GESTIÓN DE RIESGOS

- La Gestión de Riesgos en la Seguridad Informática nos permite analizar y clasificar el riesgo para posteriormente implementar mecanismos que nos permitan controlarlo.

Riesgo de un incidente de seguridad

Riesgo de un incidente de seguridad

- El **riesgo** es una medida del daño probable que causará una amenaza, que aprovecha una vulnerabilidad para causar un daño.
- Es mayor cuanto más frecuente sea la aparición de la amenaza, y cuanto mayor sea el daño del incidente que acarree.
- Una aproximación cuantitativa sencilla es emplear la siguiente fórmula:

Riesgo = (probabilidad de ocurrencia de la amenaza) x (impacto o daño)

Riesgo de un incidente de seguridad

- Se puede **reducir el riesgo**, añadiendo las contramedidas que reduzcan las vulnerabilidades a las posibles amenazas.

- Cuantas más contramedidas se dispongan, es decir, cuantos más recursos se dediquen a la seguridad de los equipos informáticos, menor es el daño probable, o lo que es lo mismo, menor es el riesgo para el sistema de información.

Política de Seguridad

- Para una correcta gestión de la seguridad de la información, se deberá definir en un documento una “política de seguridad”.

- Esta política proporciona a la Dirección de la empresa las directrices y ayudas en materia de seguridad de la información, procedentes de requerimientos comerciales, requerimientos legales, nacionales e internacionales, de objetivos de la organización y de otras regulaciones aplicables

- Se parte de una empresa que provee alojamiento de páginas web, con un sistema de información valorado en 250.000 €. Un análisis de riesgos revela que hay dos amenazas:

- Un fallo del suministro eléctrico, caracterizado por:
  - Impacto o daño = 10.000 €
  - Probabilidad de ocurrencia de la amenaza= 0. 1
- Un ataque dirigido desde internet, caracterizado por:
  - Impacto o daño =500.000 €
  - Probabilidad de ocurrencia de la amenaza= 0.005
- El modelo de seguridad de la empresa tiene el criterio de **“optimizar la inversión concentrando los recursos en eliminar la mayor amenaza, y asumir el riesgo de las amenazas menores”**. Se pide que:

- Se cuantifique el riesgo de cada amenaza.
- Se calcule el presupuesto en seguridad que resultaría justificado invertir.
- Se calcule el riesgo que asume la empresa tras la inversión.

- CÁLCULO DE RIESGOS:

  Amenaza 1: riesgo = 10.000 x 0. 1 = 1.000 €.
  Amenaza 2: riesgo = 500.000 x 0.005 = 2.500 €.
  La amenaza 2, pese a ser veinte veces menos probable que la amenaza 1, es la de mayor riesgo a causa de su elevado impacto.

- PRESUPUESTO EN SEGURIDAD:

  El modelo de seguridad indica que, por criterio de la empresa, debe eliminarse la mayor amenaza, que es la que tiene un riesgo de 2.500 €. El presupuesto que se puede dedicar a combatir la amenaza es de 2.500 €.

- RIESGO TRAS LA INVERSIÓN:

  El modelo de seguridad indica que, por criterio de la empresa, se asume el riesgo del resto de amenazas, es decir el de amenaza 1. El riesgo asumido resultante es de 1.000 €.

¿Cómo gestionar el riesgo?

- **LA GESTIÓN DE RIESGOS** FORMA PARTE DE LA ESTRATEGIA DE ADMINISTRACIÓN DE UNA EMPRESA, Y NO SE LIMITA A LA SEGURIDAD DE LA INFORMACIÓN, SINO QUE PUEDE APLICARSE A LA GESTIÓN DE RIESGOS FINANCIEROS O DEL MERCADO.

1 - POLITICAS SALVAGUARDA

Persiguen detectar, prevenir, impedir, reducir, y controlar una amenaza y el daño que pueda generar. Son elementos de defensa, para que las amenazas no causen tanto daño. Como en el caso de las amenazas, las salvaguardas se pueden clasificar según distintas categorías.

- Por ejemplo, existirán:

  - **Salvaguardas preventivas o proactivas**, que persiguen anticiparse a la ocurrencia del incidente.
  - **Salvaguardas reactivas**, que persiguen reducir el daño una vez ocurre el incidente.
  - **Salvaguarda de "no hacer nada", o de aceptar el riesgo existente** para los equipos (cuando se cumplan los criterios de aceptación de riesgo de la empresa, y solo cuando esta decisión sea autorizada por la Dirección).

- Resumidamente, un **Modelo de Seguridad orientado a la gestión del riesgo,** emplea el cálculo del riesgo, y unos criterios empresariales (normativa, legislación, etc.), para poder decidir si es viable reducir el riesgo que se asume, o no.

- Para estudiar el riesgo, existen dos pasos claramente diferenciados:
- El **análisis de riesgos,** que consiste en identificar amenazas, determinar las vulnerabilidades, y medir el impacto o daño que causaría un incidente. Se pueden emplear métodos cuantitativos o cualitativos (valorando el riesgo en muy alto, alto, bajo, medio, etc.), para ordenar los riesgos.
- La **gestión de riesgos,** que partiendo de los resultados del análisis de riesgos, y una vez determinados los criterios para aceptar un riesgo (legales, económicos, etc.), permite elegir las contramedidas de seguridad que se implantarán

Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes

- Para determinar las amenazas, o encontrar nuevas, ayudará saber que pueden clasificarse como:

  - Amenazas naturales o artificiales.
  - Amenazas debidas al entorno (ambiente), o debidas al hombre.
  - Amenazas accidentales o intencionadas.

Desastres naturales

Amenaza	Riesgos usuales	Salvaguardas usuales
Incendios	Que el fuego acabe con recursos del sistema	Protección de las instalaciones frente a incendios
Inundaciones	Que el agua acabe con recursos del sistema	Protección de las instalaciones frente a inundaciones
Rayo, tormenta eléctrica	Destrucción de sistemas electrónicos	Protección de las instalaciones frente a descargas eléctricas

De origen industrial

Amenaza	Riesgos usuales	Salvaguardas usuales
Incendios	Que el fuego acabe con recursos del sistema	Protección de las instalaciones frente a incendios
Inundaciones, escapes	Que el agua acabe con recursos del sistema	Protección de las instalaciones frente a inundaciones
Otros desastres industriales: sobrecarga eléctrica, fluctuaciones eléctricas	Destrucción de sistemas electrónicos	Protección de las instalaciones frente a descargas eléctricas
Contaminación mecánica: vibraciones, polvo, suciedad	Destrucción de sistemas electromecánicos	Mantenimiento preventivo de limpieza, y reposición de componentes electromecánicos
Avería de origen físico o lógico: fallos en los equipos, fallos en los programas	Paradas de sistemas y/o pérdida de trazabilidad	Disponer de sistemas de funcionamiento redundante
Corte del suministro eléctrico	Paradas de sistemas	Sistemas de alimentación ininterrumpida
Condiciones inadecuadas de temperatura y humedad	Destrucción de componentes	Sistemas de aire acondicionado, y alarma por exceso de temperatura y humedad
Fallo de servicios de comunicaciones	Parada de sistema	Disponer rutas de comunicación redundantes
Degradación de los soportes de almacenamiento	Paradas de sistemas y/o pérdida de trazabilidad	Empleo de soportes redundantes, y realización de copias de seguridad

Errores y fallos no intencionados

Amenaza	Riesgos usuales	Salvaguardas usuales
Errores de los usuarios	Pérdida de información	Copias de seguridad, incluidos registros de transacciones para deshacer operaciones
Errores del administrador	Parada de sistema, ausencia de seguridad y trazabilidad	Disociación de responsabilidades, para reducir daño de los errores
Errores de configuración	Parada de sistema, ausencia de seguridad y trazabilidad	Procedimientos de reinstalación y configuración del sistema. Copias de seguridad
Deficiencias en la organización: cuando no está claro quién es responsable de hacer qué y cuándo	Paradas de sistemas, causadas por acciones descoordinadas u omisiones	Políticas de seguridad con establecimiento de responsables
Difusión de *software* dañino (virus, *spyware,* gusanos, troyanos, bombas lógicas, etc.)	Parada de sistema, ausencia de seguridad y trazabilidad	*Software* de eliminación de virus, y de eliminación de *software* malicioso. Procedimientos de reinstalación y configuración del sistema. Copias de seguridad.
Escapes de información: la información llega a quien no debe	Perdida completa de confidencialidad	Uso de técnicas de encriptación
Alteración de la información: alteración accidental de la información	Pérdida completa de integridad	Sistemas de revisión y validación de transacciones (mediante totales, revisión por otra persona u otras vías).
Vulnerabilidades de los programas (defectos en el código que producen errores)	Paradas del sistema y/o perdida de integridad	Entornos de prueba y sistemas de revisión
Errores de mantenimiento o actualización de programas *(software)*	Paradas del sistema	Plan de mantenimiento preventivo, para revisar fecha de actualización aplicada a las aplicaciones
Caída del sistema por agotamiento de recursos	Paradas del sistema	Aplicaciones de monitorización de recursos disponibles con alarmas

Indisponibilidad del personal: ausencia accidental del puesto de trabajo por enfermedad, alteraciones de orden público, guerra, etc.	Paradas del sistema	Política de seguridad con establecimiento de responsables, y designación de suplentes de responsables

Ataques intencionados

Amenaza	Riesgo	Salvaguarda
Manipulación de la configuración	Parada de sistema, ausencia de seguridad y trazabilidad	Copias impresas de procedimientos de reinstalación, y configuración del sistema
Suplantación de la identidad del usuario	Pérdida completa de confidencialidad e integridad	Sistemas de autenticación fuertes, que incluyan medidas biométricas
Uso no previsto: típicamente en interés personal, juegos, etc.	Paradas del sistema	Impedir ejecución de procesos no autorizados
Difusión de *software* dañino: virus, *spyware,* gusanos, troyanos, bombas lógicas, etc.	Parada de sistema, ausencia de seguridad y trazabilidad	*Software* de eliminación de virus y de eliminación de *software* malicioso. Procedimientos de reinstalación y configuración del sistema. Copias de seguridad.
Análisis de tráfico	Conocimiento de las pautas de actividad de la empresa	Aleatorización de las rutas de comunicaciones, y encapsulamiento de protocolos
Repudio	Pérdida de trazabilidad de las operaciones	Empleo de firmas digitales
Interceptación de información (escucha)	Pérdida de confidencialidad	Empleo de técnicas de criptografía
Destrucción de la información	Paradas de sistema	Copias de seguridad
Divulgación de la información	Pérdida de confidencialidad	Empleo de técnicas de criptografía

Denegación de servicio	Paradas de sistema	Penalización a solicitudes recurrentes. Monitorización de recursos disponibles y alarma
Robo de equipos o soportes	Paradas de sistema y perdida de confidencialidad	Alarmas antirrobo, sistemas de anclaje de equipos, técnicas de criptografía
Ataque destructivo (vandalismo, terrorismo, etc.)	Paradas de sistema	Copias de seguridad fuera de las instalaciones, acuerdos de alquiler de equipos para casos de emergencia, copias impresas de procedimientos de reinstalación y configuración del sistema
Ingeniería social	Parada de sistema, ausencia de seguridad y trazabilidad	Formación, empleo de mecanismos de autenticación fuertes con métodos biométricos

Salvaguardas y tecnologías de seguridad más habituales

- Las salvaguardas, o contramedidas, **persiguen detectar, prevenir, impedir, reducir, y controlar una amenaza y el daño que pueda generar.** Por ejemplo, existirán:
- Salvaguardas **preventivas o proactivas,** que persiguen anticiparse a la ocurrencia del incidente.
- Salvaguardas **reactivas,** que persiguen reducir el daño una vez ocurre el incidente.
- Salvaguarda de **"no hacer nada",** o de aceptar el riesgo existente para los equipos (cuando se cumplan los criterios de aceptación de riesgo de la empresa, y solo cuando esta decisión sea autorizada por la Dirección).

- **Seguridad de recursos humanos**
- **Seguridad ambiental**
- **Seguridad física**

Seguridad de acceso lógico (I)

- Definir una política de control de acceso, que identifique la información relacionada con actividades comerciales, los responsables de conceder-configurar-revocar los accesos, el procedimiento de solicitud, etc.
- Existencia de un registro de usuarios, y de los servicios a los que acceden. Nota: Es importante mantener un registro actualizado de los usuarios, de los servicios, y de los accesos autorizados de los usuarios a los servicios.
- Gestión de privilegios de acceso, sobre la base de “solo lo que necesitan saber”.
- Gestión de claves de usuario, tanto de las características técnicas o de complejidad, como de la prohibición de divulgación de las mismas.
- Revisiones periódicas de los derechos de acceso de los usuarios.

Seguridad de acceso lógico (II)

- El establecimiento de responsabilidades del usuario, en cuanto al uso de claves secretas, equipos desatendidos, políticas de “mesas” y pantallas “limpias” (que no muestren información que no sea de carácter público).
- La existencia de una política de uso de los servicios de red (internet, correo electrónico, etc.).
- Mecanismos de autenticación y registro para las conexiones externas a la empresa o remotas, como técnicas de redes privadas virtuales (VPN).
- Separaciones de redes, por ejemplo, en base a servicios de información, o grupos de usuarios o sistemas.
- Controles de las conexiones que realizan los usuarios hacia fuera de la empresa.

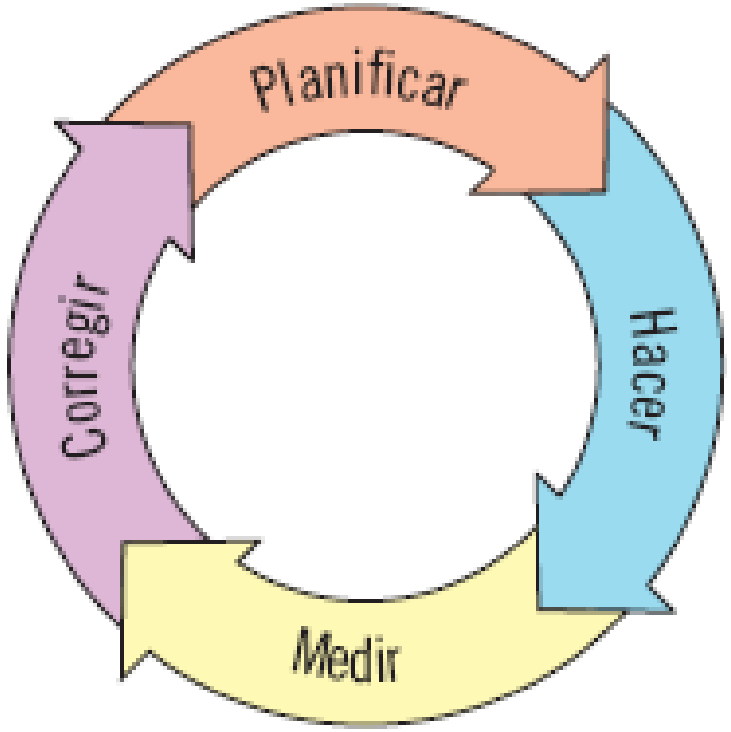
- Controles de acceso al sistema operativo, como la identificación y autenticación del usuario, un sistema automático de gestión de contraseñas, la restricción del uso de las utilidades del sistema operativo, el cierre de sesiones por inactividad, y la limitación de los periodos válidos para los inicios de sesión.
- Controles de acceso a las aplicaciones y la información, como controles de lectura, escritura, modificación de archivos, y carpetas; o el aislamiento de la información confidencial, por ejemplo, en sistemas con cifrado integrado.
- Establecimiento de una política para trabajo en movilidad, que incluya las comunicaciones móviles y el teletrabajo.

La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

- **Sistema de Gestión de Seguridad de la Información (SGSI),** como un sistema de gestión usado para establecer y mantener un entorno seguro.
- repetición continua de fases de planificación (en inglés, *plan)*, ejecución (en inglés, *do)*, medida (en inglés, *check)* y corrección (en inglés, *act)*, constituyendo un ciclo de mejora continua de *Deming* (P-D-C-A),

“el SGSI debe ser proporcional al valor de la continuidad del negocio”

Ciclo de mejora continua de Deming, aplicable al proceso de ejecución de un SGSI



- Las herramientas elementales para la correcta gestión de la seguridad informática, no son equipos de alta tecnología y costes inabordables. Las herramientas elementales son dos:
- La redacción de una política de seguridad de la información, que recoja de las directrices del SGSI a partir de las cuales derivarán todas las demás acciones.
- recomendaciones recogidas en **ISO 17799 y en la serie ISO 27000,** así como en la **RGPD ,** de manera proporcional a la empresa objetivo de aplicación.

- La serie ISO 27000 está formada por muchas normas, entre las que destacan:
- ISO 27000: términos y definiciones.
- ISO 27001: requisitos de un SGSI.
- ISO 27002: controles o salvaguardas (muy similar a la ISO 17799).
- ISO 27004: cómo medir la eficacia de un SGSI.
- ISO 27005: gestión de riesgos.
- ISO 27007: auditoria de un SGSI.
- ISO 27011: seguridad de la información para telecomunicaciones.

1. Análisis

-
- Tras realizar el BIA en el que mediante formularios y entrevistas a empleados clave conocíamos los recursos del sistema asociados a una actividad, ahora podemos pasar a identificar las vulnerabilidades que los debilitan y las amenazas que los pueden llegar a poner en peligro para así conocer su nivel de riesgo.

2. Clasificación

- Aquí pasamos a clasificar si los riesgos que hemos encontrado son aceptables para determinar si vamos a implementar alguna medida de protección contra ellos o si los podemos aceptar.
- Si los vamos a combatir o aceptar dependerá de la voluntad por parte de la organización y la viabilidad económica.
-

3.-Reducción

- En este paso definimos e implementamos las medidas de protección además de capacitar y concienciar a los usuarios conforme a las medidas .

Algunas de las medidas más comunes son:

- **Físicas**
- Controles de acceso como tarjetas inteligentes, lectores de huellas, vigilantes jurados, videocámaras, etc.
- Sistemas de anclajes de equipos, sistemas de alimentación ininterrumpida, sistemas de armarios fijos tipo rack, etc.

- **Técnicas**
- Antivirus, cifrado de datos, contraseñas complejas, copias de seguridad, etc.

- **Personales**
- Capacitación y sensibilización de los trabajadores.

- **Organizativas**
- Normas y reglas de utilización de ciertos recursos de la empresa, seguimiento de control, etc.

4. Control

- Por último y tras analizar el funcionamiento, la efectividad y el cumplimiento de las medidas adoptadas, pasamos a ajustar las que consideremos que son mejorables.
-

Finalidad

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables.