NORMA ISO 27000

• SISTEMAS DE GESTION DE SEGURIDAD INFORMATICA

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONOMICAS
ESCUELA DE CONTADURIA PÚBLICA

Cátedra : AUDITORIA DE SISTEMAS

Catedrático : ELSY GUADALUPE MONGE

Grupo Teórico No. : 04

Integrantes :

JAQUELYN GRACIELA ALARCON RAMIREZ	**AR04064**
ROLANDO ROBERTO AGUILAR MARROQUIN	**AM05060**
ANGEL MARCELO CANALES REYES	**CR05098**
NORA ALICIA RODRIGUEZ GUARDADO	**RG05066**
GABRIEL ENRIQUE RAMIREZ MENJIVAR	**RM05024**

Ciudad Universitaria, 23 de Septiembre de 2009

OBJETIVOS

GENERAL

Conocer la aplicabilidad de los controles establecidos y regulados bajo la ley sarbanes oxley, tanto en las empresas que cotizan en bolsa como en firmas que prestan servicios de auditoría y contabilidad en el salvador.

ESPECIFICO

- Indagar sobre la factibilidad de aplicación de la ley sarbanes oxley, en empresas listadas en bolsa y entidades nacionales de servicios de auditoría y contabilidad en el salvador.
- Determinar las ventajas y desventajas que repercuten en la aplicación de la ley sarbanes oxley.
- Diseñar un instrumento de consulta dirigido a profesionales en contaduría pública, sobre la factibilidad de aplicación de la ley sarbanes oxley a empresas en El Salvador.

RESUMEN EJECUTIVO.

La Serie ISO 27000 de normas se ha reservado expresamente por la norma ISO en materia de seguridad de la información. Esto, por supuesto, se alinea con una serie de otros temas, incluyendo la norma ISO 9000 (gestión de la calidad) e ISO 14000 (gestión medioambiental).

Al igual que con los temas arriba mencionados, la serie 27000 se rellenará con una serie de normas individuales y de los documentos.

Entre las principales normas referentes a la seguridad de la información tenemos:

ISO 27001. El objetivo de la propia norma es "proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información". En cuanto a su adopción, esto debe ser una decisión estratégica. Además, "El diseño y la implementación de un SGSI organización está influida por sus necesidades y objetivos, requisitos de seguridad, el proceso empleado y el tamaño y la estructura de la organización".

La norma define su "enfoque basado en procesos" como "La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos y su gestión".

Las secciones de contenido de la norma son:

- Responsabilidad de la Dirección
- Auditorías internas
- Mejora del SGSI
- Anexo A - los objetivos de control y los controles de
- Anexo B - Principios de la OCDE y de esta norma internacional
- Anexo C - Correspondencia entre ISO 9001, ISO 14001 y esta norma

ISO 27002. Es el cambio de nombre de la norma ISO 17799, y es un código de prácticas para la seguridad de la información. Básicamente describe cientos de posibles controles y mecanismos de control, que pueden ser aplicadas, en teoría, con sujeción a la orientación proporcionada en la norma ISO 27001.

La norma "establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información dentro de una organización". Los controles reales que figuran en la norma están destinados a atender las necesidades específicas identificadas a través de una evaluación de riesgo formal. La norma tiene también por objeto proporcionar una guía para el desarrollo de "normas de seguridad de la organización y prácticas de gestión eficaz de seguridad y para ayudar a construir la confianza en las actividades entre la organización".

La base de la norma fue originalmente un documento publicado por el gobierno del Reino Unido, que se convirtió en un estándar "adecuado" en 1995, cuando fue re-publicado por la BSI como BS 7799. En 2000 se volvió a re-publicar, esta vez por la ISO, como ISO 17799. Una nueva versión de este apareció en 2005, junto con una nueva publicación, la norma ISO 27001. Estos dos documentos están destinados a ser utilizados en conjunto.

Planes de futuro de la ISO para esta norma se centran en gran medida en torno al desarrollo y publicación de versiones específicas de la industria (por ejemplo: sector de la salud, la fabricación, y así sucesivamente).
Las secciones de contenido son:

- Estructura
- Evaluación del riesgo y tratamiento
- Política de Seguridad
- Organización de la Seguridad de la Información
- Gestión de Activos
- De Recursos Humanos de Seguridad
- Seguridad Física
- De Comunicaciones y Gestión de Operaciones
- Control de Acceso
- Sistemas de Información de Adquisición, desarrollo, mantenimiento
- Gestión de la información a Incidentes de Seguridad
- Continuidad del Negocio
- Conformidad

MARCO TEORICO

ISO 27000

Uno de los activos más valiosos que hoy en día posee las diferentes empresas, es ***la información*** y parece ser que con la globalización, ésta peligra ya que cada vez sufre grandes amenazas en cuanto a su confiabilidad y su resguardo, de igual forma la información es vital para el éxito y sobrevivencia de las empresas en cualquier mercado. Con todo esto todo parece indicar que uno de los principales objetivos de toda organización es el aseguramiento de dicha información, así como también de los sistemas que la procesan.

Para exista una adecuada gestión de la seguridad de la información dentro de las organizaciones, es necesario implantar un sistema que aborde esta tarea de una forma metódica y lógica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.
Para lograr estos objetivos, existen organizaciones o entes especializados en redactar estándares necesarios y especiales para el resguardo y seguridad de la información, estos estándares son llamado o reconocidos como ISO.

¿Qué son las normas ISO?

Las normas ISO surgen para armonizar la gran cantidad de normas sobre gestión de calidad y seguridad que estaban apareciendo en distintos países y organizaciones del mundo.

Los organismos de normalización de cada país producen normas que resultan del consenso entre representantes del estado y de la industria. De la misma manera las normas ISO surgen del consenso entre representantes de los distintos países integrados a la I.S.O.

Existen grandes familias de normas ISO:

Las de la familia 9000, las de la familia 14000 y las de la familia 27000 además de otras complementarias (ISO 8402; ISO 10011).

¿Quién elabora estas normas?

Existe la organización ISO, que significa **International Organization for Standardization** (Organización Internacional para la Estandarización), constituye una organización no gubernamental organizada como una Federación Mundial de Organismos Nacionales de Normalización, creada en 1947, con sede en Ginebra (Suiza). Reúne las entidades máximas de normalización de cada país, por ejemplo, BSI (British Standards Institute), DIN (Deutsches Institut für Normung), INN (Instituto Nacional de Normalización-Chile) etc.

FAMILIA DE ISO 27000

SERIE ISO 27000

La ISO 27000 es realmente una serie de estándares desarrollados, por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

Esta ISO Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

ESTANDAR DE SEGURIDAD ISO 27001

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION - REQUERIMIENTOS

Este estándar a sido preparado para proporcionar y promover un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar in Sistema de Gestión de Seguridad de Información. La adopción de este estándar diseño e implementación debe ser tomada en cuenta como una decisión

estratégica para la organización; se pretende que el SGSI se extienda con el tiempo en relación a las necesidades de la organización. El SGSI puede ser utilizado por entidades internas y externas para evaluar la conformidad.

ENFOQUE DEL PROCESO

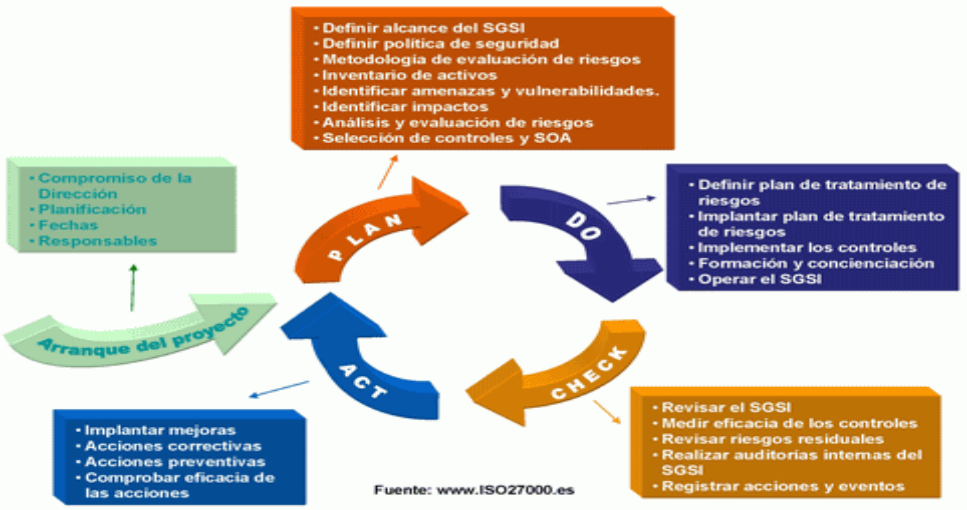
Las organizaciones necesitan identificar y manejar muchas actividades para poder funcionar de manera eficiente. Las actividades que necesitan recurso y es manejada para la transformación de insumos outputs es considerado como un proceso.

El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

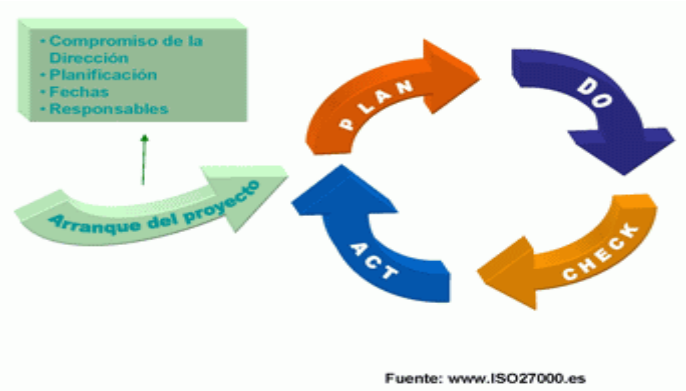
- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño del SGSI
- Mejoramiento continuo en base a la medición del objetivo

Este Estándar Internacional adopta el modelo del proceso (PDCA):

- Planear
- Hacer
- Chequear
- Actuar



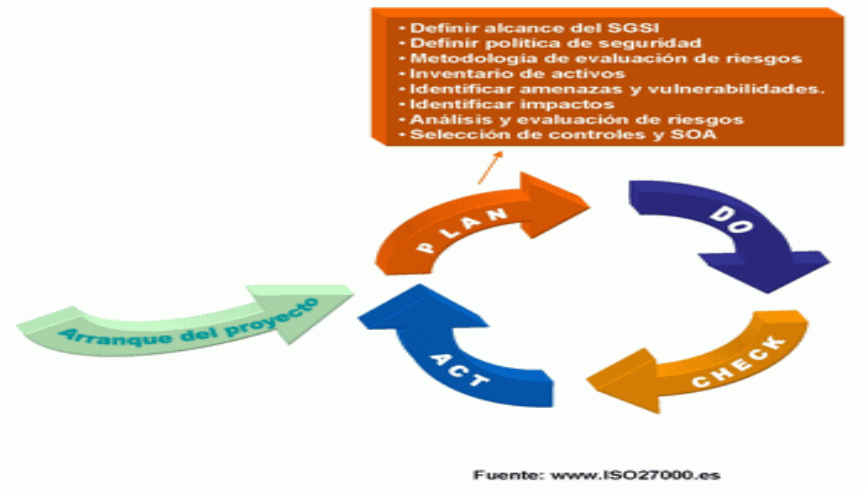
Arranque del proyecto



• Compromiso de la Dirección: una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.

• Planificación, fechas, responsables: como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

PLANIFICACION



• Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.

• Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.

• Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla (en el futuro, ISO 27005 proporcionará ayuda en este sentido). El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.

• Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

• Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.

• Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

• Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

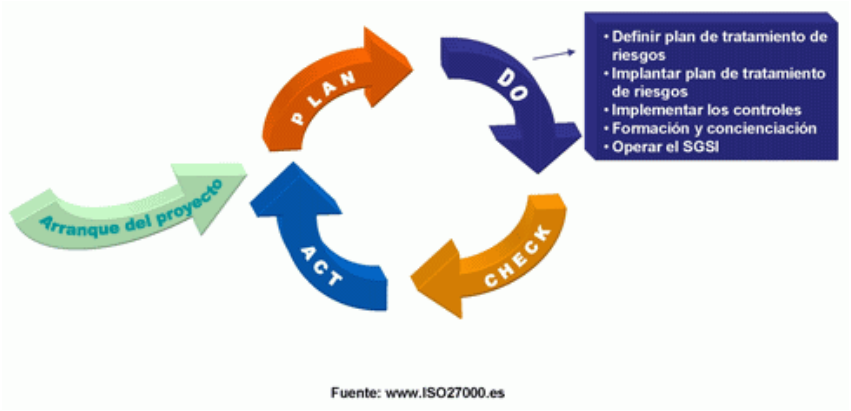
• Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).

• Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.

• Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

• Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

IMPLEMENTACION (HACER)



• Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

• Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.

• Implementar los controles: todos los que se seleccionaron en la fase anterior.

• Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.

• Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

• Gestionar las operaciones del SGSI y todos los recursos que se le asignen.

• Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

SEGUIMIENTO (CHEQUEAR)

• Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.

• Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.

• Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.

• Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

• Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

• Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

• Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.

• Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

MEJORA CONTINUA (ACTUAR)

• Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.

• Acciones correctivas: para solucionar no conformidades detectadas.

• Acciones preventivas: para prevenir potenciales no conformidades.

• Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.

• Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

ESTANDAR DE SEGURIDAD ISO 27002

CODIGO PARA LA PRÁCTICA DE LA GESTION DE SEGURIDAD DE LA INFORMACION

INTRODUCION AL ESTANDAR

¿Qué es seguridad de la información?

La información es un activo vital que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. En el curso de los años la globalización ha originado que la información fluya mas rápido de tal manera que para ello debe haber interconectividad entre las organizaciones a grandes distancias.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

¿Por qué se necesita seguridad de la información?

Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, el flujo de caja, rentabilidad, observancia legal e imagen comercial. Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; para evitar o reducir los riesgos relevantes.

¿Cómo establecer los requerimientos de seguridad?

Existen tres fuentes principales de requerimientos de seguridad,

- ✓ Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

- ✓ Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural.
- ✓ Otra fuente es el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

Punto de inicio de la seguridad de la información

El punto de inicio de la seguridad de información son los controles *considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación del país aplicable:*

a) protección de datos y privacidad de la información personal;

b) protección de los registros organizacionales;

c) derechos de propiedad intelectual.

Los controles considerados práctica común para la seguridad de la información incluyen:

a) documento de la política de seguridad de la información;

b) asignación de responsabilidades de la seguridad de la información;

c) conocimiento, educación y capacitación en seguridad de la información;

d) procesamiento correcto en las aplicaciones;

e) gestión de la vulnerabilidad técnica;

f) gestión de la continuidad comercial;

g) gestión de los incidentes y mejoras de la seguridad de la información

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios.

Tecnología de la información y Técnicas de seguridad

Código de práctica para la gestión de la seguridad de la información.

Alcance

Este Estándar establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Estructura del Estándar

Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

Cláusulas

Cada cláusula contiene un número de categorías de seguridad principales. Las once cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

a) Política de Seguridad

b) Organización de la Seguridad de la Información;

c) Gestión de Activos;

d) Seguridad de Recursos Humanos;

e) Seguridad Física y Ambiental;

f) Gestión de Comunicaciones y Operaciones;

g) Control de Acceso;

h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información;

i) Gestión de Incidentes de Seguridad de la Información;

j) Gestión de la Continuidad Comercial;

k) Conformidad.

Categorías de seguridad principales

Cada categoría de seguridad contiene:

a) un objetivo de control que establece lo que se debiera lograr; y

b) uno o más controles que se pueden aplicar para lograr el objetivo de control.

Evaluación y tratamiento del riesgo de Seguridad.

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deberan guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado.

Tratamiento de los Riesgos de Seguridad

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

a) aplicar los controles apropiados para reducir los riesgos;

b) aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;

c) evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;

d) transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Los controles deberán asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

a) los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales:

b) objetivos organizacionales;

c) requerimientos y restricciones operacionales;

d) costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;

e) la necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

CLAUSULAS DEL ESTANDAR Y SUS CATEGORIAS DE SEGURIDAD

C-01 POLITICAS DE SEGURIDAD.

La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.

Documento de la política de seguridad.

El documento que contenga la política de seguridad deberá ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.

Implantación de la política de seguridad

El documento de la política de seguridad de la información debiera enunciar el compromiso de la gerencia y establecer el enfoque de la organización para manejar la seguridad de la información. Deberá contener:

a) una definición de seguridad de la información, sus objetivos y alcance generales;

b) un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales;

c) un marco referencial para establecer los objetivos de control y los controles incluyendo la gestión de riesgo.

d) una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia, incluyendo:

1. conformidad con los requerimientos legislativos y reguladores.
2. educación, capacitación y conocimiento de seguridad,
3. gestión de la continuidad del negocio,
4. consecuencias de las violaciones de la política de seguridad de la información;

e) una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información,

f) referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar.

C-02 Organización de la política de seguridad.

La gerencia debiera aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización.

Compromiso de la gerencia con la seguridad de la información

La gerencia debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.

Lineamiento de implementación

La gerencia deberá:

a) asegurar que los objetivos de seguridad de la información estén identificados y cumplan con los requerimientos organizacionales.

b) formular, revisar y aprobar la política de seguridad de la información;

c) revisar la efectividad de la implementación de la política de seguridad de la información;

d) proporcionar una dirección clara y un apoyo gerencial visible para las iniciativas de seguridad;

e) proporcionar los recursos necesarios para la seguridad de la información;

f) aprobar la asignación de roles y responsabilidades específicas para la seguridad de la información a lo largo de toda la organización;

g) iniciar planes y programas para mantener la conciencia de seguridad de la información;

h) asegurar que la implementación de los controles de seguridad de la información sea coordinado en toda la organización.

La gerencia debiera identificar las necesidades de consultoría especializada interna o externa para la seguridad de la información, y revisar y coordinar los resultados de la consultoría a través de toda la organización.

Dependiendo del tamaño de la organización, estas responsabilidades podrían ser manejadas por un foro gerencial dedicado o por un organismo gerencial existente, como la junta de directores.

Típicamente, la coordinación de la seguridad de la información debiera involucrar la cooperación y colaboración de los gerentes, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo. Esta actividad debiera:

a) asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información;

b) identificar cómo manejar las no-conformidades;

c) aprobar las metodologías y procesos para la seguridad de la información;

d) identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas;

e) promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización;

Identificación de los riesgos relacionados con los grupos externos

Se debieran identificar los riesgos para la información y los medios de procesamiento de la información de la organización a raíz de procesos comerciales que involucran a grupos externos y se debieran implementar controles apropiados antes de otorgarles acceso.

Lineamiento de implementación

La identificación de los riesgos relacionados con el acceso del grupo externo toma en cuenta los siguientes puntos:

a) los medios de procesamiento de información a los cuales necesita tener acceso el grupo externo;

b) el tipo de acceso que tendrá el grupo externo a la información y los medios de procesamiento de la información; por ejemplo;

1) acceso físico; por ejemplo, oficinas, edificios de cómputo, archivadores;

2) acceso lógico; por ejemplo, a las bases de datos o sistemas de información de la organización;

3) conectividad de red entre las redes de la organización y el grupo externo; por ejemplo, conexión permanente, acceso remoto;

4) si el acceso se da fuera o dentro del local;

c) el valor y sensibilidad de la información involucrada, y su grado crítico para las operaciones comerciales;
d) los controles necesarios para proteger la información que no está destinada a ser accesible para los grupos externos;
e) el personal del grupo externo involucrado en el manejo de la información de la organización;
f) cómo se puede identificar a la organización y el personal autorizado que tiene acceso, cómo verificar la autorización, y con cuánta frecuencia se necesita reconfirmar esto;
g) los diferentes medios y controles empleados por el grupo externo cuando almacena, procesa, comunica, comparte e intercambia información;
h) el impacto del acceso no disponible para el grupo externo cuando lo requiere, y el grupo externo que ingresa o recibe información inexacta o confusa;
i) prácticas y procedimientos para lidiar con los incidentes en la seguridad de la información y los daños potenciales, y los términos y condiciones para la continuación del acceso del grupo externo en caso de un incidente en la seguridad de la información;
j) requerimientos legales y reguladores y otras obligaciones contractuales relevantes que se debieran tomar en cuenta para el grupo externo;
k) cómo los intereses de cualquier parte interesada pueden verse afectados por los arreglos.

C-03 Gestión de Activos

Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

Inventario de los activos

Control

Se debieran identificar todos los activos y se debiera elaborar y mantener un inventario de todos los activos importantes.

Lineamiento de implementación

Una organización debiera identificar todos los activos y documentar la importancia de estos activos. El inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial. El inventario no debiera duplicar innecesariamente otros inventarios, pero se debiera asegurar que el contenido esté alineado.

Propiedad de los activos

Control

Toda la información y los activos asociados con los medios de procesamiento de información debieran ser propiedad2 de una parte designada de la organización.

Lineamiento de implementación

El propietario del activo debiera ser responsable de:

a) asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente;

b) definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.

La propiedad puede ser asignada a:

a) un proceso comercial;

b) un conjunto de actividades definido;

c) una aplicación; o

d) un conjunto de data definido.

C-04 Seguridad de Recursos Humanos.

Esta clausula establece que se debe asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Los empleados, contratistas y terceros usuarios de los medios de procesamiento de la información debieran firmar un acuerdo sobre sus roles y responsabilidades con relación a la seguridad.

Roles y responsabilidades

Control

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

Lineamiento de implementación

Los roles y responsabilidades debieran incluir requerimientos para:

a) implementar y actuar en concordancia con las políticas de seguridad de la información de la organización (ver 5.1);

b) proteger los activos contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada;

c) ejecutar procesos o actividades de seguridad particulares;

d) asegurar que se asigne a la persona la responsabilidad por las acciones tomadas;

e) reportar eventos de seguridad o eventos potenciales u otros riesgos de seguridad para la organización.

Responsabilidades de la gerencia

Control

La gerencia debiera requerir a los usuarios empleados, contratistas y terceras personas que apliquen la seguridad en concordancia con políticas y procedimientos bien establecidos por la organización.

Conocimiento, educación y capacitación en seguridad de la información

Control

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

Lineamiento de implementación

La capacitación y el conocimiento debieran comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios.

La capacitación constante debiera incluir los requerimientos de seguridad, responsabilidades legales y controles comerciales, así como la capacitación en el uso correcto de los medios de procesamiento de información; por ejemplo, procedimiento de registro, uso de paquetes de software e información sobre los procesos disciplinarios.

C-05 Seguridad física y Ambiental

Se debe evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Perímetro de seguridad física

Control

Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

Control

Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos:

a) se debiera registrar la fecha y la hora de entrada y salida de los visitantes, y todos los visitantes debieran ser supervisados a no ser que su acceso haya sido previamente aprobado; sólo se les debiera permitir acceso por propósitos específicos y autorizados y se debieran emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia;

b) el acceso a áreas donde se procesa o almacena información sensible se debiera controlar y restringir sólo a personas autorizadas; se debieran utilizar controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos; se debiera mantener un rastro de auditoría de todos los accesos;

c) se debiera requerir que todos los usuarios empleados, contratistas y terceras personas y todos los visitantes usen alguna forma de identificación visible y se debiera notificar inmediatamente al personal de seguridad si se encuentra a un visitante no acompañado y cualquiera que no use una identificación visible;

d) al personal de servicio de apoyo de terceros se le debiera otorgar acceso restringido a las áreas seguras o los medios de procesamiento de información confidencial, solo cuando sea necesario; este acceso debiera ser autorizado y monitoreado;

e) los derechos de acceso a áreas seguras debieran ser revisados y actualizados regularmente, y revocados cuando sea necesario.

C-06 Gestión de Comunicaciones y Operaciones

Se debieran establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.

Procedimientos de operación documentados

Control

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

Gestión del cambio

Control

Se debieran controlar los cambios en los medios y sistemas de procesamiento de la información.

Separación de los medios de desarrollo, prueba y operación

Control

Los medios de desarrollo, prueba y operación debieran estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional.

Lineamiento de implementación

Se debiera identificar el nivel de separación necesario entre los ambientes de desarrollo, prueba y operación para evitar los problemas operacionales y se debieran implementar los controles apropiados.

C-O7 Control del acceso

Se debiera controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.

Las reglas de control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información.

Política de control del acceso

Control

Se debiera establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.

Lineamiento de implementación

Las reglas de control del acceso y los derechos para cada usuario o grupos de usuarios se debieran establecer claramente en la política de control de acceso. Los controles de acceso son tanto lógicos como físicos (ver también la sección 9) y estos debieran ser considerados juntos. Se debiera proporcionar a los usuarios y proveedores del servicio un enunciado claro de los requerimientos comerciales que debieran cumplir los controles de acceso.

La política debiera tomar en cuenta lo siguiente:

a) los requerimientos de seguridad de las aplicaciones comerciales individuales;
b) identificación de toda la información relacionada con las aplicaciones comerciales y los riesgos que enfrenta la información;
c) las políticas para la divulgación y autorización de la información;
d) los perfiles de acceso de usuario estándar para puestos de trabajo comunes en la organización;
h) segregación de roles del control del acceso;

Gestión de acceso del usuario

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

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta el des-registro final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debiera prestar atención especial a la

necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema.

Registro del usuario

Control

Debiera existir un procedimiento formal para el registro y des-registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información.

Control de acceso a la red

El objetivo primordial es evitar el acceso no autorizado a los servicios de la red.

Se debiera controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no debieran comprometer la seguridad de los servicios de la red asegurando:

a) que existan las interfases apropiadas entre la red de la organización y las redes de otras organizaciones, y redes públicas;

b) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;

c) el control del acceso del usuario a la información sea obligatorio.

C- 08 Adquisición, desarrollo y mantenimiento de los sistemas de información

Requerimientos de seguridad de los sistemas de información

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

Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones comerciales, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso comercial puede ser crucial para la seguridad. Se debieran identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

C-09 Gestión de un incidente en la seguridad de la información

Reporte de los eventos y debilidades de la seguridad de la información

Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

Se debieran establecer procedimientos formales de reporte y de la intensificación de un evento. Todos los usuarios empleados contratistas y terceros debieran estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales. Se les debiera requerir que reporten cualquier evento y debilidad de la seguridad de la información lo más rápidamente posible en el punto de contacto designado.

C-10 Gestión de la continuidad del negocio

Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Se debiera implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la organización y recuperarse de la pérdidas de activos de información (lo cual puede ser resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación. Este proceso debiera identificar los procesos comerciales críticos e integrar los requerimientos de gestión de la seguridad de la información de la continuidad del negocio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y medios.

Las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio debieran estar sujetas a un análisis del impacto comercial. Se debieran desarrollar e implementar planes para la continuidad del negocio para asegurar la reinundación oportuna de las operaciones esenciales. La seguridad de la información debiera ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización.

La gestión de la continuidad del negocio debiera incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debiera limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos comerciales.

C-11 Cumplimiento

Cumplimiento de los requerimientos legales

Objetivo: Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

Se debiera buscar la asesoría sobre los requerimientos legales específicos de los asesores legales de la organización o profesionales legales calificados adecuados. Los requerimientos legislativos varían de un país a otro y pueden variar para la información creada en un país que es transmitida a otro país (es decir, flujo de data inter-fronteras).

Identificación de la legislación aplicable

Control

Se debiera definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes, y el enfoque de la organización para satisfacer esos requerimientos, para cada sistema de información y la organización.

Lineamiento de implementación

Similarmente, se debieran definir y documentar los controles y responsabilidades individuales específicos para satisfacer estos requerimientos.

MARCO ANALITICO

ISO 27001 Un enfoque de procesos para la gestión de la seguridad de la información presentado en este Estándar Internacional facilita a los administradores tener una visión y control sobre:

- entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- implementar y operar controles para manejar los riesgos de la seguridad de la información.
- monitorear y revisar el desempeño y la efectividad del SGSI; y
- mejoramiento continúo en base a la medición del objetivo.

Entre otros beneficios de la ISO 27001 tenemos:

- La ISO 27001 es importante por que abarca a todos los tipos de organizaciones (comerciales, gubernamentales, organizaciones sin fines de lucro, etc.).
- Este estándar internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los proceso SGSI.
- Nos da lineamientos acerca la importancia del mejoramiento del SGSI atreves de el mejoramiento continuo, Acción correctiva, Acción Preventiva.
- también proporciona una guía importante de los objetivos de control y controles, enfocados a política de seguridad de información, organización interna, entidades externas, gestión de activos entre otras; así también nos dan los fundamentos en los cuales tiene como base este estándar los cuales se encuentran en los principios y como estos deberán ser de interpretados.

ISO 27002

Esta norma permite diseñar controles y evaluaciones de los riesgos a los que las entidades están expuestas desde diferentes puntos de vista como:

Entre las principales utilidades de esta norma tenemos:

Legislativo.

a) protección de data y privacidad de la información personal

b) protección de los registros organizacionales

c) derechos de propiedad intelectual

Los controles considerados práctica común para la seguridad de la información incluyen:

a) documento de la política de seguridad de la información

b) asignación de responsabilidades de la seguridad de la información

c) conocimiento, educación y capacitación en seguridad de la información

d) procesamiento correcto en las aplicaciones

e) gestión de la vulnerabilidad técnica

f) gestión de la continuidad comercial

g) gestión de los incidentes y mejoras de la seguridad de la información

- La ISO 27001 y 27002 establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.
- Sirve como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales.
- Los requerimientos identificados por una evaluación de los riesgos, serán la base para la elaboración de los objetivos de control.

CASO PRÁCTICO ISO 27001

La empresa "ABC, S. A. de C. V." Se dedica a la venta electrodomésticos en general, operando en toda la región Centroamericana, actualmente posee un sistema de información, dados ciertos eventos, en los que se involucran:

1. Pérdida de información
2. Filtro de información
3. Accesos no autorizados a la información
4. Modificación no autorizada de la información, entre otros

Decide adoptar un Sistema de Gestión de Seguridad de la Información en base a la norma ISO27001, por lo que desarrollan los siguientes procedimientos:

I. ESTABLECIMIENTO DEL SGSI

1. ALCANCE: Tras las reuniones realizadas por la administración, se determinó que en relación a la cobertura y amplitud del SGSI, éste comprenderá todas las áreas en las que se utiliza el sistema de información.
2. POLITICA DE SGSI
   - La política definida establece: que todos los procesos del sistema de información deberán realizarse en base a los lineamientos determinados por la administración, y deberán cumplirse todas las medidas de seguridad que se establezcan, esto debido al compromiso que se tiene con los clientes de proporcionar una atención adecuada.

3. IDENTIFICACIÓN DE RIESGOS

Dentro del marco de trabajo del SGSI, periódicamente (Cada seis meses, por ejemplo) se deberán identificar los riesgos que puedan afectar la seguridad del sistema, dentro de los que se incluyen: identificar amenazas, aspectos de vulnerabilidad, impacto de los riesgos.

4. ENFOQUE DE EVALUACIÓN DE RIESGOS

Para efectos de darle cumplimiento al SGSI, los riesgos se valorarán en relación a la probabilidad de ocurrencia y el impacto que puedan causar a la empresa.

5. IDENTIFICACIÓN Y EVALUACIÓN DE OPCIONES PARA EL TRATAMIENTO DE RIESGOS

El SGSI de esta empresa establece que la administración deberá buscar alternativas para el tratamiento de riesgos, las cuales pueden ser:

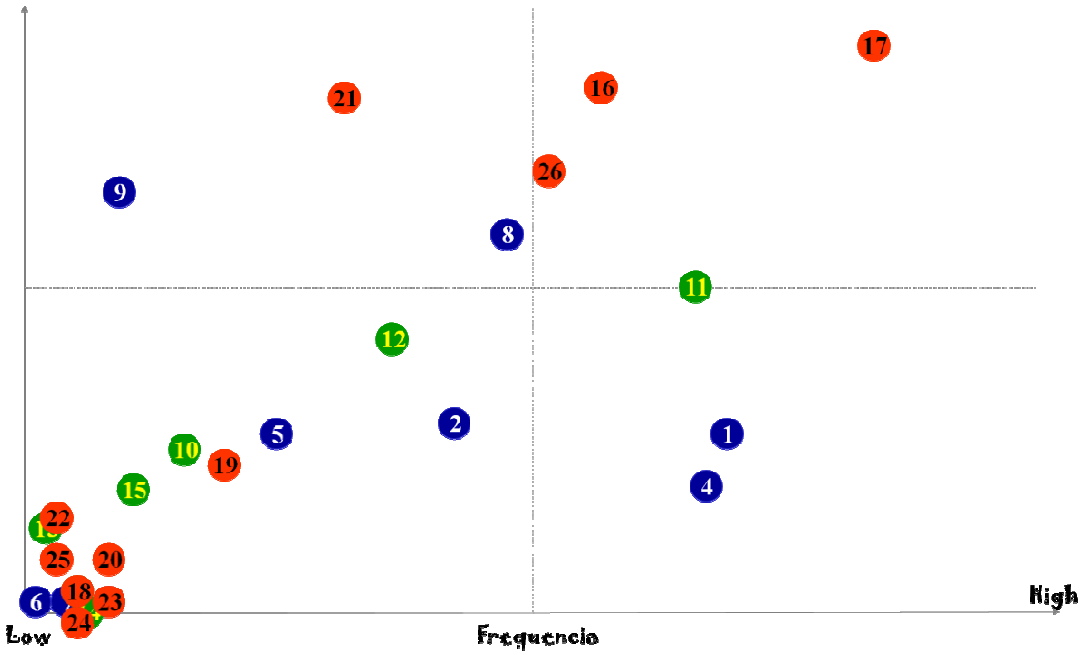
- Aplicación de controles adecuados
- Aceptar los riesgos
- Evitar los riesgos
- Transferir los riesgos

II. IMPLEMENTAR Y OPERAR EL SGSI

La empresa procede a la implementación del SGSI, no sin antes capacitar a todo el personal involucrado en la aplicación de dicho sistema, tras la aplicación del SGSI se identifican una serie de riesgos:

- Captura de PC desde el exterior
- Violación de e-mails
- Robo de información
- Violación de contraseñas
- Destrucción de equipamiento
- Virus
- Programas “bomba”
- Interrupción de los servicios
- Acceso clandestino a redes
- Acceso indebido a documentos impresos
- Intercepción de comunicaciones
- Falsificación de información para terceros

Por lo que se elaboró el correspondiente mapa de riesgos



Dadas las circunstancias la administración decide Aplicar una serie de controles que minimicen los riesgos identificados, y en el caso especial de aquellos riesgos que se relacionan con el daño de equipos, decide transferir el riesgo, por lo que contrata una póliza de seguros.

III. MONITOREAR Y REVISAR EL SGSI

Posterior a la implementación, la empresa realiza frecuentes actividades orientadas al monitoreo y revisión del funcionamiento del SGSI, dentro de los cuales se pueden mencionar:

- Detección de errores en los resultados de procesamiento
- Verificar que las actividades planeadas y toda la normativa emitida se están aplicando correctamente
- Aplicar indicadores para evaluar el desempeño del SGSI

En esta etapa se determina que el SGSI está funcionando correctamente y es efectivo en la seguridad de la información.

IV. MANTENER Y MEJORAR EL SGSI

Dado que los resultados del monitoreo determinan que el SGSI continúa siendo útil, deciden mantenerlo y darle seguimiento, bajo la condición de una constante actualización en relación a los cambios experimentados en la normativa y sobre todo en las condiciones de la organización.

GUIA DE EVALUACION

1. ¿Cuál es el objetivo de las serie ISO 27000?
2. ¿Para qué ha sido diseñado este estándar?
3. ¿En qué consiste el modelo PDCA adoptado por la norma?
4. ¿Qué es seguridad de la información?
5. ¿Por qué se necesita seguridad de la información?
6. ¿Cómo establecer los requerimientos de seguridad?
7. ¿Menciones algunos beneficios de la ISO 27001?
8. ¿Cuál es el enfoque del proceso de la ISO 27001?
9. Mencione algunos de los tratamientos de Políticas de seguridad relacionados con el SGSI
10. Mencione cuales son los lineamientos para la implementación de los SGSI