pirani

Módulo 5

Pruebas, sensibilización y evaluación del Sistema de Gestión de Seguridad de la Información

CONTENIDO

1. Pruebas de seguridad de la información
2. Sensibilización y cultura del SGSI
1. Auditoría del SGSI
1. Actualización para la mejora continua
1. Impactos del Covid 19
1. Futuro de la seguridad de la información

1.

Pruebas de seguridad de la información

Pruebas y ejercicios

Las pruebas y ejercicios de seguridad permiten determinar cómo quedó **implementado** el sistema y qué se debe corregir para mejorar y evitar una infiltración. Las pruebas dicen si **el plan funciona** y permiten demostrar la madurez y robustez en seguridad de la información.

Qué debemos tener en cuenta:

- Hacer pruebas que generen valor agregado.
- Comenzar de lo particular a lo general.
- Hacer un adecuado plan de pruebas.
- Aprovechar las pruebas para probar el árbol de comunicación.
- Aplicar escenarios de pruebas cercanos a la realidad.
- Las pruebas no deben ser exitosas, deben tener oportunidades de mejora

2.

Sensibilización y cultura del SGSI

Sensibilizar es muy diferente a capacitar

La sensibilización es un proceso mediante el cual se genera **conciencia y cultura** en seguridad de la información, por lo que no debemos capacitar, debemos sensibilizar generando concientización y adaptación del personal.

Utilizar métodos **prácticos** y claros para sensibilizar sin desgastar al personal, y hacerlo de manera muy dinámica:

- **Videos**
- **Publicidad**
- **Obras de teatro**
- **Incentivos**
- **Cuestionarios**
- **Conferencias**
- **Retiros**

Conciencia en seguridad de la información

Para generar cultura y toma de conciencia es necesario hacer ver la importancia y los beneficios de la seguridad, así como dar incentivos y motivar a los funcionarios para que ayuden al funcionamiento del sistema.

- **Bonificaciones**
- **Semana de la seguridad**
- **Flexibilidad**
- **Días libres**
- **Incentivos**

Sensibilización y cultura

Sensibilización y cultura

Fase	Detalle
Plan de sensibilización y capacitación	- Identificar el público objetivo. - Definir los objetivos, alcance y premisas de desarrollo de la sesión de sensibilización o capacitación. - Definir el medio por el que se transmitirá el mensaje. - Definir el método adecuado para la ejecución de la sesión. - Desarrollar el material de apoyo que será presentado durante la sesión. - Garantizar la logística para el correcto desarrollo de la sesión.
Ejecución de sesiones de sensibilización y capacitación	- Desarrollo y ejecución de la sesión. - Ejecución de procedimientos y actividades planeadas. - Seguimiento de actividades y registro de participantes.
Evaluación de resultados	- Análisis de resultados. - Medición de resultados de las sesiones y cumplimiento del plan. - Acciones de mejoramiento a desarrollar en el próximo plan de capacitación.

3.
Auditoría del SGSI

Auditorías

Las auditorías internas o externas hacen parte del proceso de **mantenimiento y revisión de seguridad de la información**. Este proceso ayuda y asegura que se tenga un programa efectivo de seguridad de la información y tiene las siguientes funciones:

- Establecer la conformidad de los requerimientos de una organización con relación al SGSI y los requerimientos del estándar, modelo o metodología aplicada.
- Asegurar que el SGSI es efectivamente implementado y mantenido.

La auditoría debe ser ejecutada por **personal idóneo y competente** que sea designado formalmente por la organización para asegurar la aplicabilidad y eficacia del SGSI.

A partir de las evidencias recogidas luego de realizada la auditoría, debe hacerse seguimiento a los cambios o planes de acción resultantes mediante control de cambios y actualización.

4.

Actualización para la mejora continua

Actualizar para la mejora continua

La actualización debe ser **práctica** y con la ayuda de todo el personal. Cada uno debe tener sus tareas frente a la actualización con base en sus roles y responsabilidades.

Proceso de actualización

La actualización al sistema de gestión de seguridad de la información se debe realizar por lo menos una vez al año. En esta se deben considerar todos los aspectos y componentes, y posterior a la actualización se deben formalizar todos los cambios alrededor de toda la organización

La actualización debe ser dinámica y por el personal responsable y experto en el tema, siempre con el aval y conocimiento de la alta gerencia.

Los documentos de seguridad de la información deben ser prácticos y entendibles para quien los interpreta.

Mantenimiento y mejora del SGSI

Es la revisión periódica de **controles, procedimientos, políticas, protocolos, informes de pruebas y los planes de capacitación al personal.**

El SGSI deberá ser revisado como mínimo una vez al año por el comité de seguridad de la información para identificar cambios y mejoras al sistema producto de los resultados de las pruebas realizadas al mismo, cambios significativos en la operación de la organización y/o servicios involucrados en el alcance. Algunas de las posibles fuentes de cambio al SGSI pueden ser:

- Requerimientos legales.
- Nuevos servicios.
- Nuevo hardware, plataformas, aplicativos u otros cambios de tecnología.
- Cambio de instalaciones.
- Cambios en el personal o reubicación del mismo.
- Consolidación o tercerización de funciones.
- Cambios en el sistema de gestión de calidad y procesos.

5.
Impactos del COVID 19

Impactos del Covid 19 en la seguridad de la información

La pandemia que hoy se vive impacta los negocios porque se debe **pensar de forma diferente y adaptarse**, es decir, ser resilientes frente al panorama mundial.

Las organizaciones deben ir pensando en la virtualidad y los lineamientos para realizarlo de forma segura. El **teletrabajo** se convirtió en una estrategia principal y real que cada vez se irá afinando y consolidando.

El Covid ha cambiado nuestras vidas y la forma de los negocios, y **quien no se adapta simplemente desaparece.**

No solamente el Covid va a afectar las empresas, las emergencias sanitarias, ambientales, cambio climático, serán frentes de trabajo para adaptarse.

Por lo tanto **la seguridad de la información y la ciberseguridad serán pilares fundamentales para las organizaciones**, ya que los delincuentes cibernéticos se están aprovechando de la coyuntura actual.

6.

Futuro de la seguridad de la información

Futuro

Las empresas están buscando la nube por temas de practicidad, contractual, beneficios, operación, nivel de servicio, entre otros.

Cada vez la seguridad de la información estará más **integrada a los procesos y sistemas de las organizaciones,** de modo que se hable un solo idioma internacional.

La seguridad de la información siempre va a existir porque para todo lo que hagamos **necesitamos protegernos y siempre utilizaremos información** en diferentes medios y ubicaciones.

La seguridad de la información no es solo los eventos, fallas o situaciones, es el **día a día** y hace parte de la **operación normal** de la organización.

Bibliografía del curso

- Norma ISO 27000: 2012.
- Norma ISO 27001: 2013.
- Norma ISO 22301: 2019.
- Norma ISO 31000: 2018.
- Norma ISO 27032: 2012.
- Norma ISO 27035: 2013.

¡Gracias!

pirani | www.pirani.co/es