1 Seguridade e Alta Dispoñibilidade (Ciclo ASIR)

Seguridade e Alta Disponibilidade do Ciclo ASIR

- **Curso:** 2º
- **Duración:** 105 horas
- **Profesorado:** Informática

1.1 Sumario

1.2 RA1. Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.

? CA1.1. Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.
? CA1.2. Describíronse as diferenzas entre seguridade física e lóxica.
? CA1.3. Clasificáronse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.
? CA1.4. Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.
? CA1.5. Adoptáronse políticas de contrasinais.
? CA1.6. Valoráronse as vantaxes do uso de sistemas biométricos.
? CA1.7. Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.
? CA1.8. Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.
? CA1.9. Identificáronse as fases da análise forense ante ataques a un sistema.

1.2.1 Contidos básicos

- Fiabilidade, confidencialidade, integridade e dispoñibilidade.
- Elementos vulnerables no sistema informático: hardware, software e datos.
- Análise das principais vulnerabilidades dun sistema informático.
- Pautas e prácticas seguras.
- Tipos de ameazas: físicas e lóxicas.
- Seguridade física e ambiental:
  - Localización e protección física dos equipamentos e dos servidores.
  - Sistemas de alimentación ininterrompida.
- Seguridade lóxica:
  - Criptografía.
  - Listas de control de acceso.
  - Establecemento de políticas de contrasinais.
  - Sistemas biométricos de identificación.
  - Políticas de almacenamento.
  - Medios de almacenamento.
- Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias.

- Ferramentas empregadas na análise forense.

1.3 RA2. Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.

? CA2.1. Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático.
? CA2.2. Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.
? CA2.3. Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.
? CA2.4. Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.
? CA2.5. Implantáronse aplicacións específicas para a detección de ameazas e a eliminación de software malicioso.
? CA2.6. Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.
? CA2.7. Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.
? CA2.8. Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.
? CA2.9. Describíronse os tipos e as características dos sistemas de detección de intrusións.

1.3.1 Contidos básicos

- Ataques e contramedidas en sistemas informáticos.
- Clasificación dos ataques.
- Anatomía de ataques e análise de software malicioso.
- Realización de auditorías de seguridade.
- Ferramentas preventivas e paliativas: instalación e configuración.
- Copias de seguridade e imaxes de respaldo.
- Recuperación de datos.
- Actualización de sistemas e aplicacións.
- Seguridade na conexión con redes públicas.
- Técnicas de cifraxe da información: clave pública e clave privada; certificados dixitais; sinaturas.
- Monitorización do tráfico en redes: captura e análise; aplicacións.
- Seguridade nos protocolos para comunicacións sen fíos.
- Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades.
- Intentos de penetración: tipoloxía.
- Sistemas de detección de intrusións.

1.4 RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.

? CA3.1. Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.
? CA3.2. Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral.
? CA3.3. Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.
? CA3.4. Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis.
? CA3.5. Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.
? CA3.6. Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.
? CA3.7. Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación.

1.4.1 Contidos básicos

- Elementos básicos da seguridade perimetral: encamiñador fronteira; tornalumes; redes privadas virtuais.
- Perímetros de rede. Zonas desmilitarizadas.
- Arquitectura débil e forte de subrede protexida.
- Redes privadas virtuais. VPN.
    - ♦ Beneficios e desvantaxes con respecto ás liñas dedicadas.
    - ♦ VPN a nivel de enlace.
    - ♦ VPN a nivel de rede. SSL e IPSec.
    - ♦ VPN a nivel de aplicación. SSH.
- Servidores de acceso remoto:
    - ♦ Protocolos de autenticación.
    - ♦ Configuración de parámetros de acceso.
    - ♦ Servidores de autenticación.

1.5 RA4. Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.

- **? CA4.1.** Describíronse as características, os tipos e as funcións dos tornalumes.
- **? CA4.2.** Clasificáronse os niveis en que se realiza a filtraxe de tráfico.
- **? CA4.3.** Configuráronse filtros nun tornalumes a partir dunha listaxe de regras de filtraxe.
- **? CA4.4.** Revisáronse os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente.
- **? CA4.5.** Interpretouse a documentación técnica de distintos tornalumes hardware nos idiomas máis empregados pola industria.
- **? CA4.6.** Probáronse distintas opcións para implementar tornalumes, tanto de software como de hardware.
- **? CA4.7.** Diagnosticáronse problemas de conectividade nos clientes provocados polos tornalumes.
- **? CA4.8.** Planificouse a instalación de tornalumes para limitar os accesos a determinadas zonas da rede.
- **? CA4.9.** Elaborouse documentación relativa á instalación, configuración e uso de tornalumes.

1.5.1 Contidos básicos

- Utilización de tornalumes.
- Filtraxe de paquetes de datos.
- Tipos de tornalumes: características e funcións principais:
    - ♦ Uso das características de tornalumes incorporadas no sistema operativo.
    - ♦ Implantación de tornalumes en sistemas libres e propietarios. Instalación e configuración.
    - ♦ Tornalumes hardware.
- Regras de filtraxe de tornalumes.
- Probas de funcionamento: sondaxe.
- Rexistros de sucesos nos tornalumes.

1.6 RA5. Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.

- **? CA5.1.** Identificáronse os tipos de proxy, as súas características e as súas funcións principais.
- **? CA5.2.** Instalouse e configurouse un servidor proxy cache.
- **? CA5.3.** Configuráronse os métodos de autenticación no proxy.
- **? CA5.4.** Configurouse un proxy en modo transparente.
- **? CA5.5.** Utilizouse o servidor proxy para establecer restricións de acceso web.
- **? CA5.6.** Arranxáronse problemas de acceso desde os clientes ao proxy.
- **? CA5.7.** Realizáronse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.
- **? CA5.8.** Configurouse un servidor proxy en modo inverso.
- **? CA5.9.** Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy.

1.6.1 Contidos básicos

- Tipos de proxy: características e funcións.
- Instalación de servidores proxy.
- Instalación e configuración de clientes proxy.
- Configuración do almacenamento na cache dun proxy.
- Configuración de filtros.
- Métodos de autenticación nun proxy.
- Proxy inverso.
- Encadeamento e xerarquías.
- Probas de funcionamento.

1.7 RA6. Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.

- **? CA6.1.** Analizáronse supostos e situacións en que cumpra pór en marcha solucións de alta dispoñibilidade.
- **? CA6.2.** Identificáronse solucións de hardware para asegurar a continuidade no funcionamento dun sistema.
- **? CA6.3.** Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.
- **? CA6.4.** Implantouse un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal.
- **? CA6.5.** Implantouse un balanceador de carga á entrada da rede interna.

? CA6.6. Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos.
? CA6.7. Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.
? CA6.8. Analizáronse solucións de futuro para un sistema con demanda crecente.
? CA6.9. Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.

1.7.1 Contidos básicos

- Definición e obxectivos.
- Análise de configuracións de alta dispoñibilidade.
    - Funcionamento ininterrompido.
    - Integridade de datos e recuperación de servizo.
    - Servidores redundantes.
    - Sistemas de clústers.
    - Balanceadores de carga.
- Instalación e configuración de solucións de alta dispoñibilidade.
- Virtualización de sistemas.
    - Posibilidades da virtualización de sistemas.
    - Ferramentas para a virtualización.
    - Configuración e uso de máquinas virtuais.
    - Alta dispoñibilidade e virtualización.
    - Simulación de servizos con virtualización.
    - Análise e optimización de sistemas virtualizados. Probas de carga.
- Virtualización en contornos de produción.

1.8 RA7. Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.

? CA7.1. Describiuse a lexislación sobre protección de datos de carácter persoal.
? CA7.2. Determinouse a necesidade de controlar o acceso á información persoal almacenada.
? CA7.3. Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
? CA7.4. Contrastouse o deber de pór ao dispor das persoas os datos persoais que lles atinxen.
? CA7.5. Describiuse a lexislación actual sobre os servizos da sociedade da información e o comercio electrónico.
? CA7.6. Contrastáronse as normas sobre xestión de seguridade da información.
? CA7.7. Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

1.8.1 Contidos básicos

- Lexislación sobre protección de datos e sobre os servizos da sociedade da información e o correo electrónico.