiento

3.5.5.1. Elementos de Entrada del Seguimiento

La entrada al proceso de seguimiento es el documento del Informe Final presentado

3.5.5.2. Procesos del Seguimiento

Durante el proceso de seguimiento la Alta Dirección, el comité de evaluación o los responsables encargados de la recepción del informe de auditoría, revisan el informe Final y la documentación de respaldo.

En base a la revisión realizada por parte de los responsables a cargo, se define un plan de acciones correctivas estableciendo responsabilidades y periodos para el cumplimiento.

En caso de incumplimiento de responsabilidades y plazos, se debe aplicar las sanciones disciplinarias correspondientes.

Este es el punto donde la organización puede reorganizar funciones, cambiar de personal si fuera necesario o reorganizar toda actividad que considere conveniente.

3.5.5.3. Elementos de Salida del Seguimiento

El elemento de salida del proceso de seguimiento, es la toma de conciencia de los integrantes de la organización, el desempeño de funciones conforme a normas, políticas y procedimientos establecidos por la organización, creando un ambiente de trabajo eficiente y satisfactorio.

Capítulo IV Concreción del Modelo de Auditoria Informática para la Seguridad Física

Capítulo IV Concreción del Modelo de Auditoria Informática para la Seguridad Física

Del trabajo realizado en el capitulo Marco aplicativo se tiene la concreción del modelo propuesto, que guía la realización de la Auditoria Informática a la Seguridad Física, en ella se encuentra definido (1) los objetivos de control para la seguridad física y (2) herramientas de aplicación tanto para el relevamiento de la información como para la evaluación.

4. Objetivos de Control para la Seguridad Física

Los diez objetivos de control del modelo se detallan a continuación:

1. Política de Seguridad		
1.1. Política de Seguridad de la Información Objetivo: Proporcionar apoyo y dirección de gestión para la seguridad de la información de acuerdo a los requisitos del negocio, leyes relevantes y regulaciones.		
1.1.1.	Documento de Política de seguridad de información.	Control.- Un documento de política de seguridad de la información debe ser aprobado por la dirección, publicado y comunicado.
1.1.2.	Revisión de la Política de seguridad de la información.	Control.- La política de seguridad de la información deber ser revisada en intervalos planificados o cuando exista cambios significativos para asegurar su continuidad, actualización, adecuación y eficacia.

2. Organización de la seguridad de la información		
2.1 Organización Interna Objetivo: Gestionar la seguridad de la información dentro de la organización		
2.1.1	Compromiso de la dirección con la seguridad de la información	Control.- La dirección debe apoyar activamente la seguridad dentro de la organización a través de una orientación clara compromiso demostrado asignación explicita y conocimiento de las responsabilidades de seguridad de la información.
2.1.2	Coordinación de la seguridad de la información.	Control.- Las actividades de la seguridad de la información deben ser coordinadas por representantes de diferentes partes de la organización con roles y funciones de trabajo relevantes.
2.1.3	Asignación de responsabilidades de seguridad de la información	Control.- Se debe definir claramente todas las responsabilidades de la seguridad de la información
2.1.4	Proceso de autorización para las instalaciones de procesamiento de la información	Control.- Un proceso de autorización de la dirección para nuevas instalaciones de procesamiento de información debe ser definido e implementado
2.1.5	Acuerdos de confidencialidad	Control.- Los requisitos para acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados y regularmente revisados.
2.1.6	Contacto con las autoridades	Control.- Deben ser mantenidos contactos apropiados con las autoridades pertinentes.
2.1.7	Contacto con grupos de interés especial.	Control.- Deben ser mantenidos contactos apropiados con grupos de interés especial u otros foros de especializados en seguridad y asociaciones de profesionales.
2.1.8	Revisión independiente de la seguridad de la información	Control.- El enfoque de la organización para la gestión de la seguridad de la información y su implementación (p ej., objetivos de control, controles, políticas procesos y procedimientos de seguridad de la información) debe ser revisada independientemente a intervalos planificados o cuando ocurran cambios significativos en la implementación de la seguridad.

2.2.		
Obje		de la
infor		dos o
gesti		
2.2.1		las
		de la
		gocio
		estar
		identificados y se debe implantar apropiados controles antes de conceder el acceso.
2.2.2.	Dirigiendo la seguridad cuando se trata con clientes.	Control.- Todos los requisitos de seguridad identificados deben ser tratados entes de dar a los clientes, acceso a la información y recursos de la organización.
2.2.3.	Tratando la seguridad en acuerdos con terceras partes.	Control.- Los acuerdos con terceras partes que involucran acceso, proceso, comunicación o gestión de la información o instalaciones de procesamiento de la información de la organización o la adición de productos o servicios a las instalaciones de procesamiento de la información deben cubrir todos los requisitos de

		seguridad relevante

3. Gestión de Recursos		
3.1. Responsabilidad por los recursos Objetivo: Alcanzar y mantener la protección apropiada de los recursos organizacionales.		
3.2.1.	Inventario de recursos.	Control.- Todos los recursos deben ser claramente identificados y se deben elaborar y mantener un inventario de todos los recursos importantes.
3.2.2.	Propiedad de los recursos.	Control.- Toda la información y los recursos asociados con las instalaciones de procesamiento de la información deben ser "propios" por una parte designada de la organización.
3.2.3.	Uso aceptable de recursos.	Control.- Deben ser identificados, documentados e implementadas las reglas para el uso aceptable de información y recursos asociados a las instalaciones de procesamiento de información.

3.2. Clasificación de la Información Objetivo: Asegurar que la información recibe un apropiado nivel de protección.		
3.2.1.	Directrices de clasificación.	Control.- La información deber ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad a la organización.
3.2.2.	Etiquetado y manejo de la información.	Control.- Un apropiado conjunto de procedimientos de etiquetado y manejo de información, debe ser desarrollado e implementado de acuerdo con el esquema de

		clasificación adaptado por la organización.

4. Seguridad de los Recursos Humanos		
4.1. Previo al empleo. Objetivo: Asegurar que los empleados contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean adecuados para sus roles para los cuales han sido considerados y reducir el riesgo de robo, fraude o mal uso de las instalaciones.		
4.1.1.	Roles de responsabilidades.	Control.- Los roles y las responsabilidades de seguridad de los empleados, contratistas y terceras partes usuarias deben ser definidos y documentados de acuerdo con la política de seguridad de la información de la organización
4.1.2.	Exanimación.	Control.- Debe ser llevada a cabo la comprobación de la verificación de antecedentes de todos los candidatos al empleo, contratistas y terceras partes usuarias de acuerdo con las leyes regulaciones y ética relevantes y proporcionales a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.
4.1.3.	Términos y condiciones del empleo.	Control.- Como parte de su obligación contractual, empleados contratistas y terceras partes usuarias deben acordar y firmar los términos y condiciones de su contrato del empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.

4.2. Durante el Empleo Objetivo: Asegurar que todos los empleados contratistas y terceras partes usuarias estén conscientes de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones y son equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal y reducir el riesgo de error humano.		
4.2.1	Responsabilidades de la dirección.	Control.- La dirección debe exigir a sus empleados, contratistas y terceras partes usuarias aplicar la seguridad de acuerdo con las políticas y procedimientos (organizacionales, como sea relevantes para su función laboral) establecidos de la organización.
4.2.2.	Toma de conciencia, educación y formación en seguridad de la información.	Control.- Todos los empleados de la organización y donde sea relevante, contratista y terceras partes usuarias deben recibir formación apropiada en la toma de conciencia y actualizaciones regulares en políticas y procedimientos organizacionales, como será relevante para su función laboral.
4.2.3.	Proceso disciplinario.	Control.- Debe existir un proceso disciplinario formal para empleados que han cometido una violación a la seguridad.

4.3. Finalización o cambios de empleado Objetivo: Asegurar que los empleados contratistas y terceras partes usuarias salen de una organización o cambian de empleo de manera ordenada.		
4.3.1.	Finalización de	Control.- Deben estar claramente definidas y asignadas las responsabilidades para llevar a

	responsabilidades.	cabo la finalización o cambio de empleo
4.3.2.	Devolución de recursos.	Control.- Todos los empleados, contratistas y terceras partes usuarias deben devolver todos los recursos de la organización en su posesión al finalizar su empleo, contrato o acuerdo.
4.3.3.	Retiro de derechos de acceso.	Control.- Los derechos de acceso a todos los empleados, contratistas y terceras partes usuarias a la información y a las instalaciones de procesamiento de la información debe ser retirada a la finalización de su empleo, contrato o acuerdo, o ajustar después del cambio.

5. Seguridad Física y Ambiental		
5.1 Áreas Seguras Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a los predios e información de la organización.		
5.1.1	Perímetro de seguridad física	Control.- Los perímetros de seguridad (barreras como paredes, puertas de entrada controladas por tarjetas, escritorios de recepción manejados por personas) deben ser usados para proteger áreas que contienen información e instalaciones de procesamiento de información.
5.1.2	Controles de entrada física	Control.- Las áreas seguras deben ser protegidas por controles de entrada apropiadas para asegurar que solo personal autorizado tenga acceso permitido.
5.1.3	Seguridad de oficinas, habitaciones e instalaciones	Control.- La seguridad física para oficinas, habitaciones e instalaciones debe ser diseñada y aplicada.
5.1.4	Protección contra amenazas externas y ambientales	Control.- Debe ser diseñada y aplicada la protección física contra el daño proveniente fuego, inundaciones, terremoto, explosión, convulsión civil, y otras formas de desastre natural u ocasionadas por el hombre.
5.1.5	Trabajo en áreas seguras	Control.- Debe ser diseñada y aplicada la protección física y las directrices para trabajar en las áreas seguras.
5.1.6	Áreas de carga, entrega y acceso público	Control.- Los puntos de acceso tales como áreas de entrega y carga y otros puntos donde personas no autorizadas pueden entrar a los predios deben ser controlados, si es posible aisladas de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
		interrupciones o daños
5.2.4	Mantenimiento del equipo	Control.- El equipo debe ser correctamente mantenido para asegurar su continua disponibilidad e integridad.
5.2.5	Seguridad de los equipos fuera de los predios	Control.- La seguridad debe ser aplicada a equipos fuera de las instalaciones tomando en cuenta los diferentes riesgos de trabajar fuera de los predios de la organización
5.2.6	Seguridad en la eliminación o reutilización de los equipos	Control.- Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software con licencia y dato sensible ó asegurar que se hayan sobrescrito de forma segura antes de la eliminación.
5.2.7	Retiro de propiedad	Control.- El equipo información o software no debe ser

6. Comunicaciones y operaciones de gestión		
6.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar la correcta y segura operación de las instalaciones de procesamiento de la información.		
6.1.1	Documentación de los procedimientos de operación	Control.- Los procedimientos de operación deben ser documentados, mantenidos y deben estar disponibles a todos los usuarios cuando estos los necesiten.
6.1.2	Gestión del cambio	Control.- Los cambios a las instalaciones y sistemas de procesamiento de la información deben ser controladas.
6.1.3	Distribución de deberes	Control.- Los deberes y áreas de responsabilidad deben ser distribuidos para reducir las oportunidades de modificación no autorizada ó no intencional o mal uso de los recursos de la organización
6.1.4	Separación de las instalaciones de desarrollo, ensayo y operación	Control.- Las instalaciones de desarrollo, ensayo y operación deben ser separadas para reducir el riesgo de acceso no autorizado a cambios al sistema operacional
6.2 Respaldo Objetivo: Mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información.		
6.2.1	Información de respaldo	Se deben tener copias de respaldo de información y software y deben ser probadas de acuerdo con la política de respaldo acordada.
6.3 Manejo de medios Objetivo prevenir la divulgación no autorizada, modificación, retiro o destrucción de activos, o la interrupción de las actividades del negocio.		
6.3.1	Gestión de medios removibles	Deben existir procedimientos en el lugar, para la gestión de medios removibles.
6.3.2	Eliminación de medios	Los medios deben ser eliminados son seguridad y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.
6.3.3	Procedimientos de manejo de información	Procedimientos ara el manejo y almacenamiento de la información debe establecerse para proteger esta información de divulgación no autorizada o mal uso.
6.3.4	Seguridad de la documentación del sistema	La documentación debe ser protegida contra el acceso no autorizado.

7. Control de Acceso		
7.1 Requisitos del negocio para el control de acceso Objetivo: Controlar el acceso de información.		
7.1.1	Política de control de acceso	Control.- Una política de control de acceso debe ser establecida, documentada y revisada basada en los requisitos del negocio y de la seguridad para el acceso.
7.2 Gestión de accesos de usuarios Objetivo: Asegurar el acceso del usuario autorizado y prevenir el acceso no autorizado a los sistemas de información.		
7.2.1	Registro de usuarios	Control.- Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar acceso a todos los servicios y sistemas de información.
7.2.2	Gestión de privilegios	Control.- La asignación y uso de privilegios deben ser

8. Gestión de incidentes de seguridad de la información		
8.1 informe sobre los eventos y debilidades de seguridad de la información Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociados con sistemas de información son comunicados de manera que permita tomar una acción correctiva oportuna.		
8.1.1	Informe de eventos de seguridad de la información	Control.- Los eventos de la seguridad de la información deben ser informados a través de canales de gestión apropiados lo más rápido posible.
8.1.2	Informe de las debilidades de seguridad	Control.- Se debe exigir a todos los empleados, contratistas u usuarios de tercera parte que anoten y reporten cualquier debilidad de seguridad observada o sospechada en sistemas o servicios.

9. Gestión de continuidad del negocio		
9.1 Aspectos de seguridad de la información de gestión de continuidad del negocio Objetivo: Contraatacar las interrupciones a las actividades del negocio y proteger los procesos de negocios críticos de los efectos de fallas mayores de los sistemas de información o de desastres y asegurar su recuperación oportuna.		
9.1.1	Inclusión de la seguridad de la información en los procesos de gestión de continuidad del negocio.	Control.- Un proceso de gestión debe ser desarrollado y mantenido para la continuidad del negocio en toda a organización que trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
9.1.2	Continuidad del negocio evaluación del riesgo	Control.- Los eventos que pueden causar interrupciones a los procesos del negocio deben ser identificados junto con la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información.
9.1.3	Desarrollo e implementación de los planes de continuidad que incluyen la seguridad de la información	Control.- Los planes deben ser desarrollados e implementados para mantener o recuperar operaciones y asegurar la disponibilidad de la información al nivel requerido y en las escalas de tiempo requerido después de la interrupción o falla de los procesos críticos de negocio.
9.1.4	Marco de referencia del	Control.- Un simple marco de referencia de los planes

10. Cumplimiento		
10.1 Cumplimiento de requisitos legales Objetivo: Evitar la violación de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.		
10.1.1	Identificación de la legislación aplicable	Control.- Todos los estatutos relevantes, regulaciones y requisitos contractuales y el enfoque de la organización para alcanzar esos requisitos debe ser explícitamente definido, mantenido y actualizado para cada sistema de información y para la organización.
10.1.2	Derechos de propiedad intelectual (DPI)	Control.- Se deben implementar procedimientos apropiados para asegurar el cumplimiento son los requisitos legales, reglamentarios y contractuales sobre el uso de material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.
101.3	Protección de los registros organizacionales	Control.- Los registros importantes deben ser protegidos de pérdidas, destrucción y falsificación de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y de negocio.
10.1.4	Protección de datos y privacidad de información personal.	Control.- La protección de datos y privacidad deben ser asegurados como se exija en la legislación y regulaciones relevantes, y cuando sea aplicable en clausulas

10.3. Consideraciones de la Auditoria de Sistemas Objetivo: Maximizar la eficacia y minimizar la interferencia de /a los procesos de auditoría de sistemas.		
10.3.1.	Controles de auditoría de los sistemas de información.	Control.- Los requisitos de auditoría y las actividades involucradas que hacen verificaciones sobre sistemas operativos deben ser cuidadosamente planeados y acordados para minimizar el riesgo de interrupciones a procesos de negocio.
10.3.2.	Protección de las herramientas de auditoría de los sistemas de información.	Control.- El acceso a las herramientas de auditoría de sistemas de información debe ser protegido para evitar su mal uso o ponerlas en peligro.

4.1. Herramientas del Modelo

Las herramientas que ayudan en la evaluación de los objetivos de control propuestos en el modelo son (1) Hojas de evaluación, (2) Hojas de relevamiento de información.

4.1.1. Hojas de relevamiento de información

Son las herramientas que permiten la recolección de información sobre el estado de la seguridad física de las unidades de sistemas, puede ser aplicado al responsable de la unidad, los asistentes, y/o usuarios, según la información que se desee obtener:

I. Información del Evaluado

Área de Evaluación:.....

Nombres y Apellidos: .....

Cargo: .....

Tiempo de Servicio: .....

Modalidad de trabajo: .....

Personas bajo su Responsable: .....

Preguntas

1) POLÍTICA DE SEGURIDAD

CONTROL PRINCIPAL: Políticas de seguridad de la información

SUB - CONTROL: Documentos de política de seguridad de la información

8. ¿Conoce el documento de política de seguridad de la información de la organización?

   Si ( ) No ( )

1.3 ¿Que parte del documento de la política de seguridad de la información es relevante y ayuda con el desempeño de sus funciones dentro de la organización?

Res.-.....

1.4 ¿Que aspectos de la política de seguridad de la información considera que deberían de actualizarse y porque?

Res.-.....

9. ¿Cuales son los objetivos, alcances e importancia de la seguridad de la información de la organización?

   Res.-.....

   .....

10. ¿Según su criterio como apoya la alta dirección en el cumplimiento de los objetivos y principios de seguridad de la información?

    Res.-.....

    .....

11. Si observa o sospecha de un incidente que amenaza la seguridad de la información de la organización,

2) ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CONTROL PRINCIPAL: Organización interna

SUB - CONTROL: Compromiso de la dirección con la seguridad de la información

1. ¿La dirección apoya, proporciona o viabiliza la entrega de recursos necesarios que apoyen a la seguridad de la información?

   Res.-.....

   .....

2. ¿Quiénes organizan la seguridad dentro de la organización?

   Res.-.....

   .....

3. ¿En la organización se define las responsabilidades para la seguridad de la información?

   Res.-.....

   .....

4. Las responsabilidades y la autoridad que tiene su cargo le permiten desempeñar adecuadamente sus funciones. ¿Porque?

   Res.-.....

   .....

5. ¿Cuando se requiere nuevas instalaciones de procesamiento de información quien es el encargado de autorizarlo y/o existen algunos casos de comunicarlo antes de realizarlo?

   Res.-.....

6. ¿Antes de asumir su cargo usted firmo un acuerdo que involucra aspectos de confidencialidad?

   Res.-.....

   .....

7. ¿Cual es el procedimiento para la notificación en casos de incidentes?

   Res.-.....

   .....

   7.1 ¿A quien y como se contacta?

   Res.-.....

   .....

CONTROL PRINCIPAL: Partes Externas

8. ¿Se tiene contactos conocidos que puedan dar soporte o ayudar con la seguridad de la información?

   Res.-.....

   .....

9. ¿Que tipos medidas de seguridad se toma en relación a partes externa o ajenas a la institución?

   Res.-.....

   .....

10. ¿Se identifica de alguna manera a personal externo donde sea posible verificar los derechos de acceso que tiene? ¿Cómo?

    Res.-.....

    .....

3) GESTIÓN DE RECURSOS

CONTROL PRINCIPAL: Responsabilidad por los recursos

SUB - CONTROL: Inventario de recursos

1. ¿Se tiene un inventario de los activos de la organización?

   Si ( ) No ( )

2. ¿Cuando ó en que casos se actualiza el (los) inventarios?

   Res.-.....

   .....

4) SEGURIDAD DE LOS RECURSOS HUMANOS

CONTROL PRINCIPAL: Previo a la contratación

SUB - CONTROL: Roles y responsabilidades

1. ¿Comprende claramente los roles y responsabilidades de seguridad que le fueron comunicadas?
   Si ( ) No ( ) Poco ( )

SUB - CONTROL: Examinación

2. ¿Cómo fue contratado(a) para el cargo que desempeña?
   Res.-.....
   .....

3. ¿Recibió alguna vez algún comentario (de algún conocido de su anterior empleo) de que de su nuevo trabajo habían llamado para saber como era usted en ese empleo?
   Si ( ) No ( )

SUB - CONTROL: Términos y condiciones de empleo

4. ¿Llego a algún acuerdo previo antes de firmar el contrato?
   Si ( ) No ( )

CONTROL PRINCIPAL: Durante el empleo

SUB - CONTROL: Responsabilidad de la dirección

1. ¿Recibió algún tipo de capacitación y/o entrenamiento por parte de la organización? ¿Cuál (es)?
   Res.-.....
   .....

2. ¿Conoce el procedimiento que se sigue para sancionar una falta? ¿Cuál es?
   Res.-.....

CONTROL PRINCIPAL: Finalización o cambios de empleado

SUB - CONTROL: Finalización de responsabilidades

1. ¿Se sigue un proceso formal para realizar la finalización o cambio del empleo?
   Si ( ) No ( )
2. ¿Cuál es el procedimiento para el recojo de los recursos de la organización, asignados al empleado o terceras partes al finalizar su empleo?
   Res.-.....
   .....
3. ¿Existe algún formulario de comprobación llenado al momento de la asignación?
   Si ( ) No ( )
4. Se retiran o ajustan los derechos y permisos de acceso a la información e instalaciones, al finalizar el empleo, contrato del empleado o terceras partes.
   Si ( ) No ( )

5) SEGURIDAD FÍSICA Y AMBIENTAL

CONTROL PRINCIPAL: Áreas seguras

SUB - CONTROL: Perimetro de Seguridad física

1. Son definidos y usados perímetros de seguridad para proteger áreas de información o instalaciones de procesamiento de información.
   Si ( ) No ( )
2. Los perímetros del edificio son físicamente sólidos.

SUB – CONTROL: Protección contra amenazas externas y ambientales

13. ¿Qué medidas se diseña y aplica para amenazas ambientales a la seguridad física?
    Res.-.....
14. ¿Los materiales peligrosos son almacenados a distancias prudentes de un área de seguridad?
    Si ( ) ¿Dónde?..... No ( )
15. ¿Los equipos de soporte, reposición de información pérdida y los medios de respaldo, están guardados a una distancia segura para evitar los daños en el sitio principal?
    Si ( ) ¿Dónde?..... No ( )
16. Los equipos contra incendios son proporcionales
    Si ( ) No ( )
17. ¿Cuál es el criterio para ubicarlos?
    Res.-.....

SUB – CONTROL: Trabajo en áreas seguras

18. El trabajo es supervisado en áreas seguras para evitar actividades maliciosas.
    Si ( ) ¿Cómo?..... No ( )
19. Las áreas seguras desocupadas reciben algún tipo de control o revisión.
    Si ( ) ¿Cuál?..... No ( )
20. Que tipo de restricciones existe para el ingreso de equipos fotográficos, video, audio u otros tipos de dispositivos de grabación.
    Res.-.....
    .....

SUB – CONTROL: Áreas de acceso público, de entrega y carga

CONTROL PRINCIPAL: Seguridad del Equipamiento

SUB - CONTROL: Ubicación y protección del equipamiento

1. ¿Cómo son ubicados y protegidos los equipos para reducir los riesgos de las amenazas y riesgos ambientales y oportunidades de acceso no autorizado?
   Res.-.....
   .....
2. ¿Qué tipo de directrices son establecidas respecto a comer, beber y fumar en proximidades a instalaciones de procesamiento de información?
   Res.-.....
3. ¿Qué tipo de seguimiento se realiza a las condiciones ambientales en las instalaciones de procesamiento de información?
   Res.-.....
   .....

SUB – CONTROL: Servicios básicos de apoyo

6) **GESTIÓN DE COMUNICACIONES Y OPERACIONES**

CONTROL PRINCIPAL: Procedimientos y Responsabilidades Operacionales

SUB - CONTROL: Procedimientos de operación documentados

1. Los procedimientos de operación están documentados, mantenidos y disponibles para todos los usuarios que lo necesiten.
   Si ( ) No ( )
2. ¿Para qué actividades son preparados los documentos de procedimientos?
   Res.-.....
   .....
3. Los procedimientos de operación especifican instrucciones para la ejecución del trabajo.
   Si ( ) ¿Cómo?..... No ( )

SUB - CONTROL: Gestión de cambios

4. Se establece responsabilidades y procedimientos formales de gestión para asegurar el control de cambios en equipos, procedimientos u otro.
   Si ( ) ¿Cómo?..... No ( )

SUB - CONTROL: Distribución de obligaciones

5. ¿Las obligaciones y áreas de responsabilidad son distribuidas?
   Si ( ) No ( )
6. Se cuida que ninguna persona pueda acceder, modificar o utilizar los recursos sin autorización o sin ser detectado.
   Si ( ) ¿Cómo?..... No ( )

SUB - CONTROL: Separación de instalaciones de desarrollo, prueba y operacionales

13. Las unidades de medios removibles son habilitados si existen razones para hacerlo.
    Si ( ) No ( )

SUB - CONTROL: Eliminación de medios

14. Existen procedimientos definidos para identificar elementos que requieren eliminación segura.
    Si ( ) No ( )

SUB - CONTROL: Procedimientos de manipulación de información

15. Se establece procedimientos para el manejo y almacenamiento de información para proteger de la revelación no autorizada o mal uso.
    Si ( ) No ( )
16. Se revisa las listas de distribución y listas de destinatarios autorizados en intervalos regulares.
    Si ( ) No ( )

SUB - CONTROL: Seguridad de la documentación

17. La documentación de sistemas esta protegido contra el acceso no autorizado.
    Si ( ) ¿Cómo?..... No ( )

SUB - CONTROL: Intercambio de información

7) CONTROL DE ACCESO

CONTROL PRINCIPAL: Requisitos del negocio para el control de acceso

SUB - CONTROL: políticas de control de acceso

1. ¿Se establece, documenta y revisa políticas de control de acceso?
   Si ( ) No ( )
2. ¿Las reglas de control de acceso son apoyadas por procedimientos formales?
   Si ( ) No ( )

CONTROL PRINCIPAL: Gestión de acceso a usuarios

SUB - CONTROL: Registro de usuarios

3. Es comprobado el nivel de acceso concedido que sea apropiado y compatible con la política de seguridad de la organización
   Si ( ) No ( )
4. Se da a los usuarios una declaración escrita de sus derechos de acceso
   Si ( ) ¿Cuándo?.....No ( )
5. Se remueve o bloquea inmediatamente los derechos de acceso de los usuarios que han cambiado de roles o trabajos, o dejan la organización
   Si ( ) ¿Cuándo?.....No ( )

SUB - CONTROL: Revisión de derechos de acceso a usuarios

6. La dirección revisa los derechos de acceso de los usuarios a intervalos regulares usando un proceso formal.
   Si ( ) No ( )
7. ¿La asignación de privilegios es comprobada a intervalos regulares?

CONTROL PRINCIPAL: Responsabilidades de los usuarios

SUB - CONTROL: Uso de contraseñas

8. Se exige a los usuarios que sigan buenas prácticas de seguridad en la selección y empleo de contraseñas.
   Si ( ) No ( )
9. ¿Cuándo el usuario tiene acceso a múltiples servicios o sistemas y tiene una sola contraseña se asegura el nivel de protección?
   Si ( ) ¿Cómo?..... No ( )
10. Se comprueba el cambio de contraseñas en intervalos regulares y que no reutilicen las contraseñas.
    Si ( ) No ( )
11. ¿Qué medidas se toman al terminar sesiones activas cuando han terminado de usar el servicio?
    Res.-.....

CONTROL PRINCIPAL: Políticas de escritorio y pantallas limpias

12. ¿Se adoptan políticas y practicas de escritorio limpio para papeles, dispositivos removibles y pantallas limpias?
    Si ( ) No ( )
13. La información sensible o crítica están protegidos cuando la oficina esta desocupada.
    Si ( ) ¿Cómo?..... ..... No ( )

SUB - CONTROL: Desarrollo e implementación de planes de continuidad incluyendo la seguridad de la información.

10) **CUMPLIMIENTO**

CONTROL PRINCIPAL: Cumplimiento de los requisitos legales

SUB - CONTROL: Identificación de la legislación aplicable

1. Se tiene definido y documentado los requisitos legales, reglamentarios y contractuales pertinentes para cada sistema de información y para la organización.

   Si ( ) No ( )

2. Los controles específicos y las responsabilidades son definidos y documentados.

   Si ( ) No ( )

SUB - CONTROL: Derecho de propiedad intelectual (DPI)

3. Se mantiene un adecuado registro de los recursos e identifica aquellos que están protegidos por lo derechos de propiedad intelectual.

   Si ( ) No ( )

4. Se verifica que se instala solamente productos con licencia y autorizado.

   Si ( ) ¿Cómo?..... ..... No ( )

SUB - CONTROL: Protección de los registros de la organización

5. Los registros importantes de la organización están protegidos contra pérdida, destrucción y falsificación de acuerdo a requisitos de la organización.

   Si ( ) ¿Cómo?..... ..... No ( )

6. Los registros se clasifican según el tipo de registro, cada uno con el periodo de retención y el medio de almacenamiento.

   Si ( ) No ( )

SUB - CONTROL: Protección de datos y privacidad de la información personal

7. Se garantiza la protección de datos y privacidad de la información, de acuerdo con la los reglamentos y las clausulas de contrato.

   Si ( ) No ( )

8. Se desarrolla e implementa una política de protección y privacidad de los datos, que es comunicada al personal relevante.

   Si ( ) ¿Cuándo?.....No ( )

SUB - CONTROL: Prevención del uso inadecuado de los servicios de procesamiento de información

9. Los usuarios se abstienen de utilizar los servicios de procesamiento de información para propósitos no autorizados.

   Si ( ) No ( )

10. ¿Qué se hace cuando se encuentra a los usuarios realizando uso inadecuado de los servicio?
    Res.-.....
11. Los usuarios conocen el alcance preciso de su nivel de acceso, se les da una autorización escrita la cual es firmada y una copia es resguardada.

    Si ( ) No ( )

4.2. Hojas de Evaluación

Esta herramienta con ayuda de la hoja de relevamiento de información, determina el nivel de seguridad física que tiene la unidad de sistemas de la institución auditada. Esta información será llenada por el encargado de la auditoria.

1) POLÍTICA DE SEGURIDAD

	Hoja de Evaluación							
	CLAÚSULA: Política de Seguridad							
	CONTROL PRINCIPAL: Política de Seguridad de la Información							
Nº	SUB - CONTROL: Documento de Política de Seguridad de la Información	Evaluación						Total
		0	1	2	3	4	5	
1	El documento de Política de Seguridad de la información es aprobado por la dirección, publicado y comunicado.							
2	Se define seguridad de la información, sus objetivos y alcances globales y la importancia de la seguridad dentro de la organización.							
3	El documento de Política de Seguridad tiene el propósito de la dirección para apoyar a los objetivos y principios de seguridad de la información de acuerdo con la estrategia del negocio y los objetivos.							
4	El documento de Política de Seguridad tiene un marco referencial, que establece controles y objetivos de control físico, incluyendo la estructura de evaluación de riesgo.							
5	El documento de Política de Seguridad tiene una breve explicación de las políticas, principios, normas y el cumplimiento de requisitos de particular importancia.							

2) ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

	Hoja de Evaluación							
	CLAÚSULA: Organización de la Seguridad de la Información							
	CONTROL PRINCIPAL: Organización Interna							
Nº	SUB - CONTROL: compromiso de la dirección con la seguridad de la información	Evaluación						Total
		0	1	2	3	4	5	
1	La dirección apoya activamente la seguridad dentro de la organización.							
2	Se proporcionan los recursos necesarios para la seguridad de la información.							
3	Las actividades de seguridad de la información son coordinadas por representantes de la organización de diferentes áreas, con roles y funciones de trabajo relevantes.							
4	Se aprueban metodologías y procesos de seguridad de la información.							
5	Se evalúa la información recibida del seguimiento y evalúa los incidentes para recomendar acciones apropiadas en respuesta.							
6	Se define claramente todas las responsabilidades para la seguridad de la información.							
7	Los niveles de autorización están claramente definidos y documentados.							
8	Existe un proceso definido e implementado de autorización de la dirección para nuevas instalaciones de procesamiento de información.							
9	Los acuerdos de confidencialidad y/o no divulgación para la protección de la información de la organización, son identificados y revisados regularmente.							
10	Se establece responsabilidades de acciones de las personas que suscriben estos acuerdos.							

	Hoja de Evaluación							
	CLAÚSULA: Organización de la Seguridad de la Información							
	CONTROL PRINCIPAL: Partes Externas							
Nº	SUB - CONTROL: Identificación de riesgos	Evaluación						Total
		0	1	2	3	4	5	
1	Los riesgos de la información y las instalaciones de procesamiento de la información que provengan de terceras partes son identificados.							
2	Se considera el tipo de acceso que tiene la parte externa a la información e instalaciones de procesamiento de información.							
3	Prácticas y procedimientos para manejar incidentes de seguridad de la información.							
4	Se asegura que la parte externa este consciente de sus obligaciones							

3) GESTIÓN DE RECURSOS

	Hoja de Evaluación							
	CLAÚSULA: Gestión de Recursos							
	CONTROL PRINCIPAL: Responsabilidad por los recursos							
Nº	SUB - CONTROL: Inventario de recursos	Evaluación						Total
		0	1	2	3	4	5	
1	Todos los recursos de la organización son claramente identificados.							
2	Se realiza y mantiene actualizado los inventarios de recursos de la organización.							
3	Se llegan a acuerdos sobre la clasificación de la información para los recursos.							

	Hoja de Evaluación							
	CLAÚSULA: Gestión de Recursos							
	CONTROL PRINCIPAL: Clasificación de la información							
Nº	SUB - CONTROL: Directrices de clasificación	Evaluación						Total
		0	1	2	3	4	5	
1	Se clasifica la información de la organización según su valor, requisitos legales, sensibilidad y criticidad.							
2	Los controles de protección asociados a la información toman en cuenta necesidades para compartir y restringir información.							
3	El propietario del recurso define la clasificación de un recurso lo revisa y mantiene actualizado un nivel de clasificación							

4) SEGURIDAD DE LOS RECURSOS HUMANOS

	Hoja de Evaluación							
	CLAÚSULA: Seguridad de los Recursos Humanos							
	CONTROL PRINCIPAL: Previo a la contratación							
Nº	SUB - CONTROL: Roles y responsabilidades	Evaluación						Total
		0	1	2	3	4	5	
1	Son definidos los roles y responsabilidades de seguridad de los empleados, contratistas y terceras partes.							
2	Los roles y responsabilidades son claramente comunicados a los candidatos al cargo durante el proceso de pre – contratación.							
3	Son documentados los roles y responsabilidades de seguridad de los empleados, contratistas y terceras partes							
4	Estos roles y responsabilidades de seguridad de los empleados están de acuerdo a las políticas de seguridad de la información de la organización							

	Hoja de Evaluación							
	CLAÚSULA: Seguridad de los Recursos Humanos							
	CONTROL PRINCIPAL: Durante el empleo							
Nº	SUB - CONTROL: Responsabilidad de la dirección	Evaluación						Total
		0	1	2	3	4	5	
1	Se verifica y solicita que los empleados, contratistas y terceras partes usuarias apliquen la seguridad de acuerdo con las políticas y procedimientos de la organización.							
2	Todos los empleados, contratistas y terceras partes usuarias, reciben formación apropiada relevante para el desempeño de sus							

	Hoja de Evaluación							
	CLAÚSULA: Seguridad de los Recursos Humanos							
	CONTROL PRINCIPAL: Finalización o Cambio de empleo							
Nº	SUB - CONTROL: Finalización de responsabilidades	Evaluación						Total
		0	1	2	3	4	5	
1	Están claramente definidas y asignadas las responsabilidades para llevar a cabo la finalización o cambio del empleo.							
2	Responsabilidades y obligaciones aún validas después de finalizado el empleo deben estar contenidas en los contratos de empleados							
	SUB - CONTROL: Retorno de recursos							
3	Todos los empleados, contratistas y terceras partes usuarias devuelven todos los recursos de la organización que están a su cargo al finalizar su empleo, contrato o acuerdo.							
4	En casos de que el empleado, contratistas y terceras partes usuarias compra o usa su propio equipamiento se asegura que la información es transferida a la organización.							
	SUB - CONTROL: Eliminación de los derechos de acceso							
5	Los derechos de acceso de un individuo a la información y a las instalaciones de procesamiento de la información son retirados, anulados ó se ajustan al finalizar su empleo, contrato o acuerdo.							
6	Los derechos de acceso a los recursos de información e instalaciones son reducidos o eliminados antes de terminar o cambiar el empleo.							
7	Se cambian todas las contraseñas de cuentas que siguen activas a							

s) SEGURIDAD FÍSICA Y AMBIENTAL

	Hoja de Evaluación							
	CLAÚSULA: Seguridad Física y Ambiental							
	CONTROL PRINCIPAL: Áreas Seguras							
Nº	SUB - CONTROL: Perímetro de Seguridad	Evaluación						Total
		0	1	2	3	4	5	
1	Son definidos y usados perímetros de seguridad para proteger áreas con información o instalaciones de procesamiento de información.							
2	Los perímetros de un edificio son físicamente sólidos.							
3	Existe un área de recepción atendida por personal u otro medio de control de acceso físico al edificio y otras áreas restringidas.							
4	"Se tiene alarmas supervisadas y probadas en puertas de incendio.							
5	Las instalaciones de procesamiento de información de la organización están físicamente separadas de aquellas							

	Hoja de Evaluación							
	CLAÚSULA: Seguridad Física y Ambiental							
	CONTROL PRINCIPAL: Áreas Seguras							
Nº	SUB – CONTROL: Protección contra amenazas externas y ambientales	Evaluación						Total
		0	1	2	3	4	5	
16	Se diseña y aplica protecciones físicas contra el daño proveniente fuego, inundaciones, terremoto, explosión, convulsión civil, y otras formas de desastre natural u ocasionadas por el hombre.							
17	Los materiales peligrosos ó combustibles son almacenados a distancias prudentes de áreas seguras, así como los materiales de escritorio.							
18	Los equipos de soporte, de reposición de información pérdida y los medios informáticos de respaldo, están a una distancia segura para evitar daños ocasionados al sitio principal.							
19	Los equipos contra incendios son proporcionales y eficazmente ubicados							
	SUB – CONTROL: Trabajo en áreas seguras							
20	Se diseña y aplica la protección física y las directrices para trabajar en las áreas seguras.							
21	El personal solo tiene conocimiento de la existencia de un área segura cuando existe la necesidad de conocer.							
22	El trabajo es supervisado en áreas seguras para evitar actividades maliciosas.							
23	Las áreas seguras desocupadas deben ser físicamente bloqueadas y							

	Hoja de Evaluación							
	CLAÚSULA: Seguridad Física y Ambiental							
	CONTROL PRINCIPAL: Seguridad del Equipamiento							
Nº	SUB - CONTROL: Ubicación y protección del equipamiento	Evaluación						Total
		0	1	2	3	4	5	
1	Los equipos son ubicados y protegidos para reducir los riesgos de las amenazas y riesgos ambientales y oportunidades de acceso no autorizado.							
2	Son establecidas directrices respecto a comer, beber y fumar en proximidades a instalaciones de procesamiento de información.							
3	Se realiza seguimiento a las condiciones ambientales que afectan a la información y a las instalaciones de procesamiento de información.							
	SUB - CONTROL: Servicios básicos de apoyo							
4	El equipo es protegido de fallas de energía y otras interrupciones o anomalías causadas por fallas en los servicios básicos de apoyo.							
	SUB - CONTROL: Seguridad del cableado							
5	El cableado de energía eléctrica y telecomunicaciones que transporta datos ó apoya los servicios de información es protegido							

	Hoja de Evaluación							
	CLAÚSULA: Seguridad Física y Ambiental							
	CONTROL PRINCIPAL: Seguridad del Equipamiento							
Nº	SUB - CONTROL: Disposición segura o reutilización del equipamiento	Evaluación						Total
		0	1	2	3	4	5	
17	Los equipos que tienen dispositivos de almacenamiento, son revisados para asegurar que sea eliminado cualquier software con licencia y dato sensible ó que sea sobrescrito de forma segura antes de ser dispuesto.							
18	Los medios de almacenamiento conteniendo información son físicamente destruidos o la información es borrada o sobrescrita.							
19	Los medios de almacenamiento dañados que contienen datos sensibles requieren ser evaluados para determinar si el elemento							

6) GESTIÓN DE COMUNICACIONES Y OPERACIONES

	Hoja de Evaluación							
	CLAÚSULA: Gestión de Comunicaciones y Operaciones							
	CONTROL PRINCIPAL: Procedimientos y Responsabilidades Operacionales							
Nº	SUB - CONTROL: Procedimientos de operación documentados	Evaluación						Total
		0	1	2	3	4	5	
1	Los procedimientos de operación están documentados, mantenidos y disponibles para todos los usuarios que lo necesiten.							
2	Los procedimientos documentados deben ser preparados para las actividades de procesamiento de información, manejo de medios y otro.							
3	Los procedimientos de operación especifican instrucciones para la							

	Hoja de Evaluación							
	CLAÚSULA: Gestión de Comunicaciones y Operaciones							
	CONTROL PRINCIPAL: Respaldo							
Nº	SUB - CONTROL: Respaldo de información	Evaluación						Total
		0	1	2	3	4	5	
1	Se hace copias de respaldo de la información y se pone a prueba regularmente.							

	Hoja de Evaluación							
	CLAÚSULA: Gestión de Comunicaciones y Operaciones							
	CONTROL PRINCIPAL: Manejo de los medios							
Nº	SUB - CONTROL: Gestión de medios removibles	Evaluación						Total
		0	1	2	3	4	5	
1	Se establece procedimientos en el lugar para la gestión de medios removibles.							
2	Si no se requiere los contenidos de cualquiera de los medios reutilizables que son retirados de la organización se los hace irrecuperables.							
3	Los medios se almacenan en un ambiente seguro y vigilado.							
4	Las unidades de medios removibles son habilitados si existen razones para hacerlo.							
	SUB - CONTROL: Eliminación de medios							
	Los medios se eliminan de forma segura y sin riesgo usando procedimientos cuando ya no son requeridos.							
6	Existen procedimientos definidos para identificar elementos que requieren eliminación segura.							
7	*La eliminación de artículos sensibles es registrada para mantener un seguimiento de auditoría.							
	SUB - CONTROL: Procedimientos de manipulación de información							

	Hoja de Evaluación							
	CLAÚSULA: Gestión de Comunicaciones y Operaciones							
	CONTROL PRINCIPAL: Intercambio de información							
Nº	SUB - CONTROL: Políticas y procedimientos de intercambio de información	Evaluación						Total
1	Se establece políticas, procedimientos y controles formales que protegen el intercambio de información.							
	SUB - CONTROL: Acuerdos de intercambio							
2	Se establecen acuerdos para el intercambio de información entre la organización y partes externas							

7) **CONTROL DE ACCESOS**

	Hoja de Evaluación							
	CLAÚSULA: Control de Accesos							
	CONTROL PRINCIPAL: Requisitos del negocio para el control de acceso							
Nº	SUB - CONTROL: Políticas de control de acceso	Evaluación						Total
		0	1	2	3	4	5	
1	Se establece, documenta y revisa las políticas de control de acceso en base a los requisitos del negocio y seguridad de acceso.							
2	Las reglas de control de acceso consideran reglas que deben aplicarse y otras opcionales							

	Hoja de Evaluación							
	CLAÚSULA: Control de Accesos							
	CONTROL PRINCIPAL: Gestión de acceso a usuarios							
Nº	SUB - CONTROL: Registro de usuarios	Evaluación						Total
		0	1	2	3	4	5	
1	Existe un procedimiento formal de registrar y suprimir usuarios en el lugar, para conceder y revocar el acceso a todos los servicios de información.							
2	Se comprueba que el nivel de acceso concedido es apropiado y compatible con la política de seguridad de la organización							

	CLAÚSULA: Control de Accesos							
	CONTROL PRINCIPAL: Responsabilidades de los usuarios							
	Hoja de Evaluación							
Nº	SUB - CONTROL: Uso de contraseñas	Evaluación						Total
		0	1	2	3	4	5	
1	Se exige a los usuarios que sigan buenas prácticas de seguridad en la selección y empleo de contraseñas.							
2	Cuando el usuario tiene acceso a múltiples servicios o sistemas tiene una sola contraseña de calidad que asegura el nivel de protección.							
3	Se cambia las contraseñas en intervalos regulares de tiempo y se asegura de no reutilizar las contraseñas.							
	SUB - CONTROL: Equipo de usuarios desatendidos							
4	Los usuarios aseguran que el equipamiento desatendido tiene la protección apropiada							

8) GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

	Hoja de Evaluación							
	CLAÚSULA: Gestión de incidentes de seguridad de la información							
	CONTROL PRINCIPAL: Reporte de los eventos y debilidades en la seguridad de la información							
Nº	SUB - CONTROL: Reporte de eventos de seguridad de la información	Evaluación						Total
		0	1	2	3	4	5	

9) **GESTIÓN DE CONTINUIDAD DEL NEGOCIO**

	Hoja de Evaluación							
	CLAÚSULA: Gestión de la Continuidad del Negocio							
	CONTROL PRINCIPAL: Aspectos de seguridad de la información en la gestión de continuidad							
Nº	**SUB - CONTROL: Inclusión de la seguridad de la información en el proceso de gestión de continuidad del negocio.**	**Evaluación**						**Total**
		0	**1**	**2**	**3**	**4**	**5**	
1	Existe un proceso de gestión que es desarrollado y mantenido para la continuidad del negocio.							
2	En el proceso de continuidad se evalúa y comprende el impacto de una interrupción causada por un incidente de seguridad de la información.							
3	En el proceso se identifica y considera posibilidades de implementación de controles preventivos adicionales y de mitigación.							
4	En el proceso de continuidad se formula y documenta los planes de continuidad del negocio de acuerdo a sus requisitos de seguridad.							
	SUB - CONTROL: Continuidad del negocio y evaluación de riesgo							
5	Se identifican los eventos que causan interrupciones en los procesos del negocio junto con la probabilidad, para estimar el impacto de la interrupción y sus consecuencias para la seguridad de la información.							
6	Los aspectos de seguridad están basados en los eventos identificados que pueden causa interrupciones en la continuidad de la organización.							
7	Las evaluaciones de riesgos para la continuidad del negocio son realizadas con la participación plena de los dueños de los procesos y de los recursos del negocio.							
8	La estrategia para la continuidad del negocio esta desarrollada de acuerdo							

10) **CUMPLIMIENTO**

	Hoja de Evaluación							
	CLAÚSULA: Cumplimiento							
	CONTROL PRINCIPAL: Cumplimiento de los requisitos legales							
Nº	**SUB - CONTROL: Identificación de la legislación aplicable**	**Evaluación**						**Total**
		0	**1**	**2**	**3**	**4**	**5**	
1	Se tiene definido y documentado claramente todos los requisitos legales, reglamentarios y contractuales pertinentes para cada sistema de información y para la organización.							
2	Los controles específicos y las responsabilidades son definidos y documentados.							
	SUB - CONTROL: Derecho de propiedad intelectual (DPI)							
3	Se tiene implementado procedimientos adecuados para garantizar el							

	Hoja de Evaluación							
	CLAÚSULA: Cumplimiento							
	CONTROL PRINCIPAL: Cumplimiento con las políticas y normas de seguridad, y cumplimiento							
Nº	SUB - CONTROL: Cumplimiento con las políticas y normas de seguridad	Evaluación						Total
		0	1	2	3	4	5	
1	Los gerentes certifican que los procedimientos de seguridad en áreas de responsabilidad se llevan acabo correctamente para alcanzara el cumplimiento delas normas y políticas de seguridad.							
2	Los gerentes revisan regularmente en su área de responsabilidad el cumplimiento de procesamiento de información con las políticas, normas y otros requisitos de seguridad.							
3	En caso de incumplimiento se determina las causas, se evalúa la necesidad de acciones para que no vuelva a ocurrir.							
4	Se verifica periódicamente la compatibilidad de los sistemas de información con los estándares de implementación de la seguridad.							
5	Los resultados de las revisiones y acciones correctivas son registrados, documentados y guardados.							
	SUB - CONTROL: Verificación del cumplimiento técnico							
6	Los sistemas de información son verificados regularmente para el cumplimiento de las normas de implementación de la seguridad.							
7	Las pruebas de cumplimiento técnico son desarrolladas por una persona autorizada y competente o bajo supervisión de tales personas.							
	RESULTADO TOTAL DE LA EVALUACIÓN							

2	Se protege el acceso a las herramientas de auditoría de sistemas de información para evitar el uso erróneo o ponerlas en peligro.							
3	Las herramientas de auditoría están separadas de los sistemas y/o áreas de usuarios, o tienen un apropiado nivel protección adicional.							
4	Existen controles que protegen las herramientas de auditoría en el transcurso de una auditoría informática.							
	RESULTADO TOTAL DE LA EVALUACIÓN							

unidad que es evaluada, y responsable que ejecuta la auditoria.

Posteriormente se recoge información a través de la aplicación de Hojas de relevamiento de información, citado en el Marco Aplicativo, que es aplicado al personal de la unidad de sistemas de la institución evaluada.

La información se recolecta en hojas de relevamiento de información; es transcrita en la Hojas de Evaluación, en el proceso el auditor se encarga de analizar la concordancia con la realidad presentada y observada durante el proceso de evaluación, lo que da una variación en el nivel del estado de la institución.

Concluido el trabajo del llenado de las hojas de evaluación, se calcula el nivel de seguridad de la unidad evaluada, en base a la ecuación expuesta y explicada del Marco Aplicativo.

El valor obtenido se encuentra en uno de los tres rangos definidos en la Escala de Clasificación, en la columna Nivel Porcentual, cada rango tiene un correspondiente Nivel de Seguridad asignado, el cual indica el Nivel de seguridad física de la unidad auditada en la institución.

Estos son los pasos y la aplicación de las herramientas que propone el Modelo de Auditoria Informática para la Seguridad Física detallado en los Capítulos III y IV.
El Modelo de Auditoria para la Seguridad Física propuesto, se implemento en instituciones (1) NAFIBO ST Y (2) MINISTERIO DE PLANIFICACION DEL DESARROLLO, luego de evaluar obtuvieron los siguientes resultados.

Por motivos de acuerdos de confidencialidad con las instituciones evaluadas, no se identifica los nombres de las instituciones y solo se muestra los resultados que obtuvieron bajo los denominativos de “Institución A” e “Institución B”.

	Institución A	Institución B
Total	48,41	31

Tabla 4.3.1. Resultados de Evaluación

A la “Institución A” según la escala de clasificación 48.41% se encuentra en un nivel medio de seguridad, se les recomendó mejorar sus seguridad física implementando, procesos de evaluación continua de Auditoria Informática, formalizar políticas de seguridad que apoyen a la preservación de la información y otras sugerencias realizadas para alcanzar el Nivel Alto de Seguridad.

A la “Institución B” su nivel porcentual de 31% indica que tiene un Nivel Bajo de Seguridad, a quienes se recomendó seguir las sugerencias realizadas para alcanzar inicialmente el Nivel Medio de Seguridad, pues debe realizar muchas mejoras para alcanzar el Nivel Alto de Seguridad.

4.4. Prueba de la Hipótesis

La presente tesis, plantea la hipótesis*: “El Modelo de Auditoria Informática para la Seguridad Física, permite evaluar de forma completa los recursos de información y activos físicos de las unidades de sistemas, en base a la norma NB-ISO-IEC 27002”.*

Para fines de prueba de la hipótesis, se niega la hipótesis de investigación y se propone la hipótesis Nula: *“El Modelo de Auditoria Informática para la seguridad Física, no permite evaluar de forma completa los recursos de*

información y activos fijos de las unidades de sistemas, en base a la norma NB-ISO-IEC 27002".

Para la investigación:

En el desarrollo del modelo se hizo una revisión de la literatura necesaria en el campo de la Auditoria, Auditoria Informática, se reviso la metodología COBIT y normas relacionadas a seguridad de la información como NB-ISO-IEC 27002 y NB-ISO-IEC 27001, que constituyen el sustento teórico para el logro de objetivos de la investigación esta información es utilizada en el análisis y diseño de objetivos de control, herramientas de relevamiento de información y evaluación, los cuales permiten la implementación adecuada del modelo.

El modelo al estar basado en la norma NB-ISO-IEC 27002 y complementado con objetivos de control del modelo COBIT, se amplía el campo de evaluación en la seguridad física de los recursos de información, lo cual permite una evaluación completa de la seguridad física de la unidad de sistemas.

En las pruebas realizadas a las instituciones con el modelo propuesto, se observa y comprueba, que evalúa la seguridad física de la información y recursos físicos relacionados con el almacenamiento de la información de las unidades de sistemas, identificando su nivel de seguridad física.

Por lo expuesto se puede afirmar que el Modelo de Auditoria Informática para la Seguridad Física evalúa los recursos de información, por tanto se rechaza la hipótesis Nula y se acepta la hipótesis de investigación.

Conclusión

En la tesis se analizo y selecciono clausulas de seguridad física de la norma NB-ISO-IEC 27002 para que en base a estas clausulas se especifique y se construya los objetivos de control.

En base a las especificaciones de clausulas se diseño los objetivos de control, a estos se adicionan objetivos de control del modelo COBIT que no se contemplan en la norma, así como los objetivos de control del modelo garantizan una evaluación completa de la seguridad física de la información.

La tesis ofrece instrumentos para el relevamiento de información y para la evaluación de la información recolectada, estos instrumentos están de acuerdo a los objetivos de control del modelo propuesto, por tanto evalúa según las exigencias de la norma NB-ISO-IEC 27002 y la metodología COBIT.

En la tesis se observa que existen instituciones que tienen poca práctica de evaluación de auditoría informática, debido a que desconocen este tipo evaluación, y en muchos casos dejan descuidados y le restan importancia a aspectos relacionados con la seguridad física.

Al realizar evaluaciones de auditoría informática se despierta el interés de los usuarios y/o personas de instituciones, lo cual es favorable porque se crea un ambiente de conciencia para seguir con las normas establecidas ya sean instituciones u otros.

Glosario

Glosario

Adquirir e Implementar (AI): Las soluciones de Tecnologías de Información necesitan ser identificadas, desarrolladas o adquiridas, así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones satisfacen los objetivos del negocio.

Auditoría Externa: Está a cargo de auditores profesionales, ajenos a la empresa y totalmente independientes.

Auditoría Contable: Analiza la adecuación de los criterios empleados para recoger los hechos derivados de la actividad de la empresa y su representación, mediante apuntes contables, en los estados financieros.

Auditoria del Desarrollo: Verifica y evalúa todo el ciclo de vida del software excepto: la exploración, el mantenimiento y el retiro del servicio o aplicación cuando esta tenga lugar.

Auditoria de Dirección: Auditor examina el proceso de planificación de sistema de información y evalúa si razonablemente se cumplen los objetivos.

Auditoría Financiera: Examen y verificación de los estados financieros de la empresa, para emitir una opinión fundada sobre el grado de la fiabilidad de dichos estados.

Auditoria Física: Verifica, evalúa y comprueba la funcionalidad, racionalidad y seguridad de los medios físicos.

Auditoría de Gestión: Afecta a la situación global de la empresa.

Auditoria Informática: Examen y verificación del correcto funcionamiento y control del sistema informático de la empresa

Auditoría Interna: Está a cargo de empleados de la propia empresa, encuadrados en un departamento directamente dependiente de la dirección general.

Auditoria de Mantenimiento (Hardware y Software): Es la evaluación de la protección y continuidad del normal funcionamiento de los soportes físicos y lógicos existentes en la organización, comprobación de la existencia de las políticas y procedimientos formales relativos al mantenimiento preventivo y correctivo del hardware, sistemas de información y red de comunicaciones dentro de la institución.

Auditoria Organizativa: Analiza si la estructura organizativa de la empresa es la adecuada, según las necesidades y problemas de la misma.

Auditoria Operacional: Determina hasta que punto una organización, una unidad o función dentro de una organización, cumple los objetivos establecidos por la gerencia; así como identificar las condiciones que necesiten mejora.

Auditoria de Seguridad: Evalúa las medidas de protección de datos y de los sistemas computarizados, involucrando en forma global Hardware y Software, las medidas de protección a ser utilizadas y los planes de contingencia preparados para enfrentar problemas con o sin conocimiento de causa.

COBIT: Es un modelo genérico de procesos, estos son cuatro dominios fundamentales de la metodología y tiene distribuidos treinta y cuatro Objetivos de control generales:

Entregar y dar Soporte (DS): Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye en la prestación del servicio, la administración de seguridad y continuidad, el soporte del servicio a los usuarios, la administración de datos e instalaciones operacionales.

Evaluación: Es el proceso de análisis y valoración continua, mediante el cual se juzga o prueba algo.

ISACA: (Information Systems Audit and Control Association), es una organización global líder de profesionales que representa a individuos en más de 100 países y comprende todos los niveles de la tecnología de información.

MAGERIT: "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" (MAGERIT); esta metodología permite conocer, evaluar y valorar el riesgo al que están sometidos y así poder gestionarlos ayudando a protegerlos, trabaja con un esquema repetitivo donde a través del análisis de riesgos, los objetivos y estrategias permite elaborar un plan de seguridad que implantado y operado, satisface los objetivos propuestos con un nivel de riesgos aceptable para la Dirección.

Monitorear y Evaluar (ME): Todos los procesos de TI se evalúan de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Norma BS7799: Aparece en 1995, con el objetivo de preparar a cualquier empresa y sobre todo a las británicas en la certificación de la seguridad de la información, por medio de auditorías realizadas por auditores certificados y externos.

Norma de Seguridad NB-ISO-IEC 27001: Esta norma adopta un enfoque de procesos para establecer, implementar, realizar, hacer, seguimiento, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) de una institución.

Norma de Seguridad NB-ISO-IEC 27002: Es la norma dedicada a la seguridad de la información, lo que permite alinear de mejor manera el modelo propuesto a la seguridad física, de este modelo la clausula fundamental para garantizar la seguridad física es: Seguridad física y ambiental, pero no se debe dejar de lado aspectos organizacionales que cooperen con esta clausula.

Planear y Organizar (PO): Este dominio cubre las estrategias y tácticas, tiene que con identificar la manera en que TI contribuye de mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estrategia requiere ser planeada, comunicada y administrada desde diferentes perspectivas.

Políticas: Son formas de comunicarse con los usuarios, establecen un canal formal de actuación del personal, en relación con los recursos y servicios.

Riesgo: Es la posibilidad de que una amenaza llegue a acaecer por una vulnerabilidad.

Seguridad: Son medidas de protección y preservación, que se toman para garantizar la confidencialidad, integridad, disponibilidad, autenticación, autorización y confiabilidad que son consideradas para los activos estratégicos y valiosos relacionados con los sistemas y la institución.

Seguridad Lógica: Son medidas para la protección de accesos lógicos, cubre requerimientos que van más allá de aspectos físicos a través del uso de barreras y procedimientos que permita el almacenamiento y acceso a los datos solo para personas autorizadas.

Seguridad Física: Es la "Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial".

Vulnerabilidad: Es la debilidad de un recurso o grupo de recursos que son aprovechados por una o varias amenazas.

Vulnerabilidad de las Comunicaciones: Es el riesgo de intercepción cuando los ordenadores están conectados a la red.

Vulnerabilidad por Emanación: Se refiere a la intercepción de las radiaciones de los dispositivos eléctricos y electrónicos para descifrar o reconstruir la información almacenada o transmitida.

Vulnerabilidad Física: Es la posibilidad de entrar o acceder físicamente para robar, modificar o destruir el ambiente del edificio o el entorno físico del sistema.

Vulnerabilidad del Hardware: Es la facilidad del acceso a los dispositivos.

Vulnerabilidad Humana: Es el riesgo que representan los usuarios o personas que administran y utilizan los sistemas tanto física o mediante conexión, ya que toda la seguridad descansa sobre ellos.

Vulnerabilidad de los Medios o Dispositivos: Son las posibilidades de robar o dañar los discos, cintas y otros dispositivos de la computadora.

Vulnerabilidad Natural: Se refiere al grado en que los activos de la institución son afectados por desastres naturales o ambientales como el fuego, inundaciones, rayos, terremotos, o fallas eléctricas. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

Vulnerabilidad del Software: Son las fallas o debilidades del sistema que hacen fácil su acceso y lo hacen menos fiable.

Recomendaciones

Debido al contante cambio de las tecnologías de información y en consecuencia a la actualización de las normas y metodologías de Auditoria Informática se recomienda la investigación de otras normas e instrumentos de evaluación que puedan contribuir en el mejoramiento de las organizaciones. Como el modelo planeado por Microsoft.

La auditoria informática se debe realizar de forma periódica al igual que las auditorias financieras, ya que de estas evaluaciones dependen el control, mejoramiento y prevención de riesgos en las instituciones.

Se recomienda adoptar y aplicar la norma NB-ISO-IEC 27001 y NB-ISO-IEC 27002 como estándares de Auditoria Informáticas de seguridad de la información, si se requiere una evaluación que contemplen aspectos como seguridad lógica u otro, porque estas normas están actualizadas y adaptadas al contexto boliviano.

Debido a que la Auditoria Informática es compleja, principalmente en la recolección de información o evidencias y luego en la evaluación de la información, se recomienda construir un sistema de Auditoria Informática a partir de este modelo con sistemas expertos que manejen bases de conocimientos y ayuden en la evaluación y obtención de mejores resultados y se asemejen al trabajo de un auditor externo. Por lo que el sistema podría llevar a cabo auditorias de acuerdo a los requerimientos o necesidades de las instituciones.

Se recomienda realizar otras investigaciones en el campo de la Auditoria Informática ya que es un campo amplio de investigación, las evaluaciones de auditorías en cada área de la Informática lograran un óptimo funcionamiento de las unidades de sistemas.

Bibliografía

Bibliografía

1. Libros

- [DEI, 2006] La Tesis: Como orientarse en su elaboración, Dei, H, Daniel.
  Prometeo Libros, 2006, Buenos Aires.
- [COBIT 4.0. 2005] Objetivos de Control para la Información y las Tecnologías Relacionadas, IT Governance Institute (ITGI), 3701 Algonquin Road, Suite 1010, Impreso en los Estados Unidos de América.
- [CISSP, 2004] The CISSP Prep Guide, Second Edition por Ronald L. Krutz and Rusell Dean Vines, Published by Willey Publishing Inc. Copyright © 2004 by Willey Publishing, Inc., Indianapolis, Indiana.
- [COBIT, 2002] Objetivos de Control para la Informacion y las Tecnologias Relacionadas, Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI), Tercera Edición.
- [MAGERIT, 2006] Metodología de Análisis y Gestión de Riesgo de los Sistemas de Informacion, Ministerio de Administraciones Publicas, Madrid, 20 de junio de 2006, Método (v 1.1), Nº Paginas 154.
- [NGA, 2005] “Normas Generales de Auditorias Gubernamental”, Contraloría General de la República de Bolivia.
- [ISO 17799, 2002] Código de prácticas para la Administración de la Seguridad de la Informacion, Marzo de 2002 (Acta2-2002).
- [ISO 27002, 2007] Tecnología de la Informacion- Técnicas de seguridad- Código de práctica para la gestión de seguridad de la información, Instituto Boliviano de Normalización y Calidad (IBNORCA), Primera Edición, Noviembre 2007.

- [ISO 27001, 2007] Tecnologias de la Informacion-Técnicas de seguridad-Sistemas de gestión de seguridad de la información-Requisitos, Instituto Boliviano de Normalización y Calidad (IBNORCA), Primera Edición, Marzo 2007
- [PIATTINI, 2001] *Auditoria informática un enfoque practico*, Piattini Mario, Del peso Emilio, Segunda Edición, Alfaomega Ra-Ma México.
- [ECHENI, 2001] *Auditoría en Informática,* Echenique García José Antonio, Segunda Edición, México Mc Graw-Hill, 2001.
- [SAMPIERI, 1998] Metodología de la Investigación, M. en C. Roberto Hernández Sampieri, Segunda Edición, Mc Graw-Hill Interamericana Editores, México, D.F.
- [Montgo,1997] [AICPA, 1997] Auditoria Montgomery, Philip L. Defliese C.P.A.
- [MAGINTRO, 2005] "Manual de Auditoria Gubernamental" Contraloría General de Cuantas, Guatemala, Junio 2005.
- [MAGRALAUD, 2003] "Manual General de Auditoria" Dirección General de Programación y Control de Auditoria, Contaduría Mayor de Hacienda de la Asamblea Legislativa del Distrito Federal, Abril de 2003.
- [ANDER-EGG, 2000] Diccionario de pedagogía, Ezequiel Ander-Egg, Magisterio del rio de la Plata, Segunda Edición, República Argentina, 2000.

2. Tesis

- [T. 1315, 2006] "Guía de Auditoria de Seguridad de la Informacion", Zenteno Flores Lorena, La Paz 2006.
- [T. 1166, 2005] "Método de Auditoria, y Control al Servicio de la Educación Superior", Miguel Cotaña Mier, La Paz-Bolivia 2005.
- [T. 1163, 2005] "Auditoria de Seguridad Lógica Asistida por Agentes Inteligentes", Quisbert Ovidio, La Paz- Bolivia 2005.

- [T. 763, 2002] “Auditoria Informática en Redes”, Ascarrunnz Martínez Henoch, La Paz- Bolivia 200.
- [T. 519, 2001] “Auditoria Informática de Calidad basada en las Normas ISO 9000”, Aliaga Moruno Ivert, La Paz- Bolivia 2001.
- [T. 493, 2000] “Auditoria en Calidad de Software” Aspiazu Castro Virginia, La Paz- Bolivia 200.
- [T. 128, 1996] “Guía de Auditoria Informática”, Perales A. & Paredes L., La Paz- Bolivia, 1996.

3. Artículos y Páginas de Internet

- [JNAVA, 2007] Apuntes de Auditoria Informática, Fco. Javier Nava García, Recuperado el 23 de Julio 2007.
- [MAMC, 2008] Modelo de auditoría para el Mejoramiento de la Calidad Recuperado el 04 de Abril del 2008.
- [ISOHIS, 2008] ISO 27000, Recuperado el 01 de Abril 2008.
- [GSII, 2007] Gestión de Seguridad de la Informacion ISO 27001 Auditoría interna de un SGSI según ISO 27001, Recuperado en Noviembre del 2007.
- [FCSI, 2007] Formación y Concienciación en Seguridad de la Informacion- Auditoria y Seguridad de la Informacion- Auditoria, Seguridad, LOPD, ISO 27001.
  Recuperado en Noviembre del 2007
- [UCC, 2007] Guía para la Elaboración y presentación de trabajos escritos basadas en las normas APA, Universidad Cattolica de Colombia (2002). Manuscrito no publicado, Bogotá.
- [AUDINF, 2007] AUDITORIA INFORMATICA. Recuperado en Mayo del 2007.
- [ASADS, 2007] Auditoria Sistemas Auditoria de Sistemas, Recuperado en Mayo del 2007
- [AIAI, 2007] Auditoria Informática Auditoria Informática, Recuperado en Mayo del 2007.

- [EDAI, 2007] Etapas de Una Auditoria Informática, Recuperado el 29 de Mayo del 2007.
- [PROFAGER, 2007] Normas de Auditoria Generalmente Aceptadas (NAGA) por Profesor: Ing. Com. Genaro Peña Cordero.
- [SYPDI, 2008] Seguridad y Protección de la Informacion, Badia Contelles, José Manuel y Coltell Simón, Oscar, Recuperado el 8/5/2008.