Universidad Israel

Seguridad de la Información

Tema: Introducción a las Seguridad de la Información

Docente: *Mg Renato Toasa*

Universidad Israel

Siempre se puede ser mejor.

Tiger Woods

Universidad Israel

Objetivo

Conocer la importancia de la seguridad de la información

Contenido

- Sistema de gestión de Seguridad de la información

Universidad Israel

Sistema de gestión de Seguridad de la información

Sistema de gestión de Seguridad de la información

SGSI

El modelo del SGSI integra la estrategia de la organización y está influenciada por factores tales como:

- » Necesidades y objetivos.
- » Requisitos de seguridad.
- » Procesos.
- » Estructura organizacional.

La norma ISO/IEC 27001 fue preparada para ofrecer un modelo para establecer, implementar, operar, monitorear, analizar críticamente, mantener y mejorar un SGSI.

Sistema de gestión de Seguridad de la información

SGSI

La adopción de un SGSI debe ser una decisión estratégica para la organización. La especificación y la implementación del SGSI de una organización están influenciadas por sus necesidades y objetivos, requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

Se espera que la implementación de un SGSI sea proporcional de acuerdo con las necesidades de la organización; por ejemplo, una situación simple requiere una solución de un SGSI sencillo.

Sistema de gestión de Seguridad de la información

Auditorías internas del SGSI

La organización debe realizar auditorías internas a intervalos planificados para determinar objetivos, controles, procesos y procedimientos del SGSI.

Una auditoría debe planificarse teniendo en cuenta el estado y la importancia de los procesos y las áreas a auditar, así como los resultados de las auditorías previas. Se deben definir los criterios de auditoría, su alcance, frecuencia y métodos.

Sistema de gestión de Seguridad de la información

Análisis crítico del SGSI

Como se ha visto anteriormente, el análisis crítico es esencial para el proceso de mejoramiento. La dirección debe analizar críticamente el SGSI a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia continua. Esta revisión debe incluir oportunidades de mejora y las necesidades de cambio del SGSI, incluyendo la política y objetivos de seguridad. Los resultados de esta revisión deben ser claramente documentados y los registros deben mantenerse.

Sistema de gestión de Seguridad de la información

Datos de entrada del análisis crítico:

Los resultados de las auditorías internas.

- Retroalimentación de las partes interesadas.
- Técnicas, productos o procedimientos que se pueden utilizar en la organización para mejorar el SGSI.
- Estado de las acciones correctivas y preventivas.
- Vulnerabilidades o amenazas no contempladas.
- Resultado de indicadores del SGSI.
- Acompañamiento de las acciones de las revisiones gestionadas.
- Recomendaciones para la mejora.
- Cualquier cambio que pueda afectar el SGSI.

Sistema de gestión de Seguridad de la información

Datos de salida del análisis crítico:

Son exactamente los que tienen por objetivo la búsqueda de la excelencia en el SGSI. Debe incluir todas las acciones y decisiones que se relacionan con:

- Mejora de la eficacia del SGSI.
- Actualización de análisis / evaluación y plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afectan a la seguridad
- La necesidad de recursos;
- Mejoras en el control de la eficacia del SGSI.

De esta manera se cierra un ciclo de vida del SGSI. Pero no debemos olvidar que el SGSI es un sistema de procesos continuos y formalizados, con el objetivo de proporcionar un procedimiento formal para la seguridad de la información de la organización con el fin de cumplir con sus objetivos de negocio.

Sistema de gestión de Seguridad de la información

Mejora del SGSI:

La organización debe mejorar continuamente la eficacia del SGSI mediante el uso de la política de seguridad de la información, los objetivos de seguridad, resultados de las auditorías, el análisis de los eventos monitoreados, acciones correctivas y preventivas y la revisión de la dirección.

- Acciones correctivas: la organización debe tomar acciones correctivas para eliminar las causas de las no conformidades con los requisitos del SGSI para evitar su repetición.
- Acciones preventivas: la organización debe determinar acciones para eliminar las causas de no conformidades potenciales con los requisitos del SGSI, para prevenir su ocurrencia.

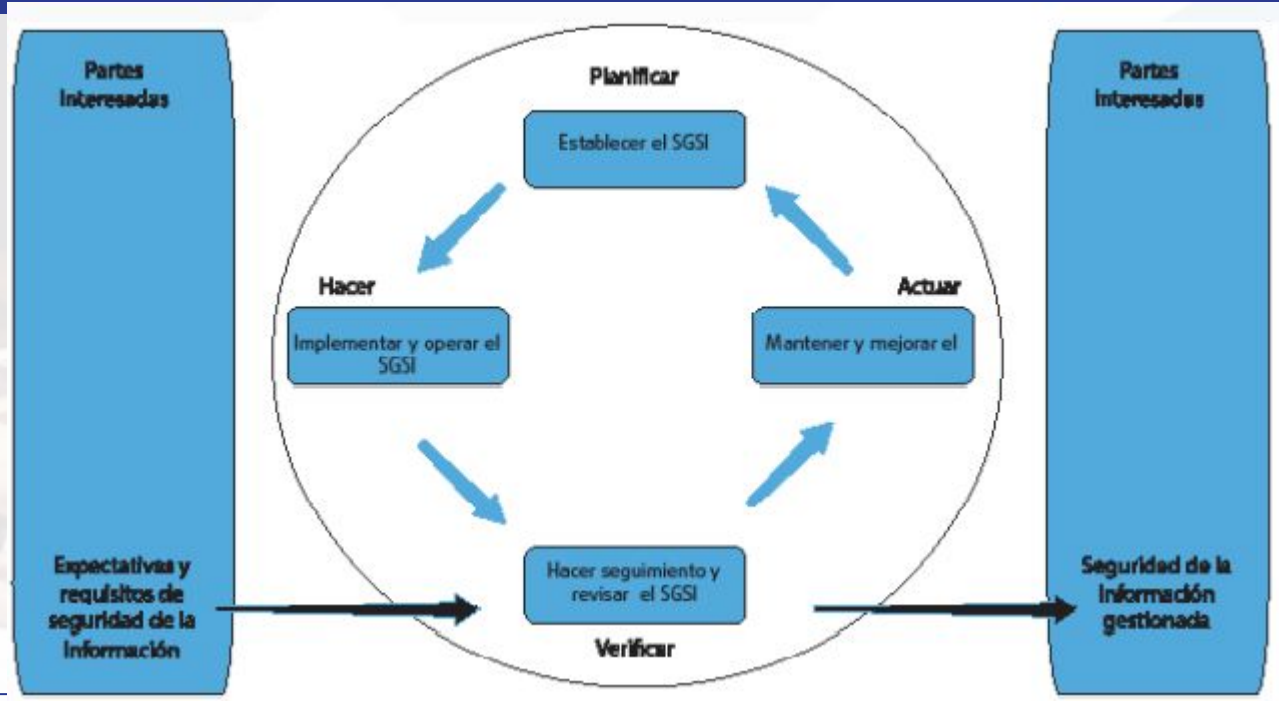
Universidad Israel

Modelo PHVA

Modelo PHVA

Introducción

La norma ISO 27001 adopta el modelo conocido como PHVA, que se aplica para estructurar todos los procesos del SGSI.



Modelo PHVA

Universidad Israel

Ecuador

El modelo PHVA comprende un conjunto de acciones en la secuencia establecida por las letras que componen las siglas: P (plan: planear), H (hacer, ejecutar), V (verificar, controlar) y, finalmente, A (actuar, actuar de manera correctiva):

- Planear (establecer el SGSI): establecer las políticas, objetivos, procesos y procedimientos del SGSI, relevantes para la gestión del riesgo y la mejora de la seguridad de información, para conseguir resultados de acuerdo con las políticas y objetivos generales de una organización.

Modelo PHVA

Ecuador

- Hacer (implementar y operar el SGSI): implementar y operar las políticas, controles, procesos y procedimientos del SGSI.
- Verificar (comprobar: monitorear y analizar críticamente el SGSI): evaluar y, si es el caso, medir el desempeño de un proceso con base en la política, los objetivos y la experiencia práctica del SGSI y presentar los resultados para la revisión de la dirección.
- Actuar (mantener y mejorar el SGSI): llevar a cabo las acciones correctivas y preventivas, basadas en los resultados de la auditoría interna del SGSI y el análisis crítico realizado por la dirección u otra información pertinente, para lograr la mejora continua del SGSI

Universidad Israel

Estableciendo y gerenciando el SGSI

Estableciendo y gerenciando el SGSI

Universidad Israel

SGSI

A continuación se presenta cada etapa en la gestión de un SGSI:

» Establecer el SGSI.

» Implementar y operar el SGSI.

» Monitorear y analizar críticamente el SGSI.

» Mantener y mejorar el SGSI.

Estableciendo y gerenciando el SGSI

Universidad Israel

Establecer el SGSI.

Los siguientes requisitos se deben cumplir dentro de cualquier organización, al iniciar un proceso de establecimiento de un SGSI:

- **Definir el alcance:** debe considerar las características del negocio, la organización, la ubicación, los activos y la tecnología;
- **Definir la política de seguridad:** además de obedecer al alcance, debe fijar objetivos y establecer la dirección general para las acciones relacionadas con la seguridad.
- **Definir la estrategia de evaluación de riesgos:** determinar la metodología y desarrollar criterios para la aceptación;

Estableciendo y gerenciando el SGSI

Universidad Israel

Establecer el SGSI.

- **Hacer la identificación, análisis y evaluación de riesgos:** identificar los activos, vulnerabilidades y amenazas.
- **Identificar y evaluar las opciones para el tratamiento de los riesgos:** implementar controles, aceptar, evitar, transferir el riesgo;
- **Seleccionar los controles y los objetivos para el tratamiento del riesgo:** seleccione los controles de la norma que han de aplicarse;
- **Obtener aprobación para los riesgos residuales;**
- **Obtener el consentimiento para la implementación del SGSI;**
- **Preparar la declaración de aplicabilidad:** debe relacionar los objetivos de control y los controles seleccionados, justificando obligatoriamente aquellos no seleccionados.

Estableciendo y gerenciando el SGSI

Universidad Israel

Implementación y operación del SGSI.

Cumplidos los requisitos necesarios para establecer el SGSI, se debe analizar, para el ambiente de la organización, la forma de cumplir los requisitos de implementación y operación:

- **Formular e implementar el tratamiento del riesgo:** como resultado del análisis de riesgos, la organización debe implementar un plan de tratamiento de riesgos eficiente;
- **Implementar los controles seleccionados:** a partir de los controles identificados como necesarios para el tratamiento de los riesgos de la organización deben implementarlos;
- **Definir parámetros para medir la eficacia de los controles:** desarrollar parámetros de medición, métricas e indicadores para evaluar la eficiencia y eficacia de los controles;

Estableciendo y gerenciando el SGSI

Universidad Israel

Implementación y operación del SGSI.

- **Implementar un programa de entrenamiento:** poseer y poner en práctica un programa de capacitación eficaz es esencial para el éxito;
- **Gestionar las operaciones del SGSI:** saber cómo está funcionando el SGSI y buscar áreas de mejora;
- **Gestionar los recursos para el SGSI:** comprobar si los recursos son suficientes;
- **Implementar controles capaces de detectar y responder a los incidentes de seguridad:** crear mecanismos de respuesta a cualquier incidente de seguridad de forma inmediata y planificada.

Estableciendo y gerenciando el SGSI

Universidad Israel

Monitoreo y análisis crítico del SGSI

Esenciales en cualquier sistema de gestión, las actividades de monitoreo y revisión son fundamentales para el éxito de un SGSI, al permitir el seguimiento, a través de evidencias, así como el proceso de mejoramiento continuo del sistema. Así tenemos, para esta fase, los siguientes requisitos:

- **Ejecutar los procedimientos de monitoreo y análisis crítico:** detectar los errores en el procesamiento, identificar inmediatamente las fallas, brechas de seguridad e incidentes, y controlar si se llevan a cabo las actividades delegadas como fue especificado, en caso de una falla de seguridad;

Estableciendo y gerenciando el SGSI

Universidad Israel

Monitoreo y análisis crítico del SGSI

- **Llevar a cabo revisiones periódicas de la eficacia del SGSI;**
- **Revisar el riesgo:** considerar los cambios relacionados con la organización, la tecnología, los objetivos y los procesos de negocio, las amenazas identificadas, eventos externos, tales como contratos, la legislación y el contexto social;
- **Actualizar el plan de seguridad;**
- **Mantenga registro de las acciones y eventos que han impactado sobre la eficacia o el rendimiento del SGSI.**

Estableciendo y gerenciando el SGSI

Universidad Israel

Mantenimiento y mejora del SGSI

Esta fase tiene como objetivo presentar los requisitos que la organización, de forma regular y estructurada, debe cumplir para que su SGSI se mantenga dentro del proceso de mejoramiento continuo del PHVA. Es interesante señalar la importancia de las acciones preventivas para este caso:

- Implementar las mejoras identificadas
- Ejecutar las acciones preventivas y correctivas: es necesario
- realizar acciones que puedan anticipar posibles ocurrencias;
- Comunicar las acciones y mejoras: Comunicar a todos los involucrados los cambios realizados en el SGSI;
- Asegurar que las mejoras alcancen sus objetivos

Universidad Israel

Requisitos generales de la documentación

Requisitos generales de la documentación

Mantenimiento y mejora del SGSI

La documentación dentro de un SGSI es un importante factor de éxito, dado que demuestra la relación de los resultados esperados con los controles implementados. La documentación será a menudo la evidencia necesaria para averiguar que un SGSI está implementado de manera Declaración de aplicabilidad:

Declaración de Privacidad: Es un documento formal que contiene los controles aplicados, los controles no aplicados, los controles no aplicables y los controles adicionales. Se trata de una lista de todos los controles de la norma indicando: los controles aplicados y el riesgo que se está tratando, los controles no aplicados y las justificaciones para su no aplicación, y los controles no aplicables en el ambiente de la organización con sus justificaciones.correcta y eficiente, permitiendo que las acciones puedan ser trazables y reproducibles.

Requisitos generales de la documentación

Mantenimiento y mejora del SGSI

Los documentos que se enumeran a continuación son los requisitos generales obligatorios y la base documental requerida para la auditoría de un SGSI:

- Declaración de la política de seguridad y los objetivos del SGSI;
- Alcance;
- Procedimientos y controles;
- Descripción de la metodología de análisis / evaluación de riesgos;
- Informe de análisis / evaluación de riesgos;
- Plan de tratamiento de riesgos;
- Procedimientos necesarios para garantizar la eficacia, la operación y los controles;
- Descripción de la medición de la eficacia de los controles;
- Registros requeridos.

Requisitos generales de la documentación

Control de documentos

- Aprobar la documentación.
- Revisar, actualizar y rechazar cuando sea necesario.
- Garantizar que los cambios y el estado de actualización estén identificados.
- Garantizar que los documentos pertinentes están disponibles en los puntos de uso en la versión más reciente.
- Garantizar que los documentos permanecen legibles y fácilmente identificables.
- Garantizar que los documentos de origen externo sean identificados.
- Garantizar que la distribución sea controlada.
- Aplicar la debida identificación en caso de que se retengan por cualquier razón.

Universidad Israel

Gracias

Responsabilidad con pensamiento positivo