TEMA 3: Seguridad de la información

2. Análisis y gestión del riesgo en seguridad de la información

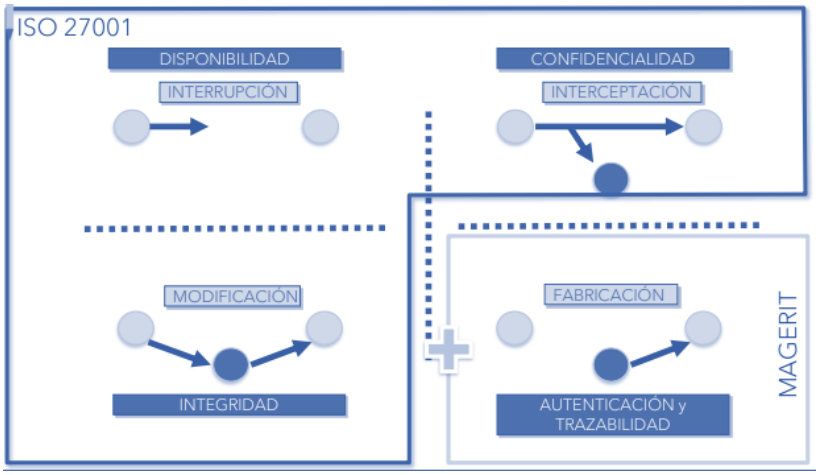
Seguridad de la información

El objetivo es establecer cuáles son los activos de la organización. Para cada uno de ellos, es necesario identificar sus diferentes dimensiones:

- **Su confidencialidad**: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- **Su integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcial-mente falsos o, incluso, faltar datos.
- **Su disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

Dimensiones de la seguridad de un activo

- **Confidencialidad**: Previene contra la divulgación no autorizada
- **Integridad**: Previene contra la modificación o destrucción no autorizada.
- **Disponibilidad**: Previene contra la denegación no autorizada de acceso a activos.

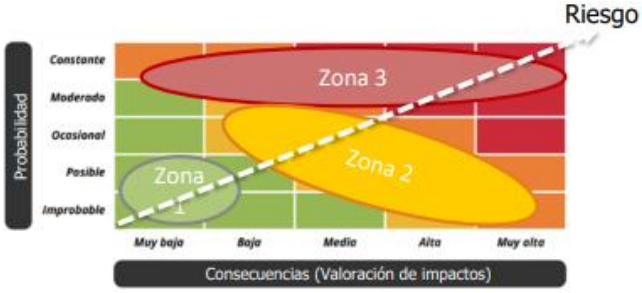


Conceptos básicos de seguridad

- **Activo**: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione y alcance los objetivos propuestos por su Dirección.
- **Amenaza**: Evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.
- **Vulnerabilidad**: Es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho Activo.
- **Riesgo**: Posibilidad de que una amenaza se materialice y produzca un impacto.
- **Impacto**: Consecuencia sobre un activo de la materialización de una amenaza.
- **Control**: Práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

Evaluación del riesgo

- Análisis de riesgo
  - El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo.
  - El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia.
  - Debe proporcionar el mapa de riesgos para poder valorar en su conjunto todos los riesgos identificados y permitir la toma de decisiones respecto a su gestión.
  - El propósito de la valoración del riesgo es apoyar a la toma de decisiones.
  - La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional.



- Valoración de riesgo

Esto puede conducir a una decisión de:

- no hacer nada más
- considerar opciones para el tratamiento del riesgo
- realizar un análisis adicional para comprender mejor el riesgo
- mantener los controles existentes
- reconsiderar los objetivos.

Estrategias

- **Disuasión**: Prevenir o reducir la probabilidad de intentar hacer daño.
- **Prevención**: Eliminar vulnerabilidades conocidas y prevenir que nuevas vulnerabilidades aparezcan.
- **Protección**: Resguardar los activos de información de las vulnerabilidades o de la exposición a amenazas adversas.
- **Detección**: Identificar la ocurrencia de un evento de seguridad con la mayor brevedad para iniciar la reacción proactiva, reactiva o de recuperación más adecuada
- **Reacción**: Responder o contrarrestar el incidente de seguridad para minimizar el daño y asegurar la continuidad de negocio.
- **Recuperación**: Reponer la integridad, confidencialidad o disponibilidad de los activos afectados por el incidente de seguridad

Tratamiento del riesgo

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo.

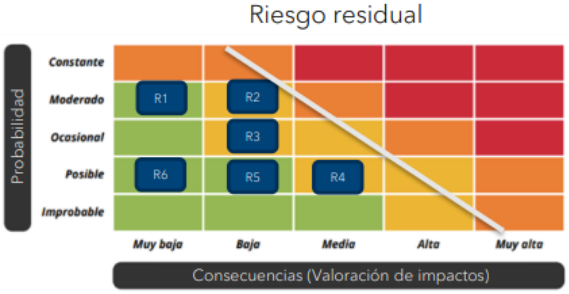
El tratamiento del riesgo implica un proceso iterativo de:

- formular y seleccionar opciones para el tratamiento del riesgo
- planificar e implementar el tratamiento del riesgo
- evaluar la eficacia de ese tratamiento
- decidir si el riesgo residual es aceptable
- si no es aceptable, efectuar tratamiento adicional

El plan de tratamiento de riesgos debe identificar un conjunto de actuaciones (proyectos) que permitan alcanzar los objetivos de reducción de riesgos planteados.

El plan debe especificar un conjunto de actuaciones, iniciativas o proyectos cuya misión es lograr alcanzar los niveles de riesgos establecidos como aceptables

Los resultados esperados de los proyectos y actuaciones a realizar deben poder proporcionar una visión del mapa de riesgos residual con el que la organización quedará conforme



PROYECTO A

- Lograr la reducción de los riesgos R3 y R1.

PROYECTO B

- Lograr la reducción de los riesgos R2 y R5.

Etc…

Registro e informe

El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados.

El registro e informe pretenden:

- comunicar las actividades de la gestión del riesgo y sus resultados a lo largo de la organización
- proporcionar información para la toma de decisiones
- mejorar las actividades de la gestión del riesgo
- asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

---------- 2ºPARCIAL ----------

3. Sistemas de gestión de la seguridad de la información (SGSI)

Fase Plan

- **Análisis de riesgos**

En la fase plan se define las cuestiones más importantes:

– Se determina la política de seguridad.

– Se concreta el alcance del sistema.

– Realizar el análisis de riesgos que es la actividad de diseño de seguridad que determina:

  - Identificar los activos de la organización dentro del alcance.
  - Identificar las amenazas, vulnerabilidades e impactos que podrían tener la perdida de confidencialidad, integridad y disponibilidad de los activos.
  - Estimar los niveles de riesgo.
  - Presentar los niveles de riesgo a la Dirección para determinar que riesgos son aceptables y cuales requieren un tratamiento.

- **Gestión de riesgos**

La gestión del riesgo implica la toma de decisiones respecto a aceptar, reducir, evitar o transferir cada uno de ellos.

– Según la decisión de la dirección respecto al umbral de riesgo aceptable, se debe determinar que riesgos son aceptables y cuales requieren un tratamiento.

– Identificar y valorar las opciones para el tratamiento.

– Seleccionar los objetivos de control y controles para el tratamiento del riesgo.

– Obtener la aprobación por parte de la Dirección de los riesgos residuales.

– Obtener la autorización por parte de la Dirección para llevar a cabo el plan de tratamiento de riesgos.

– Elaborar una Declaración de aplicabilidad.

Fase Do-Hacer

Define los pasos implantar el SGSI.

- Se ejecuta el plan de tratamiento de los riesgos, se implantan y aplican las medidas de seguridad seleccionadas.
- Se deben definir también los criterios de medición de objetivos y eficacia de los controles.
- Se realizan los programas de formación y capacitación a los empleados.
- Se establecen los procesos de detección de anomalías e incidentes y respuesta inmediata.

Fase Check-Revisar

Determina como controlar y medir el SGSI.

- Realizar las actividades de monitorización y revisión.
- Revisar el análisis de riesgos.
- Realizar las auditorías internas.
- Medir la eficacia de las contramedidas.
- Actualización de los planes de seguridad.
- Revisión por la Dirección del funcionamiento y eficacia del SGSI.

Fase Act-Reaccionar

Define como mejorar el SGSI.

- Emprender las acciones correctivas y preventivas pertinentes.
- Comunicar las acciones de mejora a las partes interesadas.
- Realizar el seguimiento de las acciones preventivas y correctivas para asegurar que las mejoras alcancen los objetivos establecidos