1 Seguridade Informática (Ciclo SMR)

Seguridade Informática do Ciclo SMR

- **Curso:** 2º
- **Duración:** 140 horas
- **Profesorado:** Informática

1.1 Sumario

1.2 RA1. Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo

- CA1.1. Valorouse a importancia de manter a información segura.
- CA1.2. Clasificouse a información no ámbito da seguridade.
- CA1.3. Describíronse as diferenzas entre seguridade física e lóxica.
- CA1.4. Identificáronse as principais técnicas criptográficas.
- CA1.5. Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.
- CA1.6. Identificáronse os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.).
- CA1.7. Recoñeceuse a necesidade de facer unha análise de riscos e a posta en marcha dunha política

de seguridade.

- CA1.8. Establecéronse as normas básicas para incluír nun manual de seguridade informática.
Tratamento seguro da información:
- ◊ Seguridade física e lóxica.
- ◊ Criptografía.
- ◊ Políticas de seguridade.

1.3 RA2. Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno

- CA2.1. Defiríronse as características da localización e as condicións ambientais dos equipamentos e dos servidores.
- CA2.2. Identificouse a necesidade de protexer fisicamente os sistemas informáticos.
- CA2.3. Verificouse o funcionamento dos sistemas de alimentación ininterrompida.
- CA2.4. Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.
- CA2.5. Esquematizáronse as características dunha política de seguridade baseada en listas de control de acceso.
- CA2.6. Valorouse a importancia de establecer unha política de contrasinais.
- CA2.7. Valoráronse as vantaxes do uso de sistemas biométricos.
Medidas de seguridade física e ambiental:
- ◊ Localización e protección física dos equipamentos e dos servidores.
- ◊ Sistemas de alimentación ininterrompida.

1.4 RA3. Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información

- CA3.1. Interpretouse a documentación técnica relativa á política de almacenaxe.
- CA3.2. Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade,

accesibilidade, etc.).

- CA3.3. Clasificáronse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.
- CA3.4. Describíronse as tecnoloxías de almacenaxe redundante e distribuída.
- CA3.5. Seleccionáronse estratexias para a realización de copias de seguridade.
- CA3.6. Tívose en conta a frecuencia e o esquema de rotación.
- CA3.7. Realizáronse copias de seguridade seguindo diversas estratexias.
- CA3.8. Identificáronse as características dos medios de almacenaxe remotos e extraíbles.
- CA3.9. Utilizáronse medios de almacenaxe remotos e extraíbles.
- CA3.10. Creáronse e restauráronse imaxes de apoio de sistemas en funcionamento.
Dispositivos de almacenaxe:
- ◊ Almacenaxe da información: rendemento, dispoñibilidade e accesibilidade.
- ◊ Almacenaxe redundante e distribuída.
- ◊ Almacenaxe remota e extraíble.
- ◊ Copias de seguridade e imaxes de respaldo.
- ◊ Medios de almacenaxe.

1.5 RA4. Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático

- CA4.1. Seguíronse plans de continxencia para actuar ante fallos de seguridade.
- CA4.2. Clasificáronse os principais tipos de software malicioso.
- CA4.3. Empregáronse ferramentas que examinan a integridade do sistema, e ferramentas de control e

seguimento de accesos.

- CA4.4. Realizáronse actualizacións periódicas dos sistemas para corrixir posibles vulnerabilidades.
- CA4.5. Verificouse a orixe e a autenticidade das aplicacións que se instalan nos sistemas.
- CA4.6. Instaláronse, probáronse e actualizáronse aplicacións específicas para a detección e a eliminación

de software malicioso.

- CA4.7. Aplicáronse técnicas de recuperación de datos.
Mecanismos de seguridade lóxica:
- ◊ Listas de control de acceso.
- ◊ Política de contrasinais.
- ◊ Sistemas biométricos de identificación.
- ◊ Recuperación de datos.
- ◊ Monitorización de sistemas.
- ◊ Auditorías de seguridade.
- ◊ Software malicioso: clasificación. Ferramentas de protección e desinfección.
- ◊ Actualización de sistemas e aplicacións.
- ◊ Manual de seguridade e plans de continxencia.

1.6 RA5. Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico

- CA5.1. Identificouse a necesidade de inventariar e controlar os servizos de rede.
- CA5.2. Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas e nos roubos

de información.

- CA5.3. Deduciuse a importancia de reducir o volume de tráfico xerado pola publicidade e o correo non desexado.
- CA5.4. Aplicáronse medidas para evitar a monitorización de redes con cables.
- CA5.5. Identificáronse as ameazas na navegación pola internet.
- CA5.6. Clasificáronse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.

- CA5.7. Describíronse e utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.
- CA5.8. Instalouse e configurouse un tornalumes (firewall) nun equipamento ou nun servidor.

Medidas de seguridade en redes:

- ◊ Métodos para asegurar a privacidade da información transmitida.
- ◊ Identificación dixital: sinatura electrónica e certificado dixital.
- ◊ Monitorización do tráfico en redes con cables.
- ◊ Seguridade en redes sen fíos.
- ◊ Riscos potenciais dos servizos de rede.
- ◊ Sistemas de seguridade nas telecomunicacións: correo, www, ftp, p2p, etc.
- ◊ Publicidade e correo non desexados.
- ◊ Fraudes informáticas e roubos de información.
- ◊ Utilización de devasas (firewalls) en equipamentos e en servidores.
- ◊ Análise dos rexistros (logs) dun sistema para identificar ataques reais ou potenciais á seguridade.

1.7 RA6. Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento

- CA6.1. Describiuse a lexislación sobre protección de datos de carácter persoal.
- CA6.2. Determinouse a necesidade de controlar o acceso á información persoal almacenada.
- CA6.3. Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
- CA6.4. Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.
- CA6.5. Describiuse a lexislación sobre os servizos da sociedade da información e o comercio electrónico.
- CA6.6. Contrastáronse as normas sobre xestión de seguridade da información.
- CA6.7. Comprendeuse a necesidade de coñecer e respectar a normativa aplicable.

Cumprimento da lexislación e das normas sobre seguridade:

- ◊ Lexislación sobre protección de datos.
- ◊ Lexislación sobre os servizos da sociedade da información e o correo electrónico.
- ◊ Normas ISO sobre xestión de seguridade da información.