UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Estándar ISO 17799 en Gobierno del Estado de Quintana Roo.

Tesis para obtener el grado de

Ingeniero en Redes

Presenta

Allan Alonso Córdova Lechuga

Director de tesis

M.T.I. Vladimir Veniamin Cabañas Victoria

Supervisores

M.S.I. Laura Yésica Dávalos Castilla

Ing. Rubén Enrique González Elixavide

Chetumal, Quintana Roo, México, Noviembre de 2012

UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Trabajo de tesis elaborado bajo supervisión del Comité de Asesoría y aprobada como requisito parcial para obtener el grado de:

Ingeniero en Redes

Comité de Trabajo Tesis

Director:

M.T.I. Vladimir Veniamin Cabañas Victoria

Supervisor:

M.S.I. Laura Yésica Dávalos Castilla

Supervisor:

Ing. Rubén Enrique González Elixavide

Chetumal, Quintana Roo, México, Noviembre de 2012.

Chetumal, Quintana Roo, Noviembre de 2012.

AGRADECIMIENTOS

Agradezco a mis padres y a mi hermana por siempre creer en mí y apoyarme en momentos de flaqueza.

De igual forma agradezco al Dr. Jaime Ortegón Aguilar por su apoyo y confianza en los momentos más difíciles, al Maestro Vladimir Veniamin Cabañas Victoria por su apoyo en la realización del proyecto y al Ingeniero Rubén Enrique González Elixavide por su orientación durante toda la carrera.

DEDICATORIA

A mi Padre, Madre y Hermana, quienes siempre me han apoyado durante mi vida de estudiante, me dan fuerza para seguir adelante y superar las barreras que se presentan en el camino.

A todos los maestros, tanto de la escuela como de la vida, quienes siempre, con sus sabios consejos me apoyaron y guiaron a través de la densa neblina.

Contenido

CAPÍTULO 1

INTRODUCCIÓN.

La información que se presenta en este proyecto ha sido organizada de manera que pueda ser interpretada por personal vinculado al uso de sistemas de información en las diversas áreas de la función pública del Gobierno del Estado de Quintana Roo, especialmente para personal de la Coordinación Estatal de Informática y Telecomunicaciones (CEIT), con la intención de observar el estándar ISO 17799 en su implementación.

Las recomendaciones fueron planteadas según el contexto de aplicación, organizadas por niveles de seguridad y siguiendo un entorno de desarrollo sobre la problemática de la institución.

Los niveles de seguridad fueron organizados procurando tener un enfoque objetivo de la situación real del Gobierno Estatal, desarrollando cada política con especial cuidado sobre qué activo proteger, de qué protegerlo, cómo protegerlo y por qué protegerlo. Estas políticas se organizan siguiendo el esquema normativo de seguridad, ISO 17799 (mejores prácticas de seguridad)

1.1 Antecedentes.

En la Coordinación Estatal de Informática y Telecomunicaciones (y en cualquier otra organización) la gestión de seguridad puede tornarse compleja y difícil de realizar, aquí influyen no sólo los factores técnicos, sino además la estructura organizacional y su función, el ambiente y su cultura laboral.

Como resultado del Programa Quintana Roo Digital (1) y de sus procesos de Diagnóstico y Planeación Tecnológica, se identificaron los principales factores críticos que afectan la productividad de la función del gobierno, entre esos factores se encontró la falta de estándares.

Una de las tareas importantes que se tiene que realizar para un buen funcionamiento de la Red Gubernamental es integrar la implementación de estándares de seguridad, los procedimientos que la regulen y el manejo de los riesgos de seguridad, los cuales no pretenden ser absolutos (dada la naturaleza de su aplicación) por lo que pueden estar sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad.

Toda persona que utilice los servicios que ofrece Gobierno del Estado dentro de la Red Gubernamental, deberá de conocer y aceptar el reglamento vigente y futuro sobre su uso, el desconocimiento del mismo no debería de exonerar de responsabilidad al usuario.

En términos generales es necesario definir nuevos procesos y establecer un estándar de mejores prácticas de seguridad en informática, englobando los procedimientos más adecuados, tomando como lineamientos principales cuatro criterios, que se detallan a continuación:

Seguridad Gubernamental: Se establece el marco formal de seguridad que debe sustentar Gobierno del Estado en general, que deberá incluir los servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad Lógica: Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos para la administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y a la documentación sobre sistemas, establecer los procesos para el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

Seguridad Física: Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad en caso de contingencias, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas, así como también establecer procedimientos con base en la importancia de los activos.

Seguridad Legal: Integra los requerimientos de seguridad que deben cumplir todos los empleados y usuarios de la Red Gubernamental bajo la reglamentación de la estandarización a aplicar en el Gobierno del Estado en cuanto al recurso humano, sanciones aplicables ante faltas cometidas y bajo qué condiciones se realizarán las contrataciones externas.

Cada uno de los criterios anteriores, sustenta un entorno de administración de suma importancia, para la seguridad de la información dentro de la Red de Gobierno del estado.

1.2 Situación actual.

En el Gobierno del Estado de Quintana Roo la administración y la reglamentación tanto de equipos tecnológicos como del personal que los opera no ha logrado ser eficaz, los documentos concernientes a reglamentos, procedimientos, políticas e inclusive en la estandarización de procesos no se ha actualizado y esto ha representado un atraso en la administración en general, no contemplan el manejo de la nueva infraestructura tecnológica implementada y sobre todo en los procedimientos que se requieren para la correcta administración de la misma.

1.3 Justificación

Junto al avance de las tecnologías de la información y su influencia en casi todas las áreas de las organizaciones se observa la necesidad de hacer un uso adecuado de ésta, ya que las amenazas y los riesgos en la seguridad informática han evolucionado también, todos los días se corre el riesgo de sufrir pérdida de información, pérdida del equipo de cómputo y pérdidas económicas; los ataques pueden ser internos y

externos, lo que daña la imagen institucional, la confianza de los usuarios y de los proveedores.

En cualquier empresa, organización e incluso la administración pública, el manejo de la seguridad puede tornarse compleja e incluso difícil de realizarse, tanto por razones técnicas como administrativas y en muchos casos el tipo de proceder dentro de la misma organización. Coordinar todos los esfuerzos para asegurar un entorno informático adecuado, por medio de una simple administración de los recursos tanto humanos como tecnológicos, sin un adecuado control que los integre, podría generar en la mayoría de los casos un ambiente hostil, para ello es necesario emplear mecanismos que regulen las funciones y las actividades desarrolladas por cada uno de los empleados.

1.4 Objetivo General

Realizar la elaboración de las recomendaciones de seguridad informática, fundamentadas bajo la norma ISO/IEC 17799 para las diferentes áreas del Gobierno del Estado de Quintana Roo.

1.4.1 Objetivos Particulares

- Analizar los procesos administrativos y tecnológicos de la función pública.
- Identificar y analizar las necesidades de la Red Gubernamental.
- Establecer los estándares aplicables en el uso de las tecnologías de la información.
- Establecer las directrices de gestión para la seguridad de la información,
- Determinar el alcance del estándar e implementar procesos de desarrollos continuos, así como de realizar las actualizaciones del mismo apegado a los estándares internacionales vigentes.

1.5 Metodología

La metodología empleada para la realización de este proyecto fue dividida en cinco etapas:

I. Planteamiento del Problema.

La normatividad informática vigente en el Gobierno del Estado data desde el mes de Mayo de 1999, la cual, a pesar de sufrir modificaciones en diferentes periodos, no se encuentra debidamente actualizada, limitando la administración de las nuevas Tecnologías de la Información.

II. Planeación.

- Revisar la documentación existente en la CEIT referente a políticas y normatividad de informática y telecomunicaciones.
- Analizar los diferentes modelos internacionales de estandarización.

III. Recopilación de la Información.

Realizar una investigación entre la documentación existente de la CEIT, en los estándares internacionales, en medios electrónicos y bibliográficos y otros medios que provean información referente a la implementación de Estándares de Seguridad en la Información.

IV. Interpretación de la Información.

Con base a la información recopilada y analizada se podrá realizar un informe en el cual se especifiquen los diversos aspectos a de la situación actual y de cómo poder

solucionarlos, en cuanto a seguridad en la información que se tiene en Gobierno y de las probables adaptaciones con el estándar a adoptar para posteriormente implementarlas.

V. Resultados.

Recomendar el modelo de estandarización más adecuado para ser implementado en primera instancia en la CEIT y posteriormente dentro de la Red Estatal así como especificar las áreas a ser implementado.

1.6 Alcances y Recomendaciones

El ámbito de aplicación de los estándares de seguridad informática, será la infraestructura tecnológica y el entorno informático de la Red que administra la Coordinación Estatal de Informática y Telecomunicaciones del Gobierno del Estado de Quintana Roo. Una de las principales funciones del CEIT será la de garantizar la ejecución y puesta en marcha del estándar de seguridad, siendo el responsable absoluto de la supervisión, cumplimiento de los reglamentos y el gestor de seguridad en todo el estado.

CAPITULO 2

2.1 Informática, concepto y generalidades. (2)

2.1.1 Definición de Informática

La definición que se encuentra en el diccionario de la Real Academia de la Lengua Española señala que la informática "es un conjunto de conocimientos científicos y técnicas las cuales hacen posible el manejo de información por medio de computadoras".

2.2 Tecnologías de la información, concepto y generalidades.

2.2.1 Definición de Tecnologías de la información (3)

Se refiere a los medios colectivos para reunir y luego almacenar, transmitir, procesar y recuperar electrónicamente palabras, números, imágenes y sonidos, así como a los medios electrónicos para controlar máquinas de toda especie, desde los aparatos de uso cotidiano hasta las vastas fábricas automatizadas. Gerstein 1988.

Gerstein trata de llevar el concepto al sentido más amplio; entender problemas y crear soluciones a través de los diferentes aparatos que conocemos, como sensores, rastreadores, redes de telecomunicaciones y computadoras de todas clases. Todas estas nuevas tecnologías nos ayudan a analizar y entender la información a nivel global.

2.2.2 Características de las Tecnologías de la Información (4)

Las tecnologías de información y comunicación tienen como características principales las siguientes:

Inmaterialidad (Posibilidad de digitalización). Las TICs convierten la información, tradicionalmente sujeta a un medio físico, en inmaterial. Mediante la digitalización es posible almacenar grandes cantidades de información, en dispositivos físicos de pequeño tamaño (discos, CD, memorias USB, etc.). A su vez los usuarios pueden

acceder a información ubicada en dispositivos electrónicos lejanos, que se transmite utilizando las redes de comunicación, de una forma transparente e inmaterial.

Esta característica, ha definido la "realidad virtual", esto es, realidad no real. Mediante el uso de las TICs se crean grupos de personas que interactúan según sus propios intereses, conformando comunidades o grupos virtuales.

Instantaneidad. Transmitir la información instantáneamente a lugares alejados físicamente, mediante las denominadas "autopistas de la información".

Se han acuñado términos como *ciberespacio,* para definir el espacio virtual no real, en el que se sitúa la información, al no asumir las características físicas del objeto utilizado para su almacenamiento, adquiriendo ese grado de inmediatez e inmaterialidad.

2.2.3 Las Tecnologías de la Información en la vida actual (5)

La tecnología de la Información (TI) está cambiando la forma tradicional de hacer las cosas, los avances actuales hacen posible capturar y utilizar la información en el momento que se genera, es decir, tener procesos en línea; este hecho no sólo ha cambiado la forma de hacer el trabajo y el lugar de trabajo sino que también ha tenido un gran impacto en la forma en la que las empresas compiten.

Indiscutiblemente hay cambios notables, particularmente hablando de México, en cuanto a la aparición de las nuevas tecnologías. Eulalio Ferrer Bojórquez (1995) señala que el cambio tecnológico no es exclusivo de nuestra época.

Entre los servicios que están modificando a nuestra sociedad están: los periódicos electrónicos, las revistas y las enciclopedias electrónicas, loa buzones electrónicos y el banco electrónico.

Las tecnologías de la información y la comunicación no son ninguna panacea ni fórmula mágica, pero pueden mejorar la vida de todos los habitantes del planeta. Se disponen de herramientas para llegar a los Objetivos de Desarrollo del Milenio, de

instrumentos que harán avanzar la causa de la libertad y la democracia, y de los medios necesarios para propagar los conocimientos y facilitar la comprensión mutua" *(Kofi Annan, Secretario general de la ONU, discurso inaugural de la primera fase de la WSIS, Ginebra 2003).*

2.3 Estándares Seguridad.

2.3.1 Definición de Seguridad (6)

Este concepto que proviene del latín *securĭtas* se refiere a la cualidad de seguro, es decir aquello que está **exento** de peligro**,** daño o riesgo. Algo seguro es algo cierto**,** firme e indudable. La seguridad, por lo tanto, es una certeza.

2.3.2 Objetivo de la Seguridad

El objetivo de la seguridad en la informática, es la de asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

2.3.3 Definición de Estándares de Seguridad

Son actividades, acciones, reglas o regulaciones obligatorias orientadas a proporcionar confiabilidad a la infraestructura tecnológica, informática y de telecomunicaciones dentro de una organización.

Existen 2 instituciones que dictan las normas internacionales en materia de seguridad informática: por una parte se encuentra la ISO (International Organization for Standardization, por sus siglas en ingles) y por otra parte a la NIST (National Institute of Standards and Technology, por sus siglas en ingles) y cada una de estas instituciones ha propuesto un marco de trabajo para el tema se la seguridad informática.

2.3.4 Estándares de Seguridad Existentes en México. (7)

En México es posible encontrar tanto empresas certificadoras como certificadas en ISO en sus diversas versiones, también es capaz de establecer sus propias Normas, conocidas como NOM y orientadas a diversos ámbitos, tales como para establecer una reglamentación en Trabajo, Salud, Comunicaciones, Construcción de edificaciones en general, que estipulan la forma de proceder en casos de emergencias, incluso las propias normas de la Comisión Federal de Electricidad (CFE)**.**

2.3.5 Empresas Certificadoras en México

Algunas compañías, autorizadas internacionalmente que se dedican a desarrollar actividades de certificación y a certificar a gobiernos o empresas en sus diversas actividades:

- La Asociación Española de Normalización y Certificación (AENOR), creada en 1986, es una entidad española, privada, independiente, sin ánimo de lucro, reconocida en los ámbitos nacional, comunitario e internacional, que contribuye, mediante el desarrollo de las actividades normalización y certificación, a mejorar la calidad en las empresas. (8)
- BSI Management Systems, es certificadora líder mundial en ISO 17799, es uno de los organismos de certificación más importantes en el mundo, con más de 60,000 localidades certificadas y clientes en más de 100 países. (9)

2.3.6 Requisitos para Certificación de una empresa o Gobierno (10)

Evidentemente, el paso previo a intentar la certificación es la implantación en la organización del Sistema de Gestión de Seguridad de la Información (SGSI) según ISO 27001. Este sistema deberá tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoría para su primera certificación.

ISO 27001 exige que el SGSI contemple los siguientes puntos:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.
- La documentación del SGSI deberá incluir:
- Política y objetivos de seguridad.
- Procedimientos y controles que apoyan el SGSI.
- Descripción de la metodología de evaluación del riesgo.
- Informe resultante de la evaluación del riesgo.
- Plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.
- Registros.
- Declaración de aplicabilidad (SOA -Statement of Applicability-).
- Procedimiento de gestión de toda la documentación del SGSI.

Hay una serie de controles clave que un auditor va a examinar siempre en profundidad:

- Política de seguridad.
- Asignación de responsabilidades de seguridad.
- Formación y capacitación para la seguridad.
- Registro de incidencias de seguridad.
- Gestión de continuidad del negocio.
- Protección de datos personales.
- Salvaguarda de registros de la organización.
- Derechos de propiedad intelectual.

El SGSI puede estar integrado con otro tipo de sistemas (ISO 9001, ISO 14001…). La propia norma ISO 27001 incluye en su anexo C una tabla de correspondencias de ISO 27001:2005 con ISO 9001:2000 e ISO 14001:2004 y sus semejanzas en la documentación necesaria, con objeto de facilitar la integración.

Es recomendable integrar los diferentes sistemas, en la medida que sea posible y práctico. En el caso ideal, es posible llegar a un solo sistema de gestión y control de la actividad de la organización, que se puede auditar en cada momento desde la perspectiva de la seguridad de la información, la calidad, el medio ambiente o cualquier otra.

2.3.7 Auditoría y certificación. (10)

Una vez implantado el SGSI en la organización, y con un historial demostrable de al menos 3 meses, se pasa a la fase de auditoría y certificación, que se desarrolla de la siguiente forma:

- Solicitud de la auditoría por parte del interesado a la entidad de certificación y toma de datos por parte de la misma.
- Respuesta en forma de oferta por parte de la entidad certificadora.
- Compromiso.

- Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoría.
- Pre-auditoría: opcionalmente, puede realizarse una auditoría previa que aporte información sobre la situación actual y oriente mejor sobre las posibilidades de superar la auditoría real.
- Fase 1 de la auditoría: no necesariamente tiene que ser *in situ*, puesto que se trata del análisis de la documentación por parte del Auditor Jefe y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2. Este informe se envía junto al plan de auditoría al cliente. El periodo máximo entre la Fase 1 y Fase 2 es de 6 meses.
- Fase 2 de la auditoría: es la fase de detalle de la auditoría, en la que se revisan i*n situ* las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto. Se inicia con una reunión de apertura donde se revisa el objeto, alcance, el proceso, el personal, instalaciones y recursos necesarios, así como posibles cambios de última hora. Se realiza una revisión de las exclusiones según la Declaración de Aplicabilidad (documento SOA), de los hallazgos de la Fase 1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés. Finaliza con una reunión de cierre en la que se presenta el informe de auditoría.
- Certificación: en el caso de que se descubran durante la auditoría no conformidades graves, la organización deberá implantar acciones correctivas; una vez verificada dicha implantación o, directamente, en el caso de no haberse presentado no conformidades, el auditor podrá emitir un informe favorable y el SGSI de organización será certificado según ISO 27001.
- Auditoría de seguimiento: semestral o, al menos, anualmente, debe realizarse una auditoría de mantenimiento; esta auditoría se centra, generalmente, en partes del sistema, dada su menor duración, y tiene como objetivo comprobar el uso del SGSI y fomentar y verificar la mejora continua.
- Auditoría de re-certificación: cada tres años, es necesario superar una auditoría de certificación formal completa como la descrita.

2.3.8 Empresas Certificadas en México (11)

Las certificaciones ISO cada vez más se vuelven un requisito para que las empresas establecidas en México puedan no sólo controlar sus estándares internos de calidad, sino también para vender sus productos a las compañías transnacionales.

México contó con 3,946 empresas certificadas ISO 9000 al cierre del 2007, una baja de 14.8% frente al año previo, de acuerdo con la última encuesta difundida por Organización Internacional de Normalización (ISO).

En la misma encuesta, México reportó 739 empresas certificadas con la ISO 14001, un alza de 80.7% frente al 2006. Esta norma permite atender el cuidado del medio ambiente.

2.3.9 Gobiernos certificados (12)

En México se encuentran las siguientes entidades certificadas de gobierno:

- Ayuntamiento de Tijuana
- Desarrollo Integral de la Familia Gobierno del D.F.
- Municipio de Aguascalientes
- Municipio de León
- Secretaria de Turismo
- Subprocuraduría Derechos Humanos del D.F.
- Gobierno del Distrito Federal Delegación Magdalena Contreras
- Secretaria de Administración de Gobierno del Estado de Hidalgo.

2.3.10 Beneficios para los ciudadanos, empleados y dependencias de Gobiernos certificados (13)

Los ciudadanos y otras dependencias se benefician de:

- Contar con una organización que se ha sometido a un riguroso proceso de evaluación realizado en forma competente, imparcial e independiente, y dónde la información es segura gracias a un cuidado constante.
- La existencia de una revisión y mejora continúa sobre el sistema de seguridad que asegura la eficiencia y robustez del mismo.
- La ventaja de la seguridad que aumenta la confianza entre clientes y proveedores.
- Gestionar sus riesgos más eficazmente.
- La protección de la imagen de la dependencia y la administración.

El personal de gobierno se beneficia de:

- La motivación gerencial de poder implantar las mejores prácticas en un área tan sensible.
- El fortalecimiento de la competitividad de la firma, alentando lealtades internas y externas.
- Poder hacerse dueños de la información y su consecuente seguridad
- Asegurar que un apropiado sistema de gestión está instalado para cuidar de la propia información de la organización
- La oportunidad de identificar y corregir las vulnerabilidades detectadas
- La reducción de incidentes de seguridad de la información.

Jerarquizar la protección de la seguridad de la información, al comprender el valor del activo información para el negocio y su continuidad.

2.4 Estándar ISO 17799 (mejores prácticas de seguridad). (14)

2.4.1 Antecedentes del Estándar ISO 17799

Es importante entender los principios y objetivos que dan vida al ISO 17799, así como los beneficios que cualquier organización, incluyendo las instituciones públicas, privadas y ambientes educativos pueden adquirir al implementarlo en sus prácticas de seguridad de la información.

El estándar de seguridad de la información ISO 17799, descendiente del BS 7799 – *Information Security Management Standard* – de la BSI (*British Standard Institute*) que publicó su primera versión en Inglaterra en 1995, con actualizaciones realizadas en 1998 y 1999, consiste de dos partes:

Parte 1. Código de prácticas.
Parte2. Especificaciones del sistema de administración de seguridad de la información.
Por la necesidad generalizada de contar con un estándar de carácter internacional que permitiera reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, se elaboró el estándar ISO17799:2000, basado principalmente en la primera parte del BS 7799 conocida como Código de Prácticas (BS *7799 Part 1: Code of Practice*).

2.4.2 Definición del Estándar ISO 17799 (14)

En toda organización que haga uso de las tecnologías de información se recomienda implementar buenas prácticas de seguridad, pues en muchas ocasiones el no seguir un proceso de implementación adecuado como el que establece el ISO 17799 puede generar huecos por la misma complejidad de las organizaciones, en ese sentido, aumenta la posibilidad de riesgos en la información.

Este estándar internacional de alto nivel para la administración de la seguridad de la información, fue publicado por la ISO (*International Organization for Standardization*) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones.

El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

Confidencialidad. Asegurar que únicamente personal autorizado tenga acceso a la información.

Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

Disponibilidad. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran**.**

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación; no obstante, dependiendo de la naturaleza y metas de las organizaciones, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

2.4.3 Características del Estándar ISO 17799 (14)

El estándar ISO 17799 se caracteriza por dividirse en diez áreas de seguridad con el objeto de incluir todos los distintos puntos de control dentro de una organización y esclarecer los objetivos de estos.

Políticas de seguridad. El estándar define como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

Seguridad organizacional. Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de *outsourcing*, entre otros aspectos.

Clasificación y control de activos. El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

Seguridad del personal. Contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información.
El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

Seguridad física y de entorno. Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

Comunicaciones y administración de operaciones. Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

Control de acceso. Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

Desarrollo de sistemas y mantenimiento. La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

Continuidad de las operaciones de la organización. El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

Requerimientos legales. La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

CAPÍTULO 3

Implementación de Recomendaciones y sus Objetivos en la Coordinación Estatal de Informática y Telecomunicaciones (CEIT) basados en el ISO/IEC 17799

E conjunto con personal de la CEIT se analiza y se establecen los puntos adecuados del estándar a implementar y asignar al departamento adecuado para llevar a cabo la supervisión de los mismos.

La CEIT se encuentra dividida en 5 áreas o departamentos, cada una orientada a determinada actividad relacionada con el funcionamiento de la Red Informática de Gobierno del Estado, estos son:

1. Departamento de Seguridad Perimetral y Servicios Electrónicos

   Función: Establecer políticas, normas y estándares de seguridad, proporcionar servicios electrónicos y de comunicación a las unidades administrativas del Gobierno del estado, así como todas las herramientas necesarias para desarrollar sus funciones con mayor rapidez, eficiencia y calidad, garantizando la administración y seguridad, tanto de los servidores como de los enlaces, equipo de computo y cualquier otro dispositivo que se encuentre dentro de la Red Gubernamental con los que cuentan las instalaciones de informática.

2. Departamento de Telecomunicaciones.

   Función: Administrar, operar y proporcionar a las Dependencias y Entidades del Gobierno del Estado redes estructuradas que integren los servicios de Voz y Datos necesarios para satisfacer las necesidades de comunicación de todas sus Áreas, así como mantener en óptimas condiciones de uso y operación la Red Gubernamental de Comunicaciones. Proporcionar el servicio tecnológico en materia de informática a las diferentes áreas que componen a las entidades del Poder Ejecutivo.

3. Departamento de Servicios WEB.

   Función: Establecer Estándares y Políticas del Diseño de Portales, para supervisar la correcta creación de los Portales Institucionales de los Órganos Descentralizados, Entidades y Dependencias del Ejecutivo Estatal.

4. Departamento de Ingeniería de Software.

   Función: Administrar y supervisar proyectos en materia de Tecnologías de Información y Comunicaciones por medio del uso de estándares, metodologías y procedimientos que aseguren la entrega de mejores servicios.

5. Departamento de Gestión y Servicios Tecnológicos.

   Función: Llevar a cabo el registro de todas las actividades que sean realizadas por cada uno de los departamentos de la Coordinación, así como de realizar las gestiones administrativas que involucren a las diversas áreas; además de realizar el mantenimiento preventivo y correctivo de todo aquel equipo que sea canalizado a la coordinación para supervisión.

Las recomendaciones y sus objetivos se derivan directamente y se alinean con aquellos enumerados en ISO/IEC 17799. Las listas mencionadas no son exhaustivas, debido a que la Coordinación podrá considerar cuales podrían ser o no necesarios, además, en cada uno de los puntos se especifica el departamento de la CEIT al que le corresponderá vigilar el cumplimiento de dicho punto.

3.1 Recomendaciones y sus objetivos

Se presentan a continuación las recomendaciones acompañadas cada una de sus objetivos, además de mencionar el o los departamentos de la Coordinación que deben involucrarse en el desarrollo de cada una de las recomendaciones:

3.2 Política de seguridad

3.2.1 Política de seguridad de información:

Objetivos: Proporcionar una dirección gerencial y apoyo en la seguridad de la información en organización, estableciendo requerimientos administrativos, normas y recomendaciones y regulaciones relevantes para la organización. Esta política presenta las siguientes recomendaciones:

3.2.1.1 Documentar la política de seguridad de la información.

El departamento encargado de regular los procedimientos debe aprobar un documento donde se especifiquen todas las políticas a ser aplicados en cada área, éste se debe publicar y comunicar a todos los empleados y entidades externas relevantes.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.2.1.2 Revisión de la política de seguridad de la Información

La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.3 Organización de la seguridad de la información

3.3.1 Organización interna

Objetivo*:* Manejar la seguridad de la información dentro de la organización. Presentando las siguientes recomendaciones:

3.3.1.1 Compromiso de los directores con la seguridad de la información.

Los jefes de departamento deben apoyar activamente en la seguridad dentro de la organización a través de una dirección clara, un compromiso demostrado, la asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.3.1.2 Coordinación de la seguridad de información.

Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.3.1.3 Asignación de responsabilidades de la seguridad de la información.

Se deben definir claramente las responsabilidades de la seguridad de la información

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.3.1.4 Proceso de autorización para los medios de procesamiento de información.

Se debe definir e implementar un proceso de autorización gerencial para nuevos medios de procesamiento de información.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.3.1.5 Acuerdos de Confidencialidad.

Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no divulgación reflejando las necesidades de la organización para la protección de la información.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.3.1.6 Contacto con autoridades.

Se debe mantener los contactos apropiados con las autoridades competentes.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.3.1.7 Contacto con grupos de interés especial.

Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.3.1.8 Revisión independiente de la seguridad de la información.

El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.3.2 Entidades externas

Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales las entidades externas tienen acceso y procesan; o son comunicados o manejados por entidades externas. Se tienen las siguientes recomendaciones:

3.3.2.1 Identificación de riesgos relacionados con entidades externas.

Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso a entidades externas.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.3.2.2 Seguridad cuando se trabaja con la población en general.

Se deben especificar todos los requerimientos de seguridad a cumplir y tenerlos bien identificados antes de otorgar al público en general acceso a la información o algún activo de la organización.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.3.2.3 Seguridad en contratos con terceras personas.

Se deben de establecer y fijar plenamente los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas en la información o los medios de procesamiento de información de la organización; y al agregar productos o servicios a los medios de procesamiento de la información se deben abarcar los requerimientos de seguridad necesarios relevantes.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.4 Gestión de activos

3.4.1 Responsabilidad por los activos

Objetivo*:* Lograr y mantener la protección apropiada de los activos de la organización.

3.4.1.1 Inventariar todos los activos

Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.4.1.2 Propiedad de los activos

Toda la información y los activos asociados con los medios de procesamiento de la información deben ser “propiedad” de una parte designada de la organización.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.4.1.3 Uso aceptable de los activos

Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.4.2 Clasificación de la Información

Objetivo: Asegurar que la información reciba un nivel de protección apropiado.

3.4.2.1 Lineamientos de clasificación

La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.4.2.2 Etiquetado y manejo de la Información

Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.5 Seguridad de los recursos humanos

3.5.1 Antes del empleo

Objetivo*:* Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; de esta forma reducir el riesgo de robo, fraude o mal uso de los medios.

3.5.1.1 Roles y responsabilidades

Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.5.1.2 Selección

Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos gubernamentales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.5.1.3 Términos y condiciones de empleo

Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar los términos y condiciones de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.5.2 Durante el empleo

Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.

3.5.2.1 Gestión de Responsabilidades

La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.5.2.2 Capacitación y educación en seguridad de la información

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.5.2.3 Proceso Disciplinario

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.5.3 Terminación o cambio del empleo

Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.

3.5.3.1 Responsabilidades de terminación.

Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio de lugar de empleo.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.5.3.2 Devolución de Activos

Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.5.3.3 Eliminación de derechos de acceso

Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.6 Seguridad física y ambiental

3.6.1 Áreas seguras

Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al edificio y a la información de la organización.

3.6.1.1 Perímetro de seguridad física.

Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.1.2 Controles de entrada físicos.

Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.1.3 Seguridad del edificio

Se deben diseñar y aplicar métodos que permitan contar con seguridad física en las oficinas, departamentos y especialmente en los sitios donde se concentren los equipos informáticos de más alto valor institucional.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.1.4 Protección contra amenazas externas y ambientales

Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.1.5 Trabajo en áreas seguras

Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.1.6 Áreas de acceso público, entrega y carga

Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no autorizadas pueden ingresar al edificio, y cuando fuese posible, se deben aislar de los medios de procesamiento de información para evitar un acceso no autorizado.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.2 Seguridad del equipo

Objetivo*:* Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

3.6.2.1 Ubicación y protección del equipo

El equipo debe estar en perfecta ubicación o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.2.2 Servicios Públicos

El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.2.3 Seguridad en el cableado

El cableado de la energía y de telecomunicaciones que llevan información o sostienen los servicios de información debe ser protegido de la intercepción o daño.

Departamento Involucrado: Telecomunicaciones.

3.6.2.4 Mantenimiento de equipo

El equipo debe de recibir mantenimiento periódicamente, previamente establecido en un calendario, para así permitir su continua disponibilidad e integridad

Departamento Involucrado: Telecomunicaciones.

3.6.2.5 Seguridad del equipo fuera del edificio

Se debe aplicar seguridad al equipo que se encuentre fuera del edificio tomando en cuenta los diferentes riesgos de trabajar fuera de la organización.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.2.6 Eliminación segura o reutilización del equipo

Todos los componentes de los equipos que contengan medios de almacenaje deben ser chequeados para asegurar que se halla removido o sobrescrito de manera segura cualquier información confidencial y software con licencia antes de su eliminación.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.6.2.7 Traslado de Propiedad

No deberán de ser extraídos los equipos, información o cualquiera que sea el software fuera de la propiedad sin previa autorización.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.7 Gestión de las comunicaciones y operaciones

3.7.1 Procedimientos y responsabilidades operacionales

Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.

3.7.1.1 Procedimientos de Operación documentados

Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.7.1.2 Gestión de cambio.

Se deben controlar y documentar los cambios en los medios y sistemas donde se procesa la información.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.7.1.3 Segregación de deberes

Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no autorizada o no intencionada o un mal uso de los activos de la organización.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.7.1.4 Separación de los medios de desarrollo y operacionales

Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en la operación de los sistemas.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.7.2 Gestión de la entrega del servicio de terceros

Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información, así como la entrega de servicios en línea de terceros.

3.7.2.1 Entrega del Servicio

Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad estipulados, así como definir los servicios que utilizaran y los niveles de acceso al que tendrán, estableciéndolos previamente al momento que solicitan algún servicio.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.7.2.2 Monitoreo y revisión de los servicios de terceros

Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.7.2.3 Manejar los cambios en los servicios de terceros.

Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos involucrados, así como la evaluación de los riesgos en el caso de realizar los cambios.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.7.3 Planeación y aceptación del sistema.

Objetivo: Minimizar el riesgo de fallas en los sistemas.

3.7.3.1 Gestión de Capacidad

Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.

Departamento Involucrado: Ingeniería de Software.

3.7.3.2 Aceptación del sistema

Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.

Departamento Involucrado: Ingeniería de Software.

3.7.4 Protección contra software malicioso y código móvil

Objetivo: Proteger la integridad del software y la información.

3.7.4.1 Controles contra software malicioso

Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos maliciosos y se deben implementar procedimientos de contingencia apropiados.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.7.4.2 Controles contra códigos móviles

Cuando se autoriza el uso de un código móvil para una configuración, se debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado.

Departamento Involucrado: Ingeniería de Software.

3.7.5 Respaldo (back-up)

Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.

3.7.5.1 Back-up o respaldo de la información

Se deben realizar copias de back-up o respaldo de la información vital y software esencial para la organización y se deben probar regularmente de acuerdo a la política.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.7.6 Monitoreo.

Objetivo: Detectar actividades de procesamiento de información no autorizadas.

3.7.6.1 Registro de Auditoria

Se deben producir registros de las actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.7.6.2 Uso del sistema de monitoreo

Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y se debe revisar regularmente el resultado de las actividades de monitoreo.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.7.6.3 Protección de la información del registro

Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no autorizado.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.7.6.4 Registros del administrador y del operador

Se deben registrar las actividades del administrador y del operador del(los) sistema(s).

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.7.6.5 Registro de fallas.

Las fallas deben ser registradas y analizadas para poder tomar la acción apropiada.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.7.6.6 Sincronización de relojes

Los relojes de los sistemas de procesamiento de información más relevantes de una organización o dominio de seguridad, deben estar sincronizados con una fuente de tiempo exacta acordada.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8 Control de acceso.

3.8.1 Requerimiento para el control del acceso

Objetivo: Controlar acceso a la información.

3.8.1.1 Política de control de acceso

Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y gubernamentales.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.2 Gestión del acceso del usuario

Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.

3.8.2.1 Inscripción del usuario

Debe existir un procedimiento formal para otorgar y quitar acceso a todos los sistemas y servicios de información.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.2.2 Gestión de privilegios

Se debe restringir y controlar la asignación y uso de privilegios para cada determinada área específica.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.2.3 Gestión de la clave del usuario

La asignación de claves se debe controlar a través de un proceso de gestión formal.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.2.4 Revisión de los derechos de acceso del usuario

El administrador debe revisar los derechos de acceso de los usuarios a intervalos regulares mediante un proceso formal y regulado.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.8.3 Responsabilidades del usuario

Objetivo: Evitar el acceso de usuarios no autorizados, y así evitar comprometer o el robo de la información y de los medios de procesamiento de la información.

3.8.3.1 Uso de clave

Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.8.3.2 Equipo de usuario desatendido

Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.8.3.3 Política de pantalla y escritorio limpio

Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.8.4 Control de acceso a redes

Objetivo: Evitar el acceso no autorizado a los servicios en red.

3.8.4.1 Política sobre el uso de servicios en red

Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.4.2 Autenticación del usuario para conexiones externas

Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.4.3 Identificación del equipo en red.

Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.

Departamento Involucrado: Departamento de Telecomunicaciones.

3.8.4.4 Protección del puerto de diagnóstico remoto

Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.

Departamento Involucrado: Departamento de Telecomunicaciones.

3.8.4.5 Segregación en redes

Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.

Departamento Involucrado: Departamento de Telecomunicaciones.

3.8.4.6 Control de conexión de redes.

Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso.

Departamento Involucrado: Departamento de Telecomunicaciones.

3.8.4.7 Control de Ruteo “routing” en las redes

Se deben implementar controles Ruteo para las redes, para asegurar que las conexiones de cómputo y los flujos de información no infrinjan las políticas de control de acceso de las aplicaciones y la información privilegiada.

Departamento Involucrado: Departamento de Telecomunicaciones

3.8.5 Control de acceso al sistema de operación

Objetivo: Evitar acceso no autorizado a los sistemas operativos.

3.8.5.1 Procedimientos de registro en los equipos.

Se debe controlar el acceso a los servicios que se otorguen, incluso a los sistemas operativos en los cuales estén operando, mediante un procedimiento de registro seguro.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.5.2 Identificación y autenticación del usuario

Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.5.3 Sistema de gestión de claves.

Se deben de establecer sistemas de manejo de claves y estos deben ser interactivos y deben asegurar la calidad de las mismas.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.5.4 Uso de utilidades del sistema

Se debe restringir y controlar estrictamente el uso de programas que podrían superar al sistema y los controles de seguridad en las aplicaciones.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.5.5 Sesión inactiva

Las sesiones inactivas deben cerrarse después de un período de inactividad definido.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.5.6 Limitación de tiempo de conexión

Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.6 Control de acceso a la aplicación e información

Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas.

3.8.6.1 Restricción al acceso de la información

Se debe restringir el acceso de los usuarios y personal de soporte a los sistemas y aplicaciones en concordancia con la política de control de acceso definida

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.6.2 Aislamiento de sistemas sensibles

Los sistemas sensibles deben estar en un ambiente dedicado (aislado).

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos

3.8.7 Computación móvil y de teletrabajo

Objetivo: Ofrecer seguridad a la información cuando se utilicen equipos de cómputo móviles y de teletrabajo.

3.8.7.1 Computación móvil y comunicaciones

Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger los sistemas contra los riesgos que genera utilizar medios de cómputo y comunicación móviles.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.8.7.2 Teletrabajo.

Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de teletrabajo.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9 Adquisición, desarrollo y mantenimiento de sistemas

3.9.1 Requerimientos de seguridad de los sistemas

Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.

3.9.1.1 Análisis y especificación de los requerimientos de seguridad

Los enunciados de los requerimientos para sistemas nuevos, o para mejorar los sistemas existentes deben especificar los requerimientos de controles de seguridad.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9.2 Procesamiento correcto en las aplicaciones

Objetivo: Evitar errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.

3.9.2.1 Validación de la información en los insumos.

Los insumos utilizados para almacenar información de los sistemas deben de ser validados para asegurar que esta información sea correcta y apropiada.

Departamento Involucrado: Ingeniería de Software.

3.9.2.2 Control de Procesamiento interno

Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.

Departamento Involucrado: Ingeniería de Software.

3.9.2.3 Integridad del mensaje

Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de los mensajes en las aplicaciones, y se deben identificar e implementar los controles apropiados para garantizar su seguridad.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9.2.4 Validación de la información de salida

Se debe validar la salida de la información de cualquier aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.

Departamento Involucrado: Ingeniería de Software.

3.9.3 Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad e integridad de la información a través de medios criptográficos.

3.9.3.1 Política sobre el uso de controles criptográficos

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9.3.2 Gestión clave.

Se deben administrar muy celosamente las claves, para dar soporte al uso de las técnicas de criptografía usadas en la organización.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9.4 Seguridad de los archivos del sistema

Objetivo: Garantizar la seguridad de los archivos del sistema.

3.9.4.1 Control del Software operacional

Se debe contar con procedimientos para controlar y regular la instalación de software en los sistemas operacionales.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9.4.2 Proteger la información de los sistemas de prueba.

Se debe seleccionar cuidadosamente la información que se maneje en los sistemas de prueba, así como protegerla y controlar su uso.

Departamento Involucrado: Ingeniería de Software.

3.9.4.3 Control de acceso al código fuente de los sistemas.

Se debe restringir el acceso al código fuente de cualquier sistema.

Departamento Involucrado: Ingeniería de Software.

3.9.5 Seguridad en los procesos de desarrollo y soporte

Objetivo*:* Mantener la seguridad del software e información de los sistemas de aplicación.

3.9.5.1 Procedimientos de control de cambio.

La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.

Departamento Involucrado: Ingeniería de Software.

3.9.5.2 Revisión técnica de las aplicaciones después de cambios en el sistema operativo.

Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas de la organización para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9.5.3 Restricciones sobre los cambios en los paquetes de software

No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser registrados y estrictamente controlados.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9.5.4 Filtración de Información

Se deben evitar las oportunidades de filtraciones en la información.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.9.5.5 Desarrollo de Outsourced software

El desarrollo de software que ha sido creado por un outsourced debe ser supervisado y monitoreado.

Departamento Involucrado: Ingeniería de Software.

3.9.6 Gestión de vulnerabilidad técnica

Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas en los sistemas.

3.9.6.1 Control de vulnerabilidades técnicas

Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.

Departamentos Involucrados: Seguridad Perimetral y Servicios Electrónicos.

3.10 Gestión de incidentes en la seguridad de la información.

3.10.1 Reporte de eventos y debilidades en la seguridad de la información.

Objetivo*:* Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.

3.10.1.1 Reporte de eventos en la seguridad de la información

Los eventos de seguridad de la información deben reportarse a través de los canales apropiados lo más rápidamente posible.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.10.1.2 Reporte de debilidades en la seguridad.

Se debe requerir que todos los empleados, usuarios de sistemas y terceros usuarios de los mismos y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.10.2 Gestión de incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar que se aplique un enfoque consistente y efectivo en la seguridad de la información.

3.10.2.1 Responsabilidades y procedimientos.

Se deben establecer las responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.10.2.2 Aprendizaje de los incidentes en la seguridad de la información.

Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.10.2.3 Recolección de evidencia

Ocurra o no la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se deberá de recolectar, mantener y presentar evidencia, para así cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.11 Continuidad en la Organización.

3.11.1 Aspectos de la seguridad de la información en la continuidad de la organización

Objetivo: Contrarrestar las interrupciones de las actividades y proteger los procesos críticos de defectos, fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

3.11.1.1 Incluir seguridad de la información en la continuidad de la organización

Se debe desarrollar y mantener uno o varios procesos que permitan la continuidad de los procesos en toda la organización, así como determinar los requerimientos de seguridad de la información necesarios para la continuidad de la organización.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.11.1.2 Continuidad organizacional y evaluación del riesgo

Se deben identificar los eventos que causan interrupciones en los procesos, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.11.1.3 Desarrollar e implementar planes de continuidad incluyendo seguridad de la información

Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos críticos.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.11.1.4 Marco referencial para la planeación de la continuidad de la organización.

Se debe mantener un solo marco referencial de planes de continuidad para asegurar que todos los planes sean consistentes y así tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.11.2 Prueba, mantenimiento y reevaluación de planes para asegurar la continuidad.

Los planes de continuidad se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.12 Cumplimiento

3.12.1 Cumplimiento con requerimientos legales

Objetivo*:* Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.

3.12.1.1 Identificación de la legislación aplicable.

Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y para la organización.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.12.1.2 Derechos de Propiedad intelectual

Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.12.1.3 Protección los registros de la Organización.

Se deben proteger de pérdida, destrucción y falsificación, todos los registros importantes de una organización, en concordancia con los requerimientos estatutarios, reguladores, contractuales, organizacionales y comerciales.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.12.1.4 Protección de la información y privacidad de la información personal

Se debe asegurar la protección y privacidad de toda la información y esta debe de ser regulada.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.12.1.5 Prevención de mal uso de medios de procesamiento de información

Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no autorizados.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.12.1.6 Regulación de controles criptográficos

Se deben utilizar controles para el cumplimiento de controles criptográficos de acuerdo a regulaciones establecidas.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.12.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico.

Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

3.12.2.1 Cumplimiento de las políticas y estándares de seguridad

Los encargados deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.

Departamento Involucrado: Gestión y Servicios Tecnológicos.

3.12.2.2 Chequeo de Cumplimiento técnico.

Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.

Departamento Involucrado: Ingeniería de Software.

3.12.3 Consideraciones de auditoría de los sistemas de información.

Objetivo: Maximizar la efectividad y minimizar la interferencia desde el proceso de auditoría de los sistema de información.

3.12.3.1 Controles de auditoría de sistemas de información

Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

3.12.3.2 Protección de las herramientas de auditoría de los sistemas de información.

Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Departamento Involucrado: Seguridad Perimetral y Servicios Electrónicos.

CAPÍTULO 4

AUDITORÍA EN LA ORGANIZACIÓN.

4.1 Estableciendo Auditorías.

Una vez establecidas las recomendaciones del estándar en cada una de las áreas de acción y ya estando en ejecución la organización debe realizar procesos de auditoría, en los cuales se debe hacer lo siguiente:

- ✓ Ejecutar procedimientos de monitoreo y revisión, y otros controles para:

  1. Detectar prontamente los errores en los resultados de procesamiento.
  2. Identificar prontamente los incidentes y violaciones de seguridad fallidas y exitosas.
  3. Permitir a los administradores determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba.
  4. Ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores.
  5. Determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

- ✓ Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.

- ✓ Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

- ✓ Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:

1. La organización.
2. Tecnología.
3. Objetivos y procesos comerciales.
4. Amenazas identificadas.
5. Efectividad de los controles implementados.
6. Eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.

✓ Realizar auditorías SGSI internas a intervalos planeados.

NOTA: Las auditorías internas, algunas veces llamadas auditorías de primera persona, son realizadas por, o en representación de, la organización misma para propósitos internos.

✓ Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI.

✓ Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.

✓ Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI.

4.2 Mantener y mejorar el SGSI

Dependiendo de los resultados de las auditorias previamente señaladas, la organización debe realizar regularmente lo siguiente:

✓ Implementar las mejoras identificadas en el SGSI.

1. Tomar las acciones correctivas y preventivas apropiadas en concordancia con los puntos establecidos dependiendo del área en donde se presenten las anomalías.
2. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.
3. Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar cómo proceder.

✓ Asegurar que las mejoras logren sus objetivos señalados.

CAPÍTULO 5

CONCLUSIONES.

La promoción y aplicación de estándares de seguridad en la Coordinación Estatal de Informática y Telecomunicaciones (CEIT) del Gobierno del Estado permitirán una correcta administración de la infraestructura en Tecnologías de la Información como con el personal que interactúa directamente con los equipos e inclusive con los sistemas que prestan el servicio solicitado por la población en general, además proporcionará una correcta forma para divulgar el conocimiento y fomentar la colaboración digital, para el óptimo desempeño de sistemas y esquemas tanto tecnológicos como humanos con el fin de adquirir, organizar y comunicar el conocimiento aprendido en la CEIT a todo Gobierno Estatal.

La aplicación de estándares en procesos que involucran tecnologías de información permite el desarrollo, actualización y consolidación de los sistemas informáticos y de la correcta administración de los bienes gubernamentales en las distintas dependencias estatales, además de facilitar la actualización informática y de los procesos que operan las tareas adjetivas y sustantivas de las instituciones públicas.

Une mejor divulgación de la información sobre trámites y servicios electrónicos brindaran al ciudadano la oportunidad de acceder a la prestación de éstos a través de los medios electrónicos, los cuales al estar certificados, permitirán ofrecer calidad en el servicio que se le proporciona a la comunidad en general y en consecuencia traerá satisfacción y un enorme beneficio a la misma, atrayendo fuentes de inversión entre otras cosas. En este propósito ha sido relevante que las dependencias y entidades del Gobierno mantengan una constante actualización y rediseño para seguir incorporando los servicios y trámites a los estándares tecnológicos de mayor impacto a la ciudadanía, en las políticas y mecanismos de seguridad y salvaguarda de privacidad de información, fundamentados en una plataforma tecnológica intergubernamental que permita la integración de toda la información relativa a servicios y trámites gubernamentales.

Bibliografía

1. **Roo, Gobierno del Estado de Quintana.** *Manual de Políticas y Normatividad Informática y Telecomunicaciones de Gobierno del Estado de Quintana Roo.* Chetumal, Quintana Roo : Gobierno del Estado de Quintana Roo, 2010.

2. **Norton, Peter.** *Introducción a la Computación.* s.l. : Mc Graw Hill.

3. **Gallardo Rebolloso, Roberto.** *La globalización y las nuevas tecnologías.* México : Trillas, 2000.

4. **Rosario, Jimmy.** La Tecnología de la Información y la Comunicacion (TIC). *Su uso como Herramienta para el Fortalecimiento y el Desarrollo de la Educación Virtual.* [En línea] Cibersociedad, 2005. [Citado el: 14 de Junio de 2012.] http://www.cibersociedad.net/archivo/articulo.php?art=218.

5. **UNAM.** ¿Qué es la tecnología de la información? [En línea] UNAM, 4 de Julio de 2010. [Citado el: 6 de Julio de 2010.] http://www.tuobra.unam.mx/publicadas/040702105342-__191_Qu.html.

6. —. Estándares de seguridad en la información. [En línea] UNAM, 27 de Noviembre de 2008. [Citado el: 1 de Julio de 2010.] http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm.

7. **Normalización.** Ley Federal sobre Metrología y Biblioteca de Leyes. *Diputados Federales. Última Reforma.* [En línea] 30 de Abril de 2009. [Citado el: 11 de Junio de 2010.] http://www.diputados.gob.mx/LeyesBiblio/pdf/130.pdf.

8. **AENOR.** Aenor México. *Sistemas de Gestión.* [En línea] 2010. http://www.aenormexico.com/.

9. **SYSTEM, BSI MANAGEMENT.** BSI Management Systems. *Súper Empresa.* [En línea] BSI Management Systems, 2010. [Citado el: 11 de Junio de 2010.] http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/Noticias-y-eventos/Nuevas-

noticias/Noticias-recientes/BSI-Management-Systems-Mexico-Super-Empresa/.

10. **27000, ISO.** Sistemas de Gestión de la Seguridad de la información. [En línea] 2005 Aviso legal - Términos de uso de información iso27000.es. [Citado el: 29 de Junio de 2010.] www.iso27000.es.

11. **Institution, The British Standards.** Directorio de clientes registrados de sistemas de gestión, empresas que cuentan con certificaciones, como ISO 9001, ISO/TS 16949, ISO 14001, BS OHSAS 18001. [En línea] [Citado el: 15 de Junio de 2010.] http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Directorio-de-clientes/.

12. **INTERNACIONAL, AENOR.** Aenor Internacional. [En línea] 2010. [Citado el: 10 de Junio de 2010.] http://www.aenorinternacional.com/ESP/buscador/empresas.asp.

13. **Ruiz Medina, Eugenia Margarita.** *La importancia de la implementación de la norma ISO 9001-2000 y la respuesta de las empresas en México*. Chetumal, Quintana roo, México : Trabajo Monográfico, Mayo de 2005.

14. *ISO/IEC 17799 Code of Best Practice for Information Security Management.*