Tema 1. Conceptos básicos sobre seguridad informática

Seguridad en Sistemas Informáticos
4^o Grado en Ingeniería Informática – ESEI

Septiembre-2018

Conceptos básicos

Definición (seguridad en sistemas de información)

Protección de los activos de un sistema de información con la intención de garantizar unos niveles adecuados de confidencialidad, integridad y disponibilidad sobre los mismos

Principios básicos de la seguridad

Confidencialidad los activos sólo han de poder ser accedidos por los elementos autorizados a ello

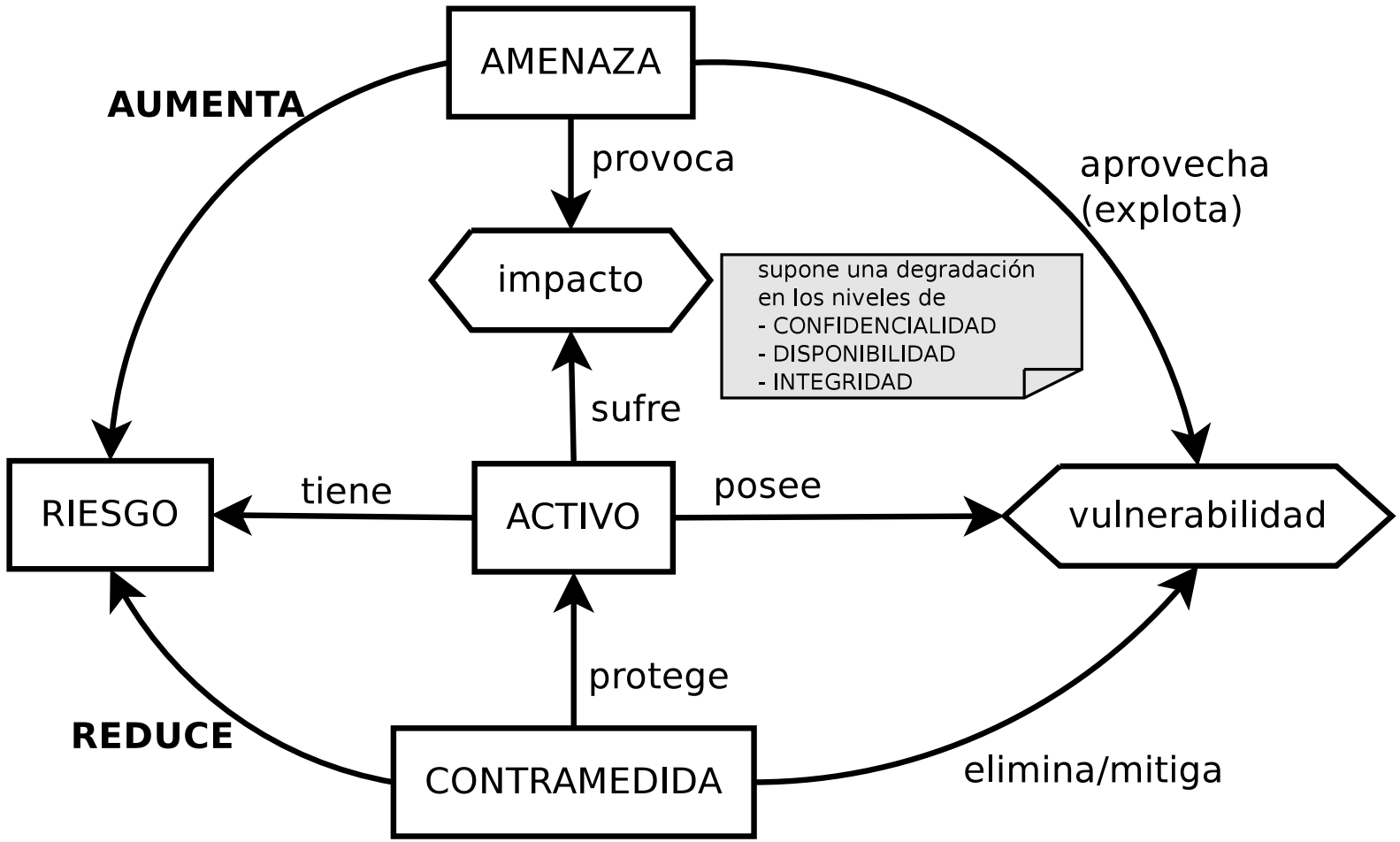
los elementos autorizados no van a poder hacer disponibles dichos activos a terceros no autorizados

Integridad los activos sólo pueden ser modificados (creación,modificación, eliminación) por elementos autorizados de modo que se salvaguarde su exactitud y completitud

Disponibilidad los activos tienen que permanecer accesibles y utilizables por parte de los elementos autorizados cuando estos los requieran

- Los mecanismos de seguridad se implementan para proteger uno o más de estos principios
- Riesgo, amenazas y vulnerabilidades se miden en función de su capacidad de comprometer alguno de estos principios
- Son principios complementarios y contrapuestos $\Rightarrow$ deben balancearse

Elementos (I)


AMENAZA
AUMENTA
provoca
aprovecha (explota)
impacto
supone una degradación en los niveles de
- CONFIDENCIALIDAD
- DISPONIBILIDAD
- INTEGRIDAD
sufre
RIESGO
tiene
ACTIVO
posee
vulnerabilidad
protege
REDUCE
CONTRAMEDIDA
elimina/mitiga

Elementos (II)

Activos

Cualquier recurso (tangible o intangible) con valor para una organización

Tipos de activos (según Libro II de la metodología MAGERIT ver. 3)

activos esenciales	información (datos personales, datos clasificados, ...), servicios
arquitectura del sistema	puntos de acceso al servicio, puntos de interconexión, ...
datos/información	ficheros, copias de seguridad, datos de configuración, credenciales, registros de control de acceso, registros de actividad, código fuente, ejecutables, datos de prueba, ...
claves criptográficas	claves de cifrado, claves de firma, certificados, soportes físicos cifrados, ...
servicios	internos, al público en general, a usuarios externos, web, correo electrónico, acceso remoto, directorio, tranferencia de ficheros, almacenamiento, ...
software/aplicaciones	desarrollo propio, desarrollo a medida, software estándar (navegadores, servidor de aplicaciones, ofimática, sistema operativo, antivirus, sistema de backup, ...)
equipamiento informático	grandes equipos, informática personal, informática móvil, equipo virtual, periféricos (impresoras, escaner, ...), dispositivos de red (modem, router, firewall, pasarela, punto de acceso inalámbrico....), centralita telefónica, ...
redes de comunicaciones	red telefónica, enlace punto a punto, ADSL, red inalámbrica, red local, telefónía móvil, ...
soportes de información	electrónicos (discos, cintas, CD/DVD, almacenamiento en red, memorias USB, ...) y y no electrónicos (papel impreso, microfilm, ...)
equipamiento auxiliar	cableado, SAI, climatización, mobiliario, robots de cintas, generadores, ...
instalaciones	recinto, edificio, sala, canalización, vehículo, instalaciones de respaldo, ...
personal	usuarios internos, usuarios externos, operadores, administradores (de red, de sistemas, de BD, de seguridad, ...), desarrolladores, proveedores, subcontratas, ...

También se consideran activos aspectos intangibles como ”reputación”, ”confianza”, ”imagen de marca”, etc

Elementos (III)

Amenazas (1)

Cualquier peligro potencial sobre un activo de la organización

- Algo o alguien que puede aprovechar una vulnerabilidad (explotarla) para causar un impacto sobre la confidencialidad, integridad o disponibilidad de un activo
- Pueden ser accidentales o intencionadas

Tipos de amenazas (según Libro II de la metodología MAGERIT ver. 3)

desastres naturales	fuego, daños por agua, terremotos, derrumbes, caídas, ...
de origen industrial	fuego, daños por agua, contaminación mecánica, contaminación electromagnética, avería física o lógica, corte de suministro eléctrico, temperatura/humedad inadecuada, fallo de comunicaciones, interrupción de servicios y suministros esenciales, degradación de soportes almacenamiento, ...
errores y fallos no intencionados	errores de usuarios, errores de administrador, errores de monitorización, errores de configuración, deficiencias en la organización, difusión de software dañino, escapes de información,alteración accidental de la información, destrucción de la información, fugas de información, vulnerabilidades del software, errores de mantenimiento/actualización del software, errores de mantenimiento o actualización del hardware, caída del sistema por agotamiento de recursos, pérdida de equipos, indisponibilidad del personal, ...
ataques intencionados	manipulación registros de actividad, manipulación de la configuración, suplantación de usuario, abuso de privilegios de acceso, uso no previsto, difusión de software dañino, repudio, acceso no autorizado, análisis de tráfico, interceptación/escucha de información, modificación o destrucción de información, divulgación de información, manipulación de programas, robo manipulación de equipos, denegación de servicio, ataque destructivo, ocupación enemiga, indisponiblidad del personal, extorsión, ingeniería social, ...

Elementos (IV)

Amenazas (2)

Tipos genéricos de amenazas (por su efecto sobre los activos)

de interrupción hacen que un activo del sistema se pierda o quede inutilizado

- atenta contra la disponibilidad

de interceptación un elemento no autorizado tiene acceso a un activo del sistema

- atenta contra la confidencialidad

de modificación además de acceder, el elemento no autorizado consigue modificar el activo

- atenta contra la integridad (y disponibilidad en caso de destrucción)

de fabricación un elemento no autorizado consigue ”construir” una réplica de un activo legítimo

Vulnerabilidades

Debilidades que pueden proporcionar a una amenaza la posibilidad de comprometer y/o causar daño a un activo

- deficiencias de configuración, ausencia de controles de seguridad, deficiencias en su instalación/uso, etc

Elementos (V)

Riesgo

Cuantificación de la posibilidad de que una amenaza aproveche una vulnerabilidad causando un impacto en la confidencialidad, integridad o disponibilidad de un activo

- Suele tener asociada una valoración del coste que supone

Mecanismos/controles de seguridad (1)

Elementos físicos, técnicos o organizativos que permiten mitigar un riesgo potencial

- También: contramedidas, salvaguardas, ...
- **Reducen el riesgo** sobre uno o varios activos
  - eliminando la vulnerabilidad de lo causa
  - reduciendo la posibilidad de que la vulnerabilidad sea explotada

Clasificación genérica

- controles **administrativos**: procedimientos, políticas, normas, etc
- controles **técnicos** (lógicos): cortafuegos, cifrado, antimalware, etc
- controles **físicos**: sistemas antiincendios, vigilancia, cerraduras, biometría, etc

Elementos (VI)

Mecanismos/controles de seguridad (2)

Tipos de controles por su funcionalidad

- preventivos: pretenden evitar que un incidente de seguridad llegue a ocurrir
- de detección: permiten identificar las actividades propias de un incidente de seguridad que está siendo desencadenado por parte de un atacante/amenaza
- de recuperación: buscan devolver el sistema a un estado que permita su operación normal
- correctivos: corrigen los componentes, sistemas o controles que no han cumplido su labor (una vez que un incidente ya ha sucedido) para evitar futuros incidentes similares
- disuasorios: buscan disuadir a los posibles atacantes/amenazas

Elementos (VII)

Ejemplos de tipos de controles

Seguridad física (controles de seg. físicos)	**Seguridad lógica** (controles de seg. técnicos)	**Seguridad organizativa y legal** (controles organizativos y legales)
Preventivos cerraduras tarjetas de acceso control biométrico guardias de seguridad bloqueo de ventanas hacia el exterior normativas de acceso a activos físicos formación de usuarios **De detección** detectores de movimiento cámaras de circuito cerrado detectores de humo **Disuasorios** vallas de seguridad **De recuperación** réplica de activos en otra localización extinción automática	**Preventivos** config. routers (reglas de filtrado) firewalls cifrado de la inform. en tránsito cifrado de la inform. almacenada software antivirus/antimalware **De detección** sistemas detección intrusiones análisis de logs **De recuperación** sistemas y políticas de back-up **Correctivos** réplicas (imágenes) de máquinas preconfiguradas	**Preventivos** políticas y procedimientos procedimientos de contratación de personal clasificación y etiquetado de recursos cumplimiento de leyes/normas **De detección** rotación en puestos investigación de actividades **Disuasorios** sanciones y penalizaciones acuerdos de confidencialidad

Controles del Libro II de Magerit versión 3

Protecciones generales u horizontales
- Identificación y autenticación
- Control de acceso lógico
- Segregación de tareas
- Gestión de incidencias
- Herramientas de seguridad
- Herramienta contra código dañino
- IDS/IPS: Herramienta de detección y prevención de intrusión
- Herramienta de chequeo de configuración
- Herramienta de análisis de vulnerabilidades
- Herramienta de monitorización de tráfico
- Herramienta de monitorización de contenidos
- Herramienta para análisis de logs
- Honey net / honey pot
- Verificación de las funciones de seguridad
- Gestión de vulnerabilidades
- Registro y auditoría

Protección de las aplicaciones (software)
- Copias de seguridad (backup)
- Puesta en producción
- Se aplican perfiles de seguridad
- Explotación / Producción
- Cambios (actualizaciones y mantenimiento)
- Terminación

Protección de los equipos (hardware)
- Protección de los Equipos Informáticos
- Puesta en producción
- Se aplican perfiles de seguridad
- Aseguramiento de la disponibilidad
- Operación
- Cambios (actualizaciones y mantenimiento)
- Terminación
- Informática móvil
- Reproducción de documentos
- Protección de la centralita telefónica (PABX)

Seguridad física – Protección de las instalaciones
- Protección de las Instalaciones
- Diseño
- Defensa en profundidad
- Control de los accesos físicos
- Aseguramiento de la disponibilidad
- Terminación

Protección de los datos / información
- Copias de seguridad de los datos (backup)
- Aseguramiento de la integridad
- Cifrado de la información
- Uso de firmas electrónicas
- Uso de servicios de fechado electrónico (time stamping)

Protección de las claves criptográficas
- Gestión de claves criptográficas
- Gestión de claves de cifra de información
- Gestión de claves de firma de información
- Gestión de claves para contenedores criptográficos
- Gestión de claves de comunicaciones
- Gestión de certificados

Protección de las comunicaciones
- Entrada en servicio
- Se aplican perfiles de seguridad
- Aseguramiento de la disponibilidad
- Autenticación del canal
- Protección de la integridad de los datos intercambiados
- Protección criptográfica de la confidencialidad de los datos intercambiados
- Operación
- Cambios (actualizaciones y mantenimiento)
- Terminación
- Seguridad Wireless (WiFi)
- Telefonía móvil
- Segregación de las redes en dominios

Continuidad de operaciones
- Prevención y reacción frente a desastres.
- Continuidad del negocio
- Análisis de impacto (BIA)
- Recuperación de Desastres (DRP)

Adquisición y desarrollo
- Adquisición / desarrollo
- Servicios: Adquisición o desarrollo
- Aplicaciones: Adquisición o desarrollo
- Equipos: Adquisición o desarrollo
- Comunicaciones: Adquisición o contratación
- Soportes de Información: Adquisición
- Productos certificados o acreditados

Salvaguardas de tipo organizativo
- Organización
- Gestión de riesgos
- Planificación de la seguridad
- Inspecciones de seguridad

Protección de los servicios
- Aseguramiento de la disponibilidad
- Aceptación y puesta en operación
- Se aplican perfiles de seguridad
- Explotación
- Gestión de cambios (mejoras y sustituciones)
- Terminación
- Protección de servicios y aplicaciones web
- Protección del correo electrónico
- Protección del directorio
- Protección del servidor de nombres de dominio (DNS)
- Voz sobre IP

Protección en los puntos de interconexión con otros sistemas
- Puntos de interconexión: conexiones entre zonas de confianza
- Sistema de protección perimetral
- Protección de los equipos de frontera

Protección de los soportes de información
- Protección de los Soportes de Información
- Aseguramiento de la disponibilidad
- Protección criptográfica del contenido
- Limpieza de contenidos
- Destrucción de soportes

Protección de los elementos auxiliares
- Aseguramiento de la disponibilidad
- Instalación
- Suministro eléctrico
- Climatización
- Protección del cableado

Externalización
- SLA: nivel de servicio, si la disponibilidad es un valor
- NDA: compromiso de secreto, si la confidencialidad es un valor
- Identificación y calificación del personal encargado
- Procedimientos de escalado y resolución de incidencias
- Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)
- Asunción de responsabilidades y penalizaciones por incumplimiento
- Acuerdos para intercambio de información y software
- Acceso externo
- Servicios proporcionados por otras organizaciones
- Personal subcontratado

Salvaguardas relativas al personal
- Gestión del Personal
- Formación y concienciación
- Aseguramiento de la disponibilidad

Ejemplo

Activo:	PCs de una organización
Amenaza:	Nuevo virus/malware (no reconocido por el software antivirus)
Vulnerabilidad:	Firmas de virus no actualizadas en el antivirus corporativo
Riego:	Posibilidad de que esos virus infecten los equipos y causen daños/pérdidas Supondrá cuantificar: - probabilidad de que suceda la infección - coste que supondría la infección, incluyendo * coste por posible pérdida/robo de datos * coste de las molestias y pérdida de tiempo productivo de los usuarios * coste de la eliminación del virus o la reinstalación de equipos * otros costes
Contramedidas:	técnicas: - programar actualización del antivirus (adquiriéndolas si es preciso o cambiando de antivirus) organizativas: - definir procedimiento de actualización, compra e instalación de antivirus - establecer políticas de concienciación de usuarios