Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

CICLO REGULAR

MÓDULO II

CLASE 01

RIESGOS Y AMENAZAS DE LA SEGURIDAD DE LA INFORMACIÓN

Ing. Johnattan Sifuentes Rojas

MODULO II – RIESGOS Y AMENAZAS SEGURIDAD DE LA INFORMACIÓN

CONTENIDO MODULO II

1. Definiciones, Conceptos e Identificación de Riesgos y Amenazas.
2. Relación con ISO 31000:2018 e ISO/OEC 27005:2022
3. Planificación y Operación de los riesgos de la seguridad de la información
4. Identificación de activos de información
5. Análisis y evaluación de riesgos de seguridad de la información
6. Determinación de criterios de riesgo
7. Tratamiento del riesgo
8. Aceptación del riesgo
9. Relación entre riesgos, controles y objetivos del SGSI

DEFINICION CONCEPTO E IDENTIFICACIÓN RIESGO AMENAZA

DEFINICION CONCEPTO E IDENTIFICACIÓN RIESGO AMENAZA

Definición de Riesgo

Efecto de la incertidumbre sobre la consecución de objetivos (ISO/IEC 31000:2018)
Es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando perdidas o daños

Ejemplo: riesgo = “probabilidad de fuga de datos por mala gestión de contraseñas”; amenaza = “ataque de phishing”; vulnerabilidad = “usuarios sin MFA”.

DEFINICION CONCEPTO E IDENTIFICACIÓN RIESGO AMENAZA

Definición de Amenaza

Causa potencial de un incidente no deseado que puede ocasionar daño al sistema u organización (ISO/IEC 31000:2018)
Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

Tipos y Fuentes de Amenazas

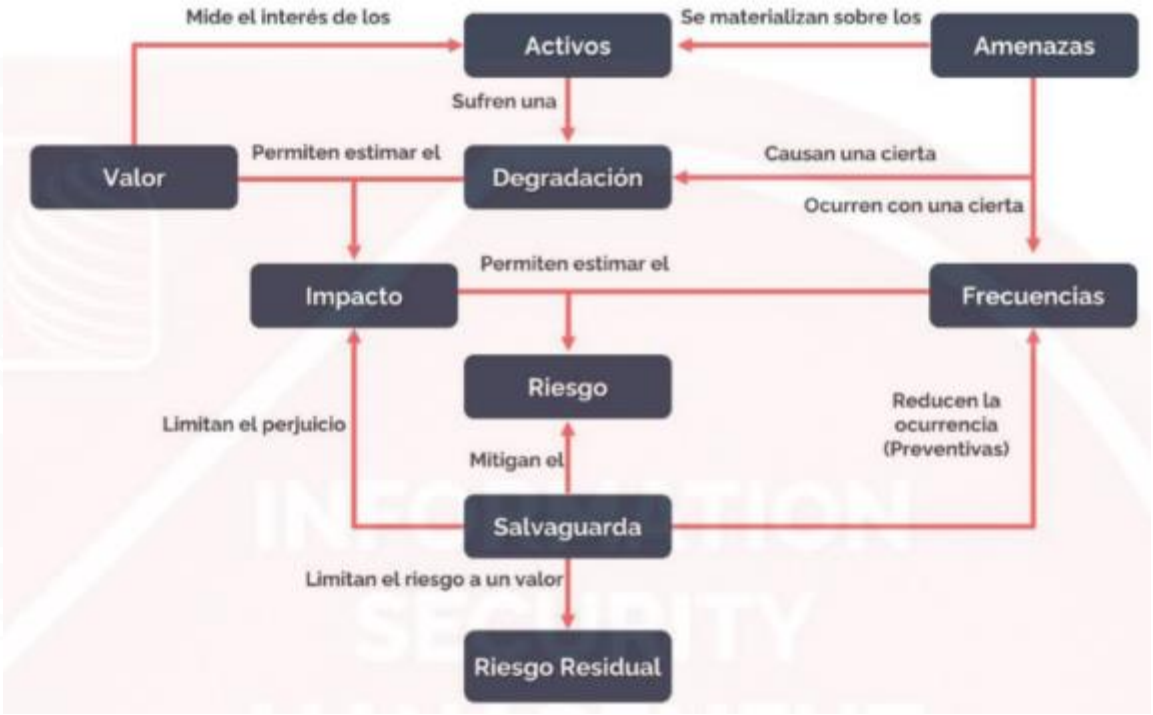
Algunas de las fuentes de amenazas mas comunes son:

- Malware o código malicioso
- Ingeniería Social
- APT o amenas persistentes
- Bootnets
- Redes sociales (reputación de empresas)
- Servicios de la nube.

DEFINICION CONCEPTO E IDENTIFICACIÓN RIESGO AMENAZA

Definición de Vulnerabilidad

Debilidad de un activo o de un control que puede ser explotada por una o mas amenazas.
Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un ataque pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.
Estos <<agujeros>> pueden tener distintos origines por ejemplo: fallos de diseño, errores de configuración o carencia de procedimientos.



DEFINICION CONCEPTO E IDENTIFICACIÓN RIESGO AMENAZA

Tipos de Daño

Daño Directo:
Robo

Daño Indirecto:
Una perdida en consecuencia a algo ocurrido.
. Ej.: Debido a un datacenter inundado no se puede proveer ningún servicio de TI causando perdida de ingresos para el negocio.

Expectativa de Pedida Anual (ALE)
Ale es una formula que multiplica el valor de un evento descrito de perdida **(expectativa de perdida individual o SLE)** por su **expectativa anual de ocurrencia (ARO)**, es decir, la pedida monetaria de un activo debido a la materialización de una o mas amenazas en un periodo de un año. Se define a través de la siguiente formula:

ALE = SLE X ARO

DEFINICION CONCEPTO E IDENTIFICACIÓN RIESGO AMENAZA

Otros Conceptos de Riesgos

Apreciación de Riesgo, proceso global de identificación de riesgos, análisis de riesgos y evaluación de riesgos.

Evaluación de Riesgos, proceso de comparación de los resultados del análisis de riesgos con los criterios de riesgos para determinar si el riesgos y/o su magnitud son aceptables o tolerables.

Aceptación del Riesgo, decisión informada de tomar un riesgos particular. La aceptación del riesgo puede ocurrir sin tratamiento de riesgo o durante el proceso del tratamiento de riesgo. Los riesgos aceptados están sujetos a monitoreo o revisión.

DEFINICION CONCEPTO E IDENTIFICACIÓN RIESGO AMENAZA

La Seguridad de la Información y la Gestión de Riesgos

Correspondencia entre la Seguridad de la Información y la Gestión de Riesgos

La ISO 27005 es una herramienta de gestión de riesgos que guía a una organización en la identificación de riesgos de seguridad de la información. Como tal, el propósito subyacente de un SGSI es:

- Identificar los riesgos estratégicamente importante, obvio y ocultos pero peligrosos.
- Asegurarse de que las actividades y los procesos operativos diarios de una organización estén diseñados, dirigidos y tengan recursos para gestionar inherentemente esos riesgos.
- Responder y se adaptarse automáticamente a los cambios para hacer frente a los nuevos riesgos y reducir continuamente la exposición a los mismos.
- Tener un plan de acción detallado que este alineado, actualizado y respaldado por revisiones y controles regulares es crucial y proporciona evidencia para el auditoria.

DEFINICION CONCEPTO E IDENTIFICACIÓN RIESGO AMENAZA

La Seguridad de la Información y la Gestión de Riesgos

En general, para determinar riesgos y oportunidades, debemos considerar:

- Garantizar alcanzar los objetivos planteados en la gestión de la seguridad de información (prevenir, reducir, mejora continua)
- Evaluar los riesgos en base a probabilidades reales, comparar resultados y priorizándolos.
- Seleccionar las opciones adecuadas para su tratamiento, apoyándonos en el uso de controles y estrategias.

- Todo ello en base a una planificación y adecuado control de cambio, sin adaptarse de los objetivos establecidos ni dejar de comunicar las acciones relacionadas a ello.

SOPORTE DE LA SEGURIDAD DE LA INFORMACION

SOPORTE DE LA SEGURIDAD DE LA INFORMACION

Recursos y Comunicación

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

La organización debe determinar la necesidad de comunicaciones internas y externas relevantes para el sistema de gestión de la seguridad de la información incluyendo:

- ✓ Sobre que comunicar;
- ✓ Cuando comunicar;
- ✓ Con quien comunicarse;
- ✓ Como comunicarse.

SOPORTE DE LA SEGURIDAD DE LA INFORMACION

Competencia

La organización deberá:

- Determinar la competencia necesaria de la(s) persona(s) que realiza(n) el trabajo bajo su control que afecta su desempeño en seguridad de la información.
- Garantizar que estas personas sean competentes sobre la base de una educación, formación o experiencia adecuadas.
- Cuando se aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas
- Conservar la información documentada apropiada como evidencia de competencia.

Nota: Las acciones aplicables pueden incluir, por ejemplo: la provisión de capacitaciones, tutorial o reasignación de empleados actuales; o la contratación o contratación de personas competentes

SOPORTE DE LA SEGURIDAD DE LA INFORMACION

Conciencia

Las personas que realicen trabajas bajo el control de las organización deben ser conscientes de:

- La política de Seguridad de la Información.
- Se contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios de un mejor desempeño de la seguridad de la información
- Las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información.

Documentar Información

El sistema de gestión de la seguridad de la información de la organización debe incluir:

- Información documentada requerida por este documento; e información documentada determinada por la organización.
- Llevar un control de cambio, actualizar, identificar y describir adecuadamente toda la documentación asociada.

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad