Seguridad en equipos informáticos

IFCT0109 – Seguridad informática

MF0486_3 (90 horas)

Docente:

José M. García Bravo

Criterios aceptados sobre seguridad en equipos informáticos

- Introducción
- Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
- Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
- Salvaguardas y tecnologías de seguridad más habituales
- La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas
- Resumen

Introducción

En el mundo actual, la seguridad de los equipos informáticos se ha convertido en un pilar fundamental para garantizar la protección de la información y la continuidad de las operaciones en las organizaciones.

Es crucial implementar medidas efectivas que salvaguarden los datos sensibles y prevengan posibles ataques cibernéticos.

En este documento, exploraremos criterios aceptados en seguridad informática que nos permitirán asegurar la integridad, confidencialidad y disponibilidad de la información en un entorno cada vez más digitalizado y conectado.

Seguridad orientada a la gestión del riesgo

En la era digital, la protección de los equipos informáticos es fundamental para salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Elementos de Seguridad Informática:

- Amenaza: Identificación de potenciales riesgos y ataques que pueden comprometer la seguridad de los equipos informáticos.
- Vulnerabilidad: Evaluación de las debilidades y puntos de entrada susceptibles a ser explotados por amenazas.
- Incidente de Seguridad: Manejo de situaciones adversas que afectan la integridad o disponibilidad de la información.

Seguridad orientada a la gestión del riesgo

Principios de Seguridad:

- Confidencialidad: Garantizar que la información solo sea accesible para aquellos autorizados.
- Integridad: Mantener la precisión y consistencia de los datos, evitando modificaciones no autorizadas.
- Disponibilidad: Asegurar que los recursos informáticos estén disponibles cuando se necesiten, sin interrupciones no planificadas.

Seguridad orientada a la gestión del riesgo

Metodología de Protección:

- Evaluación de Riesgos: Identificación y análisis de posibles amenazas y vulnerabilidades para determinar el nivel de riesgo asociado.

- Implementación de Controles: Desarrollo e implementación de medidas de seguridad para mitigar los riesgos identificados.

- Monitoreo y Mejora Continua: Supervisión constante del entorno de seguridad y ajustes según sea necesario para mantener la eficacia de las medidas de protección.

Seguridad orientada a la gestión del riesgo

Definiciones de Seguridad de la Información:

- ISO/IEC 27001:2017: Preservación de confidencialidad, integridad y disponibilidad de la información.

- Metodología MAGERIT v3: Capacidad de resistir acciones que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos y servicios.

Seguridad orientada a la gestión del riesgo

Amenazas, vulnerabilidades e incidentes de seguridad

- **Amenazas:** Posibles acciones que podrían dañar los equipos informáticos (ejemplos: incendio, robo, borrado de información).
  - No se pueden eliminar, pero se pueden analizar para reducir su impacto.
  - Obligación de identificar y comprender las amenazas para proteger los equipos.

- **Vulnerabilidades:** Debilidades en los equipos que permiten que las amenazas los afecten.
- **Incidente de Seguridad:** Ocurre cuando una amenaza explota una vulnerabilidad, resultando en daño al equipo.
- **Contramedidas:** Medidas para prevenir, reducir y controlar el impacto de los incidentes de seguridad.
  - Enfoque en la identificación y aplicación de contramedidas efectivas para mitigar riesgos.

Seguridad orientada a la gestión del riesgo

Amenazas, vulnerabilidades e incidentes de seguridad

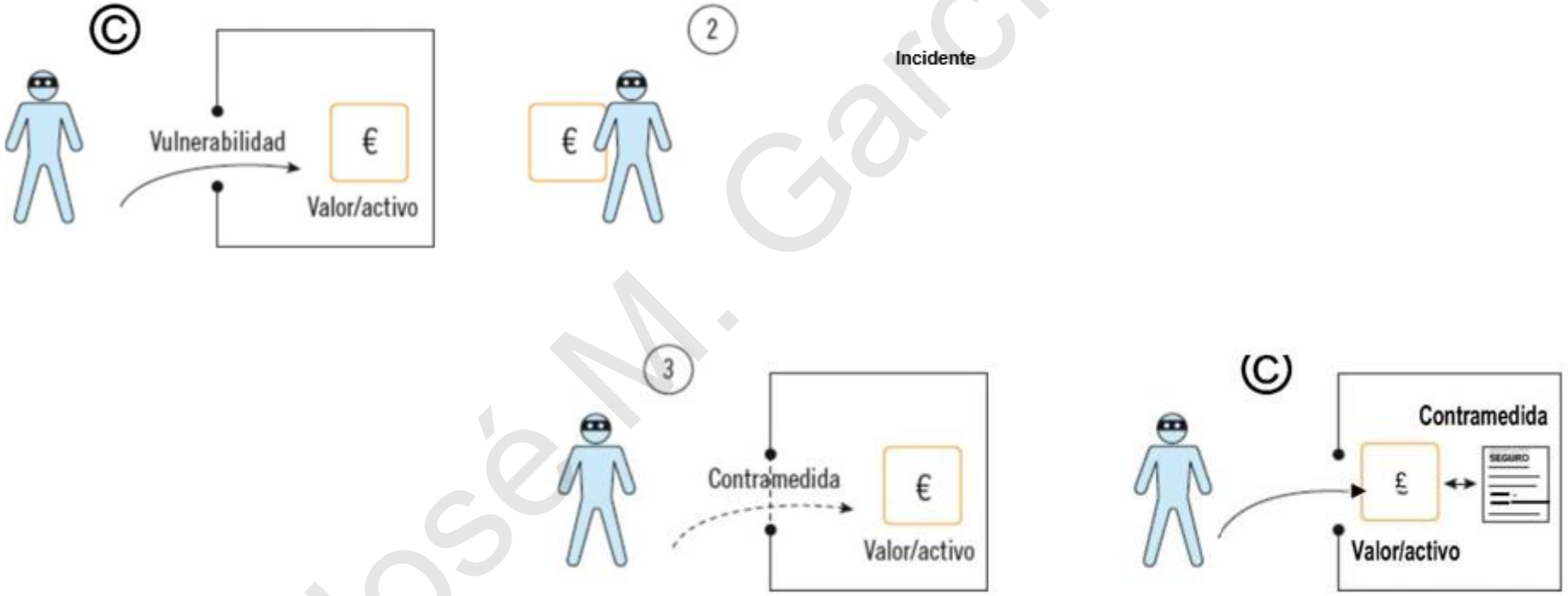
Estrategia de seguridad y enfoque preventivo

- Estrategia: Reconocimiento del inevitable riesgo de incidentes de seguridad.
- Prioridad en la reducción de la frecuencia y el daño potencial de los incidentes.
- Enfoque en maximizar la relación beneficio/coste al implementar contramedidas.
- Análisis constante de opciones efectivas para fortalecer la seguridad y minimizar riesgos.

Seguridad orientada a la gestión del riesgo

Amenazas, vulnerabilidades e incidentes de seguridad

Representación gráfica de los conceptos de amenaza y vulnerabilidad (1) de un objeto valioso para la empresa o activo. El incidente de seguridad (2) es la suma de la existencia de la amenaza y de la vulnerabilidad. Las posibles contramedidas incluyen dificultar la ocurrencia del incidente (3), reduciendo su probabilidad, o reducir el daño, reembolsando parte del importe robado (4)



Seguridad orientada a la gestión del riesgo

Principios de seguridad

Limitaciones de la Seguridad Informática

- A pesar de los esfuerzos por aplicar contramedidas, siempre persiste alguna vulnerabilidad que puede ser explotada.
- La seguridad absoluta es una meta inalcanzable en el ámbito de la informática y los sistemas de información.
- La comprensión de estas limitaciones es crucial para una gestión adecuada del riesgo y la seguridad de la información.

Seguridad orientada a la gestión del riesgo

Principios de seguridad

Principios de Seguridad de la Información

- La norma **ISO 27001:2017** establece tres principios esenciales para la seguridad de la información: **confidencialidad, integridad y disponibilidad**.
- Confidencialidad: Garantiza que la información solo esté accesible para quienes estén autorizados.
- Integridad: Asegura la exactitud y completitud de la información, evitando modificaciones no autorizadas.
- Disponibilidad: Garantiza que la información esté accesible cuando sea necesario para los usuarios autorizados.
- Estos principios, a menudo referidos como la "Triada de la Seguridad" o "CIA", proporcionan una base sólida para la implementación efectiva de medidas de seguridad informática.

Seguridad orientada a la gestión del riesgo

Principios de seguridad

Principios de Seguridad de la Información

La información es segura o fiable cuando hay confidencialidad, integridad y disponibilidad

Seguridad orientada a la gestión del riesgo

Principios de seguridad

Dimensiones de la seguridad de la información según Magerit V3

- Las propiedades principales de la seguridad de la información son tres (**Confidencialidad, Integridad y Disponibilidad**)
- MAGERIT v3 las denomina **dimensiones** fundamentales de la seguridad de la información.

- Además de estas dimensiones principales, se pueden añadir otras derivadas para mejorar la percepción de los usuarios de los sistemas de información:
  - Autenticidad: Garantiza la veracidad de la entidad que accede a los datos, especialmente importante para evitar la suplantación de identidad.
  - Trazabilidad: Permite determinar quién realizó qué acción y cuándo, esencial para analizar incidentes, rastrear atacantes y aprender de la experiencia.

Seguridad orientada a la gestión del riesgo

Riesgo de un incidente de seguridad

Gestión del Riesgo en Seguridad de la Información

- El riesgo es la medida del daño probable causado por una amenaza que explota una vulnerabilidad.
- Se puede calcular el riesgo mediante la fórmula:

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

- La reducción del riesgo se logra mediante la implementación de contramedidas que disminuyan las vulnerabilidades.

Seguridad orientada a la gestión del riesgo

Riesgo de un incidente de seguridad

Modelo de Seguridad y Política de Seguridad

- La gestión del riesgo en seguridad de la información requiere un enfoque metódico.
- Un modelo de seguridad organiza los procesos de gestión de seguridad según directrices empresariales y métodos para calcular los riesgos.
- Es fundamental establecer una política de seguridad que proporcione directrices y ayudas basadas en requisitos comerciales, legales y objetivos organizacionales.

Seguridad orientada a la gestión del riesgo

Riesgo de un incidente de seguridad

Análisis de Riesgos en Seguridad de la Información

- El análisis de riesgos es el primer paso para gestionar la seguridad de la información.
- Consiste en identificar amenazas, determinar vulnerabilidades y medir el impacto potencial de un incidente.
- Se pueden emplear métodos cuantitativos o cualitativos para evaluar y ordenar los riesgos.

Seguridad orientada a la gestión del riesgo

Riesgo de un incidente de seguridad

Gestión de Riesgos en Seguridad de la Información

- La gestión de riesgos permite elegir las contramedidas de seguridad en base a los resultados del análisis de riesgos.
- Se definen criterios para aceptar un riesgo (legales, económicos, etc.) y se seleccionan las contramedidas apropiadas.
- El análisis y gestión de riesgos son fundamentales para proteger una empresa y asegurar una actividad futura efectiva y controlada.

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

Identificación de Amenazas en la Gestión de Riesgos

- En la fase inicial de la gestión de riesgos, es importante centrarse en las principales amenazas a las que está expuesto un sistema de información.
- El conocimiento detallado de la empresa, incluyendo su estructura organizativa, procesos productivos, ubicación geográfica y competencia, es fundamental para identificar estas amenazas.
- Las amenazas pueden clasificarse según su origen: naturales o artificiales, debidas al entorno o al ser humano, accidentales o intencionadas.
- A continuación, se presenta un conjunto de amenazas frecuentes extraídas del catálogo de amenazas de MAGERIT, que aunque no es exhaustivo, cubre la mayoría de situaciones generales y algunos de los riesgos principales junto con las salvaguardas usuales.

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

De origen industrial

Amenaza	Riesgos usuales	Salvaguardas usuales
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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

De origen industrial

Amenaza	Riesgos usuales	Salvaguardas usuales
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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

Errores y fallos no intencionados

Amenaza	Riesgos usuales	Salvaguardas usuales
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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

Errores y fallos no intencionados

Amenaza	Riesgos usuales	Salvaguardas usuales
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, guera, etc, …	Paradas del sistema	Política de seguridad con establecimiento de responsables y designación de suplentes de responsables.

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

Ataques intencionados

Amenaza	Riesgos usuales	Salvaguardas usuales
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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

Ataques intencionados

Amenaza	Riesgos usuales	Salvaguardas usuales
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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

Ataques intencionados

Amenaza	Riesgos usuales	Salvaguardas usuales
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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

Ataques intencionados

Amenaza	Riesgos usuales	Salvaguardas usuales
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 segundad 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

Seguridad orientada a la gestión del riesgo

Amenazas más frecuentes, riesgos que implican y salvaguardas habituales

Qué es la criptografía

La criptografía es el estudio y la práctica de técnicas para asegurar la comunicación de manera segura, protegiendo la confidencialidad, integridad y autenticidad de la información. Se utiliza para cifrar y descifrar datos, garantizando que solo los destinatarios autorizados puedan acceder a ellos.

Ejemplo práctico: Cuando enviamos un mensaje privado por correo electrónico, podemos utilizar criptografía para proteger su contenido. Al cifrar el mensaje con una clave única, solo el destinatario, que posee la clave para descifrarlo, puede leer el mensaje original. De esta manera, se asegura que el mensaje permanezca confidencial durante su transmisión.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

Salvaguardas en la Seguridad de la Información

- Las salvaguardas, también conocidas como contramedidas, son elementos de defensa para detectar, prevenir, reducir y controlar amenazas y el daño que puedan generar.
- Se clasifican en:
  - Preventivas o proactivas: Para anticiparse a la ocurrencia del incidente.
  - Reactivas: Para reducir el daño una vez ocurrido el incidente.
  - "No hacer nada": Aceptar el riesgo existente cuando se cumplan los criterios de aceptación de riesgo de la empresa.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

1.- Seguridad de Recursos Humanos en la Gestión de Información

Proteger la información durante el ciclo laboral es crucial, desde la contratación hasta la terminación del empleo. Salvaguardas habituales incluyen:

- Definición de roles y responsabilidades.
- Investigación de antecedentes.
- Formación en seguridad de la información.
- Procesos disciplinarios.
- Definición de responsabilidades al finalizar el contrato.
- Devolución de activos.
- Retiro de derechos de acceso a la información.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

2.- Seguridad Ambiental en Equipos Informáticos

- Es fundamental proporcionar un entorno adecuado para los equipos informáticos, como servidores empresariales, para minimizar riesgos.
- Se deben considerar medidas como suministro eléctrico ininterrumpido, temperatura controlada (20°-25°), y ubicación en un Centro de Proceso de Datos (CPD) separado.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

Salvaguardas en Seguridad Ambiental

Para proteger contra amenazas como desastres naturales o industriales, se pueden implementar diversas medidas:

- Sistemas anti-incendio y anti-inundaciones.
- Fijación en armarios industriales o rack para evitar vibraciones y golpes.
- Aire acondicionado y alarmas de temperatura y humedad.
- Respaldo de suministro eléctrico y seguridad de cableado.
- Mantenimiento preventivo y seguridad en desplazamientos del equipo.
- Además, es importante asegurar una destrucción segura al final del ciclo de vida del equipo.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

3.- Seguridad Física en Acceso a Equipos Informáticos

- El acceso físico a los equipos informáticos aumenta el riesgo de incidentes y debe limitarse a quienes lo necesiten para sus funciones, en horarios y condiciones específicas.
- Los usuarios, desarrolladores de aplicaciones, administradores de bases de datos y la Dirección de la empresa no deben tener acceso físico a servidores o equipos de comunicaciones, a menos que sea estrictamente necesario.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

Salvaguardas en Seguridad Física

Para proteger contra posibles ataques con acceso físico, se pueden implementar las siguientes medidas:

- Establecer un perímetro de seguridad física con elementos constructivos adecuados.
- Utilizar mecanismos de control de ingreso físico, como acreditaciones y cerraduras automáticas.
- Definir áreas específicas de acceso público, entrega y carga.
- Proteger contra actividades cercanas que puedan representar riesgos, como incendios, explosiones o movimiento de vehículos.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

4.- Seguridad de Acceso Lógico

Acceso lógico: Acceso remoto a la información sin necesidad de periféricos directamente conectados al equipo.

Implicaciones: Requiere una red de comunicaciones para extender el acceso al servidor más allá del CPD.

Medidas de seguridad:

- Política de control de acceso: Define quién puede acceder a qué información y quién gestiona esos accesos.
- Registro de usuarios y servicios: Mantener un registro actualizado de usuarios y sus accesos autorizados.
- Gestión de privilegios: Limitar el acceso a lo esencial basado en el principio de "solo lo que necesitan saber".

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

4.- Seguridad de Acceso Lógico

Medidas de seguridad:

- Gestión de claves de usuario: Asegurar la complejidad de las claves y prohibir su divulgación.
- Revisiones periódicas de derechos de acceso: Garantizar que los usuarios solo tengan acceso necesario.
- Responsabilidades del usuario: Establecer normativas sobre el uso adecuado de claves y equipos.
- Política de uso de servicios de red: Definir el uso adecuado de servicios como internet o correo electrónico.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

4.- Seguridad de Acceso Lógico

Medidas de seguridad:

- Mecanismos de autenticación y registro para conexiones externas: Utilizar tecnologías como VPN para conexiones seguras.
- Separaciones de redes: Dividir la red en base a servicios de información o grupos de usuarios.
- Controles de acceso al sistema operativo y aplicaciones: Restringir el acceso a funciones y datos sensibles.
- Política para trabajo en movilidad: Establecer reglas para el uso seguro de dispositivos móviles y acceso remoto.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

4.- Seguridad de Acceso Lógico

Medidas de seguridad:

- Mecanismos de autenticación y registro para conexiones externas: Utilizar tecnologías como VPN para conexiones seguras.
- Separaciones de redes: Dividir la red en base a servicios de información o grupos de usuarios.
- Controles de acceso al sistema operativo y aplicaciones: Restringir el acceso a funciones y datos sensibles.
- Política para trabajo en movilidad: Establecer reglas para el uso seguro de dispositivos móviles y acceso remoto.

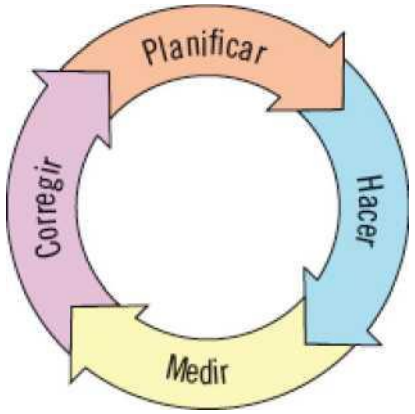
Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

5.- Gestión de la Seguridad Informática

- No es suficiente implementar medidas de seguridad tecnológicas aisladas.
- Necesidad de una gestión adecuada que incluya procesos, revisiones y adaptaciones.
- Surge el concepto de Sistema de Gestión de Seguridad de la Información (SGSI) para establecer y mantener un entorno seguro.
- El ciclo de mejora continua de Deming (P-D-C-A) se aplica al proceso de ejecución de un SGSI.

Se analizan o planifican las necesidades de segundad de la empresa, estableciendo las medidas de protección necesarias para alcanzarlas; se implantan las medidas, se mide el resultado de satisfacción de las necesidades de seguridad, se determinan las correcciones que hay que realizar en las medidas de protección, y se vuelve a comenzar (revisando las necesidades y las medidas que permitirían alcanzar esas necesidades, incluyendo las correcciones detectadas en la ejecución anterior).



Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

5.- Gestión de la Seguridad Informática

- El proceso del SGSI incluye fases de planificación, ejecución, medición y corrección.
- Objetivo: Asegurar la continuidad del negocio, minimizar riesgos y maximizar el retorno de la inversión.
- Las PYMEs pueden enfrentar dificultades para implementar un SGSI completo debido a su complejidad.
- Se propone aplicar el principio de proporcionalidad: las medidas deben adecuarse a los objetivos y al riesgo. Ejemplo de aplicación del principio de proporcionalidad: control de acceso a estaciones de trabajo.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

5.- Gestión de la Seguridad Informática

- El SGSI debe ser proporcional al valor de la continuidad del negocio. La inversión en seguridad debe estar alineada con los objetivos y riesgos de la organización.
- Herramientas esenciales para la gestión de la seguridad informática: política de seguridad de la información y metodología de evaluación de riesgos.
- Ambas herramientas permiten planificar, medir y mejorar la seguridad de la información de manera continua.
- La ejecución de las medidas y correcciones debe adecuarse a la proporcionalidad de la política de seguridad.
- Es factible aplicar una metodología adaptable a los recursos disponibles en una PYME para lograr una mejora continua en la seguridad de la información.
- La implantación de un SGSI demasiado exhaustivo puede ser inviable y conducir a una ejecución lenta.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

6.- Resumen

- Los equipos informáticos son esenciales para las empresas debido al valor de la información y las consecuencias de las acciones.
- Las amenazas comprometen la actividad de los equipos debido a las vulnerabilidades.
- El riesgo se puede reducir disminuyendo el daño probable o la probabilidad de ocurrencia de las amenazas.
- El daño se evalúa en términos de confidencialidad, integridad y disponibilidad de la información.
- Se emplea un modelo de gestión de la seguridad de la información basado en el riesgo.
- Las herramientas fundamentales de un SGSI son una política de seguridad y una metodología para medir el riesgo.

Seguridad orientada a la gestión del riesgo

Salvaguardas y tecnologías de seguridad más habituales

6.- Resumen

- El Sistema de Gestión de la Seguridad de la Información (SGSI) busca garantizar la continuidad del negocio, minimizando riesgos y maximizando el retorno de la inversión en seguridad.
- Las empresas deben profundizar en el conocimiento de los riesgos habituales de los equipos informáticos y establecer salvaguardas adecuadas.
- Las herramientas elementales de un SGSI son una política de seguridad y una metodología para evaluar el riesgo, adaptadas a las necesidades y recursos de la empresa.