

Unidad 1: Principios de seguridad y alta disponibilidad

Resultados de Aprendizaje a trabajar en esta Unidad:
RA1: Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
Contenidos a trabajar en esta Unidad:
- Introducción a la seguridad informática - Fiabilidad, confidencialidad, integridad y disponibilidad - Elementos vulnerables en el sistema informático: hardware y software - Amenazas provocadas por personas - Amenazas físicas y lógicas - Técnicas de ataque - Protección - Auditoría de seguridad de sistemas de información - Medidas de seguridad

Contenidos de la Unidad:

1. INTRODUCCIÓN 2
2. PRINCIPIOS BÁSICOS DE LA CIBERSEGURIDAD 3
3. AMENAZAS Y VULNERABILIDADES 4
4. CIBERPROTECCIÓN 6
5. ALTA DISPONIBILIDAD 9
6. ANÁLISIS FORENSE DIGITAL 10
7. BIBLIOGRAFÍA 12

1. INTRODUCCIÓN

La **seguridad informática** consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se haya decidido, y que el acceso a la información allí contenida, así como su modificación, sólo sea posible para las personas que se encuentren acreditadas para ello, y dentro de los límites de su autorización.

Por tanto, podemos definir la seguridad informática como el conjunto de medidas preventivas y reactivas que posibilitan la protección de la información, con objeto de conseguir una elevada fiabilidad del sistema. Nunca va a ser posible garantizar la total seguridad del sistema, por ello hablamos de niveles de fiabilidad.

Los **principales objetivos** de la seguridad informática son:

- Detectar posibles problemas y amenazas de seguridad, minimizando y gestionando los riesgos.
- Garantizar la adecuada utilización de recursos de las aplicaciones.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un accidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo.

La seguridad en una organización es un problema integral: afecta a software, hardware y datos. Los datos son el principal elemento que se debe proteger al ser el más difícil de recuperar. Por tanto, cualquier organización debe establecer una política de copias de seguridad.

Existen diferentes perspectivas desde las que abordar la seguridad informática:

- **Seguridad pasiva**: medidas que tratan de reparar o minimizar un daño que ya se ha producido en un sistema informático. Por ejemplo, las copias de seguridad.
- **Seguridad activa**: medidas que tratan de prevenir algún daño en un sistema informático. Por ejemplo, controles de acceso, cortafuegos...
- **Seguridad física**: medidas que tratan de proteger al hardware de los sistemas informáticas. Las amenazas físicas no tienen por qué ser malintencionadas (incendios, inundaciones, sobrecargas eléctricas...).
- **Seguridad lógica**: medidas que tratan de proteger el software y los datos de los sistemas informáticos. Por ejemplo, gestión del sistema (usuarios, privilegios, claves...), software antimalware cifrado de información y comunicaciones...
- **Configuraciones de alta disponibilidad**: redundancia, balanceo, virtualización...

Uno de los principales problemas en seguridad informática es que sus amenazas evolucionan muy rápidamente con el tiempo, y por tanto, hay que ir actualizando y modificando las medidas de seguridad de las organizaciones.

Algunas páginas importantes para consultar y estar actualizado en este ámbito son:

- INCIBE (Instituto Nacional de Ciberseguridad de España): www.incibe.es/
- CNI-CERT (Centro Criptológico Nacional): www.ccn-cert.cni.es/es/

2. PRINCIPIOS BÁSICOS DE LA CIBERSEGURIDAD

"El único sistema que es totalmente seguro es aquél que se encuentra apagado y desconectado, guardado en una caja fuerte de titanio que está enterrada en cemento, rodeada de gas nervioso y de un grupo de guardias fuertemente armados. Aun así, no apostaría mi vida en ello". Eugene H. Spafford (experto en seguridad).

Los **principios básicos de la ciberseguridad** son aquellos elementos que al ponerse en riesgo comprometen la información, así como el funcionamiento de los sistemas que estén relacionados de alguna manera con ella.

A continuación, se enumeran los principales:

- **Fiabilidad**: el sistema informático debe permanecer en funcionamiento, sin bajar de un nivel mínimo de rendimiento que se considere óptimo. Se debe mantener la consistencia entre el comportamiento esperado del sistema y los resultados obtenidos del mismo.
- **Confidencialidad**: los datos del sistema solo deben ser accesibles para las personas que estén autorizados para manejarlos.
- **Integridad**: el sistema debe mantener el conjunto de sus datos sin pérdidas o alteración no deseada de estos (corrupción de datos).
- **Disponibilidad**: el sistema informático y sus datos deben estar accesibles en todo momento que sean requeridos, sin momentos de desconexión (a excepción de los mínimos imprescindibles para tareas de mantenimiento).

Además, existen otros conceptos importantes:

- **Autenticación**: verificación de la identidad de un usuario que pretende acceder a un servicio, o bien, verificación de que un documento ha sido elaborado o pertenece a quien el documento dice.
- **No repudio**: permite probar la participación de todas las partes en una comunicación, ni el emisor ni el receptor pueden negar que el envío de información se realizó.
    - No repudio en origen: el emisor no puede negar haber realizado el envío, la prueba la crea el propio emisor. Por ejemplo, una firma digital.

- No repudio en destino: el receptor no puede negar haber recibido la comunicación. La prueba la crea el receptor. Por ejemplo, acuse de recibo.

2.1. La paradoja de la seguridad

Hay tres propiedades de un sistema informático que todo administrador de sistemas persigue:

- **Funcionalidad**: el sistema pone a disposición de sus usuarios multitud de herramientas y servicios para facilitar su trabajo.
- **Usabilidad**: el sistema es amigable para los usuarios.
- **Seguridad**: el sistema y sus datos son seguros.

Sin embargo, estas tres propiedades no son totalmente compatibles entre sí, pues cuanto más seguro sea un sistema, menos funcional y usable será.

El administrador deberá tender a acercar el sistema lo más posible a la seguridad, pero sin restringir demasiado la funcionalidad o la usabilidad.

3. AMENAZAS Y VULNERABILIDADES

En el ámbito de la ciberseguridad, una **amenaza** es una acción que pretende ser dañina para un sistema, es decir, un potencial ataque malicioso. En ocasiones, estas amenazas se deben a que el sistema en cuestión tiene vulnerabilidades.

Una **vulnerabilidad** se refiere a una debilidad o fallo en el diseño, implementación o proceso del sistema, que puede ser explotado por factores externos. Es decir, una brecha de seguridad en los componentes del sistema, que en caso de explotarse, tendría un impacto negativo en el sistema.

Existen diferentes **tipos de amenazas**:

- **Amenazas físicas** (y ambientales): afectan a las instalaciones y al hardware. Son el primer nivel de seguridad. Pueden ser intencionadas o no.
  - Robos, sabotajes, accesos no autorizados.
  - Cortes de red eléctrica o alteraciones de tensión.
  - Condiciones atmosféricas adversas.
  - Catástrofes naturales o provocadas.
  - Interferencias electromagnéticas.
- **Amenazas lógicas**: afectan al software y especialmente, a los datos.
  - Acceso ilegítimo al sistema informático, por ejemplo, hackers suplantando a un usuario administrador.
  - Software malicioso: virus, gusanos, troyanos…

- Privacidad de los datos y las comunicaciones: captación de datos, suplantación de identidad...

3.1. Técnicas de ataque

Podemos diferenciar diferentes técnicas de ataque que nuestros sistemas pueden sufrir:

- Malware: programas malintencionados. Por ejemplo, virus, spyware, troyanos...
- Ingeniería social: obtener información confidencial (usuarios, claves, datos personales...) mediante el engaño y manipulación a los usuarios para lograr que estos realicen alguna acción perjudicial para ellos.
- Spam: correo basura, propaganda no deseada y/o fraudulenta, remitente desconocido. Puede ser parte de las técnicas de ingeniería social, o portador de archivos adjuntos con código malicioso.
- Spoofing: suplantación de identidad. Puede ser a nivel de dirección IP, dirección MAC, modificación de tablas ARP, suplantación de sitios web, suplantación de remitentes de correo...
- Sniffing: monitorización del tráfico de red que puede dar lugar a la captura de información confidencial.
- Phishing: estafa basada en la suplantación de identidad e ingeniería social para obtener credenciales de acceso a sitios.
- Password cracking: técnicas para descifrar contraseñas de sistemas y comunicaciones. Puede ser por sniffing, fuerza bruta, ataques de diccionario, etc.
- DDoS: ataques de denegación de servicio. Su finalidad es agotar la capacidad de respuesta de servidores por inundación de peticiones.

3.2. Malware

Malware es la abreviatura de software malicioso, o código malicioso. Es código o software específicamente diseñado para dañar, interrumpir, robar o efectuar otras acciones malintencionadas o ilegítimas de datos, hosts o redes.

El malware se transforma tan rápidamente que los incidentes de seguridad relacionados con malware son muy comunes, ya que el software antimalware no se puede actualizar lo suficientemente rápido para detener las nuevas amenazas.

Existen diferentes **tipos de malware:**

- Virus: código malicioso que se acopla a un archivo ejecutable (anfitrión) de forma que se ejecuta cuando el archivo anfitrión lo hace. Hay muchos tipos de virus informáticos.

- Troyano: programas aparentemente normales, pero con código malicioso oculto que se ejecuta sin conocimiento del usuario.
- Ransomware: es malware que deniega el acceso al sistema informático infectado o a sus datos. Después de atacar, los ciberdelincuentes exigen dinero para liberar el sistema informático. Suele utilizar un algoritmo de encriptación para encriptar los datos y archivos del sistema.
- Spyware: recopila la actividad de un usuario en el sistema, para enviarla al ciberdelincuente.
- Adware: consiste en mostrar anuncios y publicidad de forma constante, siendo bastante molesto, y haciendo que los ciberdelincuentes obtengan un beneficio económico.
- Keylogger: registra todas las teclas que se han pulsado en el sistema, pudiendo descubrir información confidencial y valiosa como contraseñas, cuentas bancarias, etc.
- Gusano: su característica principal es que puede autopropagarse a través de redes de ordenadores infectando a todos los equipos conectados.

Algunos de los síntomas más comunes que aparecen en sistemas infectados con malware son los siguientes:

- Aparecen archivos, programas o iconos de escritorio extraños.
- Los programas antivirus y firewall se apagan o sus ajustes se reconfiguran.
- La pantalla del ordenador se congela o el sistema deja de funcionar.
- Se envían mensajes de correo electrónico a la lista de contactos sin nuestro conocimiento.
- Se modifican o eliminan archivos.
- Aumenta el uso de la CPU o de la memoria.
- Hay problemas para conectarse a redes.
- Se reduce la velocidad del ordenador o del navegador.
- Se ejecutan procesos o servicios desconocidos.
- Aparecen puestos TCP o UDP desconocidos abiertos.

4. CIBERPROTECCIÓN

Una auditoría de seguridad es un estudio que incluye el análisis de sistemas para identificar vulnerabilidades. Los objetivos principales de una auditoría de seguridad en sistemas de información son:

- Revisar la seguridad de entornos y sistemas.
- Verificar el cumplimiento de la normativa y legislación vigentes.
- Elaborar un informe.

Estas auditorías se realizan en base a un patrón de "buenas prácticas" de seguridad. Existen diferentes estándares que sirven como base a las auditorías informáticas:

- COBIT (Objetivos de Control de las Tecnologías de la Información)
- ISO 27002 (Código internacional de buenas prácticas de seguridad de la información).
- ISO 27001 (Requisitos de auditoría y sistemas de gestión de seguridad informática)

Generalmente, los servicios de auditoría constan de las siguientes partes:

- Enumeración de todos los dispositivos, sistemas operativos, servicios, aplicaciones, topologías y protocolos de red, etc. existentes en el sistema.
- Detección, comprobación y evaluación de vulnerabilidades existentes.
- Medidas específicas de corrección y protección.
- Recomendaciones sobre implantación de medidas preventivas.
- Elaboración de un informe que recoja todo lo anterior.

Existen diferentes tipos de auditoría de seguridad:

- **Auditoría interna**: son realizadas por el propio personal del departamento encargado de la seguridad de la información, que deberá ser dependiente del departamento encargado de las TIC, y se encargan de comprobar que las medidas de control establecidas se están implementando correctamente en los sistemas de la organización. En este caso, los encargados de realizar la auditoría conocen perfectamente la organización, así como todos los sistemas implicados en ella.
- **Auditoría externa**: son contratadas a personas externas a la organización. Este proceso suele ser más largo, pero tiene unos objetivos muy similares. Para este tipo de auditorías es imprescindible garantizar un acuerdo de confidencialidad por contrato antes de que se lleve a cabo la auditoría.
- **Test de intrusión**: se intenta acceder a los sistemas para comprobar el nivel de resistencia a la intrusión no deseada.
- **Análisis forense**: tras un incidente de seguridad, trata de reconstruir cómo se ha producido el problema y valorar los daños ocasionados.

4.1. Medidas de seguridad

A partir de los resultados obtenidos con las diferentes auditorías realizadas, habrá que diseñar una política de seguridad que defina las reglas a seguir para evitar amenazas o minimizar daños.

Para ello, se definen una serie de mecanismos de seguridad. Estos se pueden clasificar:

- Según el recurso a proteger:
    - **Seguridad física**: acceso físico, protección ante robos, catástrofes naturales… Medidas de este tipo son ubicación correcta, medidas de seguridad de acceso, protección física, eléctrica, generadores, sistemas anti-incendios, refrigeración, etc.
    - **Seguridad lógica**: proteger el software tanto a nivel de aplicación como de sistema operatico y, por supuesto, a nivel de datos de usuario. Medidas de este tipo son copias de seguridad, política de contraseñas, permisos de usuario, cifrado de datos y comunicaciones, software antimalware, etc.
- Según el momento en el que se ponen en marcha:
    - **Seguridad activa**: medidas preventivas para evitar daños frente a posibles amenazas.
    - **Seguridad pasiva**: medidas correctivas que minimizan el impacto de los efectos causados por los incidentes.

4.2. Plan de formación y concienciación

Una vez implantadas todas las medidas de seguridad que se han considerado necesarias durante las auditorías, se debe concienciar y formar a los usuarios de la organización. Para ello se deberá establecer un plan de formación y concienciación.

La **formación** tiene la misión de capacitar al personal para prevenir, mitigar o dar respuesta a las posibles amenazas que puedan afectar al sistema.

La **concienciación** debe garantizar que todos los miembros de la organización están sensibilizados con la importancia de participar activamente en la seguridad de la información, e involucrarlos en la puesta en práctica de los diferentes controles de seguridad, cada cual al nivel que corresponda.

Todo plan de formación y concienciación debe tener en cuenta:

- Que todo el personal debe recibir una formación y concienciación iniciales.
- Que tanto la concienciación como la formación deben refrescarse y actualizarse regularmente.

El objetivo de este plan es fomentar una cultura de ciberseguridad dentro de la organización, y educar a todos los empleados en la importancia de protección de datos, prácticas seguras, etc. Para ello, hay que tener en cuenta una serie de criterios que garantice que todo el personal conoce, entiende y cumple las normas y medidas establecidas.

- Nivel inicial de conocimientos sobre ciberseguridad

Dentro de una organización nos encontraremos con perfiles de usuario de muy diferentes tipos, con niveles de conocimientos sobre medidas de seguridad muy diferentes entre sí. Por tanto, es muy recomendable realizar una evaluación inicial para identificar el nivel existente de conocimiento entre los empleados, antes de diseñar el plan de formación y concienciación.

- Roles existentes en la organización

La formación se deberá ajustar a los diferentes roles y responsabilidades del personal de la organización, ya que en función de ello variarán aspectos como la información a la que tienen acceso, los sistemas con los que trabajan, los procesos que realizan, las personas con las que tienen relación laboral, las ubicaciones desde las que llevan a cabo sus funciones, etc.

- Tipo de información

Dependiendo del tipo de datos a los que tenga acceso una organización, se deberán adecuar los contenidos de la formación a la legislación correspondiente para cada uno de ellos.

- Servicios

También se han de tener en cuenta los diferentes servicios con los que trabaja la organización. Algunos de los servicios sensibles podrían ser la página web corporativa, un sistema de almacenamiento en la nube, redes sociales de la organización, etc.

- Políticas de empresa

Otro factor a tener en cuenta de cara a la planificación de la formación es cómo se trabaja en dicha organización. Dependiendo de si el trabajo es presencial, remoto o mixto, o de si únicamente se utilizan dispositivos corporativos o no, la formación deberá ser diferente, para adecuarse a la realidad de la organización.

5. ALTA DISPONIBILIDAD

La **alta disponibilidad (HA, High Availability)** se refiere a la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones.

El objetivo de la alta disponibilidad es mantener operativos los sistemas las 24 horas al día, los 365 días al año.

Se diferencian dos tipos de posibles interrupciones:

- **Interrupciones previstas**: están programadas. Son las realizadas para hacer cambios o mejoras en el sistema.
- **Interrupciones imprevistas:** apagones, errores de hardware o software, desastres naturales, incidentes de seguridad, etc.

La métrica utilizada para evaluar la alta disponibilidad es el tiempo medio entre fallos (MTTF) y el tiempo medio en recuperarse (MTTR). El tiempo fuera de servicio se mide habitualmente como MTTR/MTTF.

Algunos sistemas que requieren alta disponibilidad son el sistema sanitario, el control aéreo, el sistema bancario, sistemas militares...

6. ANÁLISIS FORENSE DIGITAL

El **análisis forense digital** es una disciplina que se centra en la recolección, preservación, examen y análisis de evidencia digital con el fin de investigar y resolver crímenes cibernéticos, incidentes de seguridad, y también auditorías.

Se aplica en casos como delitos informáticos, fraudes, intrusiones en sistemas y robo de datos, entre otros.

Se basa en un conjunto de técnicas de recopilación y peritaje exhaustivo de datos, que pueden aplicarse para responder en algún tipo de incidente con el objetivo de entender la naturaleza del ataque.

Podemos resumir el análisis forense en **fases** que facilitan la verificabilidad y la reproducibilidad del análisis:

1) Adquisición y recopilación de evidencias

El primer paso en un análisis forense de ciberseguridad es identificar todos aquellos dispositivos y recursos que contienen los datos que formarán parte de la investigación. Revisar qué sistemas muestran síntomas, confirmar si se trata de un incidente real, identificar sistemas afectados...

Los analistas extraen datos de una variedad de fuentes como pueden ser móviles, ordenadores, tablets, servicios de computación en la nube, redes... Se recopilan todas las evidencias digitales del sistema afectado (archivos, registro de eventos, programas maliciosos, correos electrónicos...).

2) Preservación

El siguiente paso es aislar, asegurar y conservar la mayor cantidad de evidencia digital posible en la red afectada, así como prevenir cualquier alteración o destrucción de las evidencias halladas. El objetivo es almacenar la información a salvo del acceso de

cualquier persona ajena a la investigación para que la víctima del ciberataque pueda hacer uso de ellas en un caso legal, si así se considera necesario.

Aquí aparece la cadena de custodia, un acta donde se registra el lugar, fecha, analista y demás personas que manipularon la muestra. Se debe asegurar la cadena de custodia (saber quién tiene la evidencia en cada momento), guardar copias de seguridad de logs y configuraciones…

3) Análisis

Una vez que los dispositivos involucrados han sido identificados y asilados, y los datos han sido duplicados y almacenados de forma segura, llega el momento de extraer datos relevantes y examinar las evidencias con minuciosidad, en busca de pistas o pruebas que apunten a irregularidades.

Este proceso puede implicar recuperar y examinar archivos eliminados, dañados o cifrados. Gracias a este análisis forense los expertos son capaces de comprender la causa, la secuencia de eventos y cómo se ejecutó el ciberataque.

4) Presentación

Finalmente, se prepara un informe claro y comprensible. Tiene que poder leerlo tanto un juez, como un responsable de la empresa afectada, es decir, personal no técnico.

Se deben incluir explicaciones simples, un glosario en caso de ser necesario, y sobre todo las conclusiones obtenidas (qué pasó, cuándo pasó, cómo pasó y qué consecuencias tuvo).

El informe sólo será válido si toda la evidencia se recogió y adquirió siguiendo todos los requisitos legales.

7. BIBLIOGRAFÍA

Análisis forense informático. M. Guerra. Ediciones de la U.

Crimen, cibercrimen y análisis forense informático. F.J. de Haro Olmo.

Incidentes de ciberseguridad. P. Pavón Rosano. Paraninfo

Fases y metodología del análisis forense. J.M.A. Soldevila, M.C. Huguet y E. de Luis Gargallo.

Seguridad Informática. Alfonso García-Cervigón, María del Pilar Alegre. Paraninfo.

Seguridad Informática. José Fabián Roa Buendía. McGraw Hill.

Seguridad y alta disponibilidad. Alfredo Abad Domingo. Garceta.

Seguridad y alta disponibilidad. Ignacio Triviño Mosquera. Síntesis

Otros: INCIBE, Wikipedia.