IMPORTANCIA DE LA IMPLEMENTACIÓN DEL SGSI 27001 EN LA SEGURIDAD INFORMÁTICA DE ACESCO

NÉSTOR MAURICIO VILLEGAS CORTÉS

SANTIAGO GAVIRIA VALENCIA

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTÁ, OCTUBRE 14 DE 2011

e-mail

nemavico@hotmail.com

gaviria_santiago@hotmail.com

1. Resumen.

La base de datos de toda organización, constituye el corazón de la misma. Por tal razón, ante el avance imparable de las nuevas tecnologías, nace la necesidad de asegurar la información. En este escenario se analizan las diferentes opciones, se hace un análisis de riesgos por el método Mossler y se determina que los principales riesgos que nos pueden afectar son: la filtración, el hurto o robo, la modificación o saboteo y la eliminación de la información. Después de mucho indagar tomamos la decisión de profundizar en el mejor sistema, o el que mejor se adapta a las necesidades de nuestra organización. **El Sistema de Gestión de la Seguridad de la Información SGSI** y dentro de éste, estudiamos la (1)**Norma ISO 27001**, con el fin de venderle a la Junta Directiva de la Compañía, la idea de generar unos procesos y procedimientos, considerando establecer unos parámetros para estructurar y garantizar que los riesgos de la seguridad de la información sean minimizados por nuestra empresa oportunamente.

Palabras Claves.

Sistema, Gestión, Seguridad, Información, Confidencialidad, Integridad, Disponibilidad, Planear, Hacer, Verificar, Actuar, Procesos, Procedimientos.

2. Introducción.

La seguridad privada en Colombia conforma uno de los pilares fundamentales del eje social y laboral de la nación, teniendo en cuenta que dicho gremio es el segundo a nivel de generación de empleo, se puede considerar el importante lugar que ocupa dentro de la economía del país.

---

*(1)**Norma ISO 27001** : Norma estándar para la seguridad de la información publicado por primera vez como ISO/IEC27001:2006 por la International Organization for Standardization en el año 2006.*

Adicionalmente, constituye un factor fundamental como soporte de la seguridad democrática en las áreas urbanas conformando la Red de Apoyo y Solidaridad Ciudadana.

Fue por ese motivo que el Gobierno Nacional emitió el (2) Decreto 3222 de 2002, por medio del cual se crean las Redes de Apoyo y Solidaridad Ciudadana, con el fin de comprometer al personal que presta los diferentes servicios de seguridad privada, en apoyo permanente a la fuerza pública.

Dentro de la seguridad privada se presenta un componente esencial, "la seguridad informática", este campo debe ser considerado de suma importancia por todas y cada una de las empresas del país, dado que en la base de datos reposa gran parte del éxito de las mismas y protegerlas debería convertirse en un esfuerzo permanente.

Por otro lado, también se debe valorar la importancia de ésta en cuanto a la estrategia comercial y de servicio al cliente de las diferentes compañías.

Por las razones expuestas anteriormente, hemos querido realizar ésta investigación concerniente a la importancia que se le debe dar a la protección de la base de datos de clientes dentro de una compañía siderúrgica de características muy particulares y específicas, más aún ante las eventuales negociaciones que se puedan presentar en un futuro, teniendo presente el reto que constituye la globalización del comercio.

La intención al desarrollar ésta investigación, es la de generar oportunamente una concientización al interior de la Junta Directiva de la empresa Acerías de Colombia ACESCO & Cía. S.C.A. para la cual laboro en la actualidad y que presenta grandes falencias respecto a la seguridad que se le debe brindar a la base de datos…

---

(2)Decreto 3222 de 2002: Norma Reglamentaria por la cual el Gobierno nacional crea y autoriza las Redes de apoyo y Solidaridad Ciudadana.

Considerando que se acerca una negociación y la permanente fuga de información concerniente a las ofertas presentadas a los posibles clientes podría convertirse en una gran vulnerabilidad estratégica comercial para la compañía, se debe convertir en una prioridad, la seguridad de dicha base de datos.

Si al final del trabajo se logra convencer a la junta de la trascendencia del tema, me daré por bien servido.

Marco Teórico.

Aprovechando la oportunidad que brinda la especialización en Administración de la Seguridad y la exigencia por parte de la Universidad de presentar un trabajo de investigación, se aplicarán los conocimientos adquiridos durante la materia Seguridad Informática, dictada por el Dr. Sánder Alberto Sánchez Arango, profundizando en las páginas web, bibliografía concerniente al tema y algunos artículos referentes, con el fin de lograr la elaboración de un documento bien sustentado y estructurado para presentar a la Junta Directiva de la Compañía, la importancia que hay actualmente al interior de la empresa; Ante la problemática que genera la constante fuga de información y la necesidad de tomar todas las medidas de seguridad informática en aras de garantizar la adecuada protección de la base de datos comercial de clientes, implementando sistemas tales como:

Direcciones IP Dinámicas, que permitan cambiar la dirección IP 2 ó 3 veces en un día.

Políticas de Seguridad en Redes, evitando pérdidas de datos o la revelación de información no autorizada para ser difundida.

La Encriptación de la Información, que consiste en utilizar un algoritmo para que la información sea indescifrable a simple vista y requiera otro algoritmo para devolverle su significado inicial.

3. Desarrollo

Términos fundamentales en la Seguridad de la Información.

Confidencialidad: Acceso a la información solo por parte de los autorizados.

Integridad: Se mantiene intacta la exactitud de la información.

Disponibilidad: Acceso inmediato a la información cuando se requiera.

La implementación de un SGSI, nos permite proteger la información, junto con los procesos y sistemas que hacen uso de ella. La confidencialidad, la integridad y la disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

El SGSI, nos protege además de los riesgos informáticos, de cualquier evento extraordinario, como una catástrofe natural, asonada, un incendio, etc...

El nivel de seguridad alcanzado por medios técnicos demuestra ser invariablemente limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la empresa, con la dirección al frente y se debe considerar, adicionalmente, a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implementación de controles de seguridad basadas en una evaluación de riesgos y una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos propios y de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información; Los asume, minimiza, transfiere y/o controla.

Implementación de un SGSI

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información, se utiliza el ciclo continuo (3)PHVA, tradicional en los sistemas de gestión de la calidad.

---

(3)PHVA: Ciclo continuo de la Metodología de Planeación que significa Planear , Hacer, Verificar y Actuar.

Planear: Establecer el SGSI.

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

Definir una política de seguridad que:

Incluya el marco general y los objetivos de seguridad de la información de la organización.

Considere requerimientos legales o contractuales relativos a la seguridad de la información.

Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI.

Establezca los criterios con los que se va a evaluar el riesgo.

Esté aprobada por la dirección.

Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y unos criterios de aceptación de los mismos.

Identificar los riesgos:

-Activos que están dentro del alcance del SGSI y a sus responsables directos.

-Las amenazas en relación a los activos.

-Las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.

-Los impactos en la confidencialidad, integridad y disponibilidad de los activos.

Analizar y evaluar los riesgos:

El impacto que le genera al negocio de la organización una falla de seguridad que ocasione la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.
De forma real la probabilidad de ocurrencia de una falla de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.

Estimar los niveles de riesgo.

Determinar si el riesgo es aceptable o necesita ser tratado.

Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

Aplicar controles adecuados.
Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos.
Evitar el riesgo mediante el cese de las actividades que lo originan.
Transferir el riesgo a terceros.
Seleccionar los controles para el tratamiento del riesgo y que cumplan con los requerimientos identificados en el proceso de evaluación y tratamiento del mismo.

Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

Definir una declaración de aplicabilidad que incluya objetivos de control: Seleccionados y motivos para su elección, implementados actualmente, excluidos y los motivos para su exclusión. Este mecanismo nos permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, la norma ISO 27001 proporciona una completa guía de implementación que contiene 133 controles, según 39 objetivos de control agrupados en 11 cláusulas.

Hacer: Implementar y utilizar el SGSI.

Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de riesgos de seguridad de la información.
Implementar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados y que incluya financiación, asignación de roles y responsabilidades.
Definir un sistema de medidas que permita cuantificar los resultados.
Desarrollar programas de capacitación en seguridad de la información dirigidos a todo el personal.
Gestionar las operaciones del SGSI y los recursos necesarios para mantener la seguridad de la información.
Implementar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Verificar: Monitorear y revisar el SGSI

La organización deberá:

Ejecutar procedimientos de monitorización y revisión para:

-Detectar oportunamente los errores en los resultados generados por los procesos.

-Identificar las brechas e incidentes de seguridad.

-Capacitar a la dirección para determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan adecuadamente.

-Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.

-Determinar la efectividad de las acciones realizadas para evitar brechas de seguridad.

-Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

-Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

-Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.

-Realizar auditorías internas del SGSI en intervalos planificados y el SGSI por parte de la dirección para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

-Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

-Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Actuar: Mantener y mejorar el SGSI

La organización deberá regularmente:

Implementar en el SGSI las mejoras identificadas.

Realizar las acciones preventivas y correctivas adecuadas con base en las lecciones aprendidas de las experiencias propias y de otras organizaciones.

Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

Elementos del Sistema de Gestión de la Seguridad de la Información

Manual de seguridad:

Alcance del SGSI: ¿Hasta qué áreas de la empresa llega el SGSI?

Política y Objetivos de Seguridad: ¿Qué compromiso hay por parte de la dirección?

Metodología de Evaluación de Riesgos: ¿Cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información?

Informe de Evaluación de Riesgos: Estudio metodológico de Evaluación de Riesgos.

Plan de Tratamiento del Riesgo: Define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información e implementar los controles necesarios para protegerla.

Declaración de Aplicabilidad: Contiene los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Procedimientos:

Aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen cómo medir la efectividad de los controles.

Instrucciones, listas de verificación y formularios:

¿Cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información?

Registros:

Proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI.

Norma Técnica ISO 27001

Después de analizar el Sistema Integrado de Seguridad de la Información, hemos tomado la decisión de implementar la norma que mejor se adapta a nuestras necesidades. La ISO 27001, razón por la cual, vamos a profundizar un poco al respecto.

Los principales dominios u objetivos que debemos controlar al interior de la compañía son:

Las Políticas de Seguridad

La Seguridad Organizacional

La Clasificación y el Control de los Activos

La Seguridad del Personal

La Seguridad Física

La Gestión de Comunicaciones y Operaciones

El Control de los Accesos

El Desarrollo y el Mantenimiento del Sistema

La Gestión de la Continuidad del Negocio

El Cumplimiento

Las Políticas de Seguridad

Brindan orientación y apoyo de la dirección, para la seguridad de la información.

La Dirección deberá establecer una política clara y manifestar su apoyo a la seguridad de la información y compromiso con ésta, mediante la publicación y mantenimiento de las políticas de seguridad en toda la organización.

La Seguridad Organizacional

Gestiona la seguridad de la información dentro de la organización.

Establecer un marco de trabajo de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Es conveniente organizar comités de gestión adecuados con los líderes de la dirección, para aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar la implementación de la seguridad en toda la organización.

Asigna responsabilidades con respecto a la seguridad de la información.

Se asesora de un especialista en seguridad de la información.

Existe cooperación entre organizaciones.

Revisa independiente la seguridad de la información.

Seguridad del acceso por terceras partes:

Se debe mantener la seguridad de las instalaciones de procesamiento de la información organizacional y los activos de información a las que tienen acceso terceras partes.

Se deberá controlar el acceso de terceras partes a las instalaciones de procesamiento de la información organizacional.

Cuando el negocio requiera dicho acceso de terceras partes, se deberá realizar una evaluación del riesgo, para determinar sus implicaciones sobre la seguridad y definir las medidas de control que se requieren. Estas medidas de control deberán definirse y aceptarse en un contrato con la tercera parte.

El acceso de una tercera parte puede involucrar a otros participantes, los contratos que confieren acceso a una tercera parte, deberán incluir la posibilidad de designar a otros participantes y las condiciones para su acceso.

Identificación de riesgos por el acceso de terceras partes.

Tipos de acceso

Motivos de acceso

Subcontratados que trabajan en la Organización

Requisitos de seguridad en contratos con terceras partes.

Contratación externa (Outsourcing):

Se deberá mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información ha sido contratada externamente con otra organización.

Los acuerdos de contratación externa deberán incluir en el contrato entre las partes, los riesgos, controles y procedimientos de seguridad para sistemas de información, redes y terminales; Además aclarar los requisitos de seguridad en contratos con personas o entidades externas.

La Clasificación y el Control de los Activos

Mantener la protección adecuada de los activos organizacionales.

Se deberá adjudicar la responsabilidad de todos los activos de información importantes y asignar un propietario, la responsabilidad sobre los activos ayuda a asegurar que se mantiene la protección adecuada. Además deberán identificarse los propietarios para todos los activos importantes, y asignar la responsabilidad para el mantenimiento apropiado de los controles, la implementación de estos puede ser delegada, pero deberá mantenerse en el propietario designado del activo.

Inventario de activos

Clasificación de la información

Asegurar que los activos de información reciben el nivel de protección apropiado.

La información deberá clasificarse para indicar la necesidad, prioridades y grado de protección.

Ésta tiene grados variables de sensibilidad y criticidad, algunos elementos de información pueden requerir un nivel adicional de protección o una utilización especial.

Deberá utilizarse un sistema de clasificación de la información para definir un conjunto de niveles de protección adecuados, y comunicar la necesidad de medidas de utilización especial.

Guías de clasificación

La Seguridad del Personal

Reducir los riesgos de error humano, robo, fraude o uso inadecuado de las instalaciones.

Las responsabilidades de la seguridad se deberá tratar en la etapa de selección de personal, incluido en contratos, y supervisar durante el desarrollo del empleo.

Deberán realizarse estudios de seguridad adecuados a los funcionarios, sobre todo para tareas sensibles, todos los empleados deberán firmar una cláusula de confidencialidad.

Formación del usuario

Se debe crear conciencia sobre las amenazas y problemas de seguridad de la información, y la preparación en el apoyo a la política de seguridad de ésta, por parte del usuario.

Los usuarios deberán recibir formación en procedimientos de seguridad y en el uso correcto de los recursos de tratamiento de información, para minimizar los posibles riesgos en la seguridad.

Responder y minimizar el daño causado por incidentes y/o anomalías en materia de seguridad, hacer el seguimiento y aprender de estos incidentes. Igualmente, informar de los incidentes que

afecten la seguridad de la información por los canales de la Organización adecuados, en el menor tiempo posible.

La Seguridad Física

Tiene como objetivo evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones e información de la empresa.

Los recursos para el tratamiento de información crítica o sensible para la organización deberán ubicarse en áreas seguras, protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados, dando protección física contra accesos no autorizados, daños e interferencias.

Dicha protección tiene que ser proporcional a los riesgos identificados, se recomienda una política de puesto de trabajo despejado y bloqueo de pantalla para reducir el riesgo de accesos no autorizados o de daños a documentos, medios y las instalaciones de tratamiento de la información.

La seguridad de los equipos:

Tiene como objetivo evitar el daño, la pérdida o puesta en peligro de los activos e interrupción de las actividades de la organización.

El equipo deberá estar físicamente protegido de las amenazas y riesgos del entorno. La protección de los equipos (incluidos aquellos que están fuera de la oficina) es necesaria para reducir el riesgo del acceso no autorizado a datos y para asegurar protección contra pérdida o daño.

También se deberá considerar la ubicación y dada de baja de los equipos. Pueden requerirse medidas o controles especiales contra riesgos de accesos no autorizados y para proteger los sistemas de apoyo, como el suministro eléctrico y la infraestructura de cableado.

La Gestión de las comunicaciones y operaciones

Su objetivo es asegurar la operación correcta de las instalaciones de procesamiento de comunicaciones y operaciones.

Se implementará la separación de funciones cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

Planificación del sistema:

Minimizar el riesgo de fallas de los sistemas.

La planeación y la preparación avanzada se requieren para asegurar la disponibilidad de los recursos y capacidad adecuada.

Las proyecciones de requisitos en cuanto a la capacidad futura deberán hacerse para reducir el riesgo de una sobrecarga al sistema.

Los requisitos operacionales de los nuevos sistemas deberán ser establecidos, documentados y probados antes de su aceptación y uso.

Mantenimiento interno:

Se deberá mantener la disponibilidad e integridad de los servicios de comunicación y procesamiento de la información. Estableciendo procedimientos rutinarios para conseguir la estrategia acordada de respaldo, haciendo copias de seguridad, ensayando su recuperación oportuna, registrando eventos o fallos y monitoreando el entorno de los equipos, cuando sea necesario.

Administración de redes:

Asegurar la protección de la información de las redes y la protección de la infraestructura de soporte.

La administración de la seguridad de las redes que cruzan las fronteras de la organización requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas.

Seguridad y manejo de los medios:

Se deberán establecer los procedimientos operativos adecuados para proteger los documentos, soportes informáticos (discos, cintas, etc.), datos de entrada o salida.

Se protegerá el sistema de daño, robo y acceso no autorizado, evitando la pérdida de los activos y las interrupciones en la actividad de la organización.

Los medios deberán ser controlados y protegidos físicamente.

Intercambio de información y de software:

Evitar la pérdida, modificación o uso inadecuado de la información intercambiada entre organizaciones.

Se deberán controlar los intercambios de información y software entre organizaciones y además se cumplirá con toda la legislación correspondiente

Se deberán realizar los intercambios sobre la base de acuerdos formales, estableciendo procedimientos y normas para proteger los soportes en tránsito. Se considerarán las implicaciones de la seguridad asociadas al comercio, correo e intercambio electrónico de datos (EDI), así como los requisitos para las medidas y controles de seguridad.

El Control de los Accesos

Controlar el acceso a la información.

Para controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad y negocio, se deberán tener en cuenta las políticas de distribución de la información y de las autorizaciones.

Administración de acceso a los usuarios:

Evitar accesos no autorizados a los sistemas de información.

Se establecerán procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios.

Estos procedimientos deben cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas de información y servicios. Se debe prestar especial atención, donde sea apropiado, al control necesario de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema.

Responsabilidades de los usuarios:

Evitar el acceso de usuarios no autorizados. Una protección eficaz necesita la cooperación de los usuarios autorizados.

Los usuarios deberán ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y la seguridad del material puesto a su disposición.

Control de acceso a redes:

Protección de los servicios en red.

Deberá controlarse el acceso a los servicios en redes internas y externas, es necesario asegurarse de que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

Interfaces adecuadas entre la red de la organización y las redes públicas y/o las privadas de otras organizaciones.

Mecanismos adecuados de autenticación para los usuarios y los equipos.

Control de los accesos de los usuarios a los servicios de información.

Control de acceso al sistema operativo:

Evitar el acceso no autorizado a la información contenida en las plataformas o sistemas operacionales.

Control de acceso a las aplicaciones:

Evitar el acceso no autorizado a la información contenida en los sistemas de información.

Las utilidades de seguridad deberán ser dirigidas a restringir el acceso dentro de las aplicaciones del sistema.

Monitoreo de acceso y usos de los sistemas:

Detectar actividades no autorizadas.

Deberá efectuarse un monitoreo y control de los sistemas para detectar desviaciones de la política de control de accesos y registrar los eventos observables que proporcionen evidencias en caso de incidencias de seguridad.

El monitoreo y control del sistema permite comprobar la efectividad de los controles instalados y verificar la conformidad con un modelo de política de accesos

Computación móvil y trabajo remoto:

Garantizar la seguridad de la información cuando se usan dispositivos de computación móviles y trabajo remoto.

La protección requerida deberá ser proporcional y adecuada a los riesgos que causan estas formas específicas de trabajo, considerando los riesgos de trabajar en un entorno desprotegido cuando se usa computación móvil.

En el caso del trabajo remoto, la organización deberá implementar protección en este sitio y asegurar que existen los acuerdos adecuados para este tipo de trabajo.

El Desarrollo y el Mantenimiento de los Sistemas.

Garantizar que la seguridad está incorporada en los sistemas de información.

Esto incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios. El diseño y la implementación de los procesos de negocio que soportan las aplicaciones o el servicio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberán ser identificados y acordados antes de desarrollar los sistemas de información. Todos los requisitos de seguridad, incluida las disposiciones para contingencias, deberán ser identificados y justificados en la fase de requisitos de un proyecto, acordados y documentados como parte del proceso de negocio global para un sistema de información.

Seguridad de las aplicaciones del sistema:

Evitar la pérdida, modificación o uso inadecuado de datos de los usuarios en los sistemas de aplicación.

Se deberán diseñar, dentro de las aplicaciones, las medidas de control y las pistas de auditoría o los registros de actividad. Estos deberán incluir la validación de los datos de entrada, el procesamiento interno y los datos de salida.

Se pueden requerir medidas y controles adicionales en los sistemas que procesen o tengan impacto sobre activos sensibles, valiosos o críticos para la Organización. Dichas medidas se deberán determinar a partir de los requisitos de seguridad y la estimación del riesgo.

Controles criptográficos:

Proteger la confidencialidad, autenticidad o integridad de la información.

Se deberán usar sistemas y técnicas criptográficos para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

Seguridad de los archivos del sistema:

Asegurar que los proyectos de Tecnología de la Información y las actividades de soporte se lleven a cabo de una forma segura; El acceso a los archivos del sistema deberá ser controlado.

El mantenimiento de la integridad del sistema deberá ser responsabilidad del grupo de desarrollo o de la función del usuario a quien pertenezcan las aplicaciones del sistema o el software.

Seguridad en los procesos de desarrollo y soporte:

Mantener la seguridad del software y la información de la aplicación del sistema.

Controlar estrictamente los entornos del proyecto y de soporte.

Los directivos responsables de los sistemas de aplicaciones también lo deberán ser de la seguridad del entorno del proyecto o su soporte. Asegurando la revisión de todo cambio propuesto al sistema para comprobar que no debilita su seguridad o la del sistema operativo.

Gestión de la Continuidad del Negocio.

Contrarrestar las interrupciones a las actividades del negocio y proteger sus procesos críticos de los efectos de fallas o desastres de gran magnitud.

Implementando un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallos de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación.

Cumplimiento.

Evitar incumplimiento a cualquier ley civil o penal, obligaciones estatutarias, reglamentarias o contractuales de cualquier requisito de seguridad.

El diseño, la operación, el uso y la gestión de los sistemas de información pueden estar sujetos a obligaciones estatutarias, reglamentarias y contractuales de seguridad.

Se deberá buscar el asesoramiento sobre requisitos legales específicos de los asesores jurídicos de la organización, o de profesionales del derecho cualificados. Los requisitos legales varían de un país a otro, al igual que en el caso de las transmisiones internacionales de datos.

Consideraciones de la auditoría de sistemas:

Maximizar la eficacia del proceso de auditoría del sistema y minimizar la interferencia a éste. Estableciendo controles para proteger los sistemas operativos y las herramientas de auditoría durante las auditorías del sistema. También se requiere protección para preservar la integridad y evitar el uso inadecuado de las herramientas de auditoría.

4. Conclusiones.

En la actualidad, ante el avance de las tecnologías y las telecomunicaciones y después de realizado el correspondiente análisis de riesgos mediante el método Mossler, se determina que los principales riesgos que nos pueden afectar son: la filtración, el hurto o robo, la modificación o saboteo y la eliminación de la información y cobra especial importancia la protección de la misma, ya que ésta se considera el principal activo de cualquier organización.

El mejor sistema a implementar en la protección de la información en nuestra organización empresarial es el SGSI, Sistema de Gestión de Seguridad Informática.

Los principales elementos a garantizar en la seguridad de la información son: la confidencialidad, la integridad y la disponibilidad de información sensible para las operaciones de la compañía.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información, se utiliza el ciclo continuo PHVA, (Planear, Hacer, Verificar y Actuar), tradicional en los sistemas de gestión de la calidad.

Los principales elementos del Sistema de Gestión de la Seguridad de la Información son el manual de seguridad, los Procedimientos y los registros.

La norma más apropiada y que se adapta plenamente a las necesidades de mi organización es la ISO 27001.

Los principales objetivos que debemos controlar al interior de la compañía son:

Las políticas de seguridad, la seguridad organizacional, la clasificación y el control de los activos, la seguridad del personal, la seguridad física, la gestión de comunicaciones y operaciones, el control de los accesos, el desarrollo y el mantenimiento del sistema, la gestión de la continuidad del negocio y el cumplimiento.

El mayor beneficio que nos representa la implementación del SGSI 27001, es establecer unos parámetros para estructurar y garantizar que los riesgos de la seguridad de la información sean minimizados por nuestra empresa oportunamente.

5. Bibliografía.

Gómez, J. (2006) Seguridad en Sistemas Operativos Windows y Linux. Madrid. Ra – Ma.

Maiorano, A., Fernández D. (2009) Criptografía. Técnicas de Desarrollo para Profesionales. México, D.F. Alfaomega Grupo Editor, S.A. de C.V.

Carballar, J. (2006) Firewall. La Seguridad de la Banda Ancha. México, D.F. Alfaomega Grupo Editor. Ra – Ma.

Daltabuit, E. Hernández, L. Mallén G. Vásquez, J. (2007) La Seguridad de la Información. México, D. F. Limusa (Noriega Editores).