CL2003 – *Fundamentos de ciberseguridad (GS).*

Ciclos formativos para los que se oferta:

- CFGS Desarrollo de aplicaciones web.
- CFGS Desarrollo de aplicaciones multiplataforma.
- CFGS Administración de sistemas informáticos en red.

Duración y curso: 54 horas, 2º curso.

Objeto:

Capacitar al alumnado para identificar y aplicar medidas de protección básicas frente a las principales amenazas de seguridad en sistemas, redes y aplicaciones informáticas.

Resultados de aprendizaje y criterios de evaluación:

1. Identifica las principales amenazas y vulnerabilidades en sistemas, redes y aplicaciones informáticas, relacionándolas con sus posibles consecuencias.

   Criterios de evaluación:

   a) Se han descrito las características y funciones de las principales amenazas informáticas, como malware, phishing, ransomware y ataques de denegación de servicio, entre otros.
   b) Se han clasificado las vulnerabilidades más comunes en sistemas operativos, redes y aplicaciones, justificando su impacto potencial en la seguridad.
   c) Se han relacionado las amenazas identificadas con las vulnerabilidades que explotan, explicando los mecanismos utilizados por los atacantes.
   d) Se han evaluado las consecuencias de las amenazas de seguridad sobre la confidencialidad, integridad y disponibilidad de los datos y servicios en casos específicos.
   e) Se han distinguido entre las diferentes categorías de ataques (internos, externos, dirigidos, masivos) según el contexto y los objetivos del atacante.
   f) Se han identificado las señales y síntomas que podrían indicar la presencia de amenazas o vulnerabilidades activas en un sistema o red.

2. Implementa medidas de protección básicas, como configuraciones seguras, control de accesos y políticas de gestión de contraseñas en sistemas operativos y redes.

   Criterios de evaluación:

   a) Se han configurado sistemas operativos y redes aplicando configuraciones seguras, incluyendo la desactivación de servicios innecesarios y la actualización de software a versiones seguras.
   b) Se han aplicado políticas de gestión de contraseñas robustas, asegurando el uso de requisitos mínimos de longitud, complejidad y periodicidad de cambio.
   c) Se han establecido controles de acceso adecuados mediante la creación de roles y permisos, garantizando que los usuarios solo accedan a los recursos necesarios.
   d) Se han implementado reglas básicas de firewall para restringir el tráfico no deseado y proteger los sistemas frente a accesos no autorizados.
   e) Se han utilizado herramientas de monitoreo y auditoría para verificar el cumplimiento de las medidas de protección implementadas.

f) Se han detectado configuraciones inseguras o inconsistentes, proponiendo y ejecutando las correcciones necesarias.
g) Se han documentado los procedimientos seguidos para la implementación de las medidas de protección, incluyendo las configuraciones aplicadas y las herramientas utilizadas.

3. Analiza casos prácticos de incidentes de seguridad informática, proponiendo soluciones adecuadas para su prevención y mitigación.

   Criterios de evaluación:

   a) Se han descrito los elementos clave de un incidente de seguridad, identificando las amenazas, las vulnerabilidades explotadas y las consecuencias del ataque.
   b) Se han clasificado los incidentes de seguridad analizados según su naturaleza, como ataques internos, externos, dirigidos o masivos, justificando la clasificación.
   c) Se han identificado los indicadores de compromiso (IoC) presentes en los casos prácticos, relacionándolos con los métodos y técnicas utilizadas por los atacantes.
   d) Se han propuesto soluciones viables para prevenir futuros incidentes, justificando las medidas de protección recomendadas.
   e) Se ha evaluado el impacto de las soluciones propuestas en términos de mitigación de riesgos, costes y viabilidad.
   f) Se han elaborado informes detallados sobre los incidentes analizados, destacando las causas, el impacto y las medidas correctivas.
   g) Se han aplicado metodologías de análisis forense básicas para recopilar y documentar evidencias en los casos prácticos, respetando los principios éticos y legales.

4. Configura herramientas y tecnologías específicas de ciberseguridad, como cortafuegos, sistemas de detección de intrusos y software antivirus, asegurando su adecuado funcionamiento.

   Criterios de evaluación:

   a) Se han instalado y configurado cortafuegos, definiendo reglas de tráfico que limiten accesos no autorizados y protejan los sistemas frente a amenazas externas.
   b) Se han configurado sistemas de detección de intrusos (IDS) y/o sistemas de prevención de intrusos (IPS), ajustando parámetros para identificar y mitigar posibles ataques.
   c) Se han implantado software antivirus y antimalware, asegurando su actualización y definiendo políticas de escaneo adecuadas a las necesidades del sistema.
   d) Se han optimizado las configuraciones de las herramientas de ciberseguridad, comprobando su integración y compatibilidad con los sistemas existentes.
   e) Se han realizado pruebas funcionales para verificar el correcto funcionamiento de las herramientas configuradas, simulando escenarios de ataque y evaluando su efectividad.
   f) Se ha documentado el proceso de configuración de cada herramienta, incluyendo los parámetros establecidos, los cambios realizados y las recomendaciones de uso para su mantenimiento.

5. Aplica normativas y buenas prácticas en la gestión de la seguridad de la información, respetando los principios de confidencialidad, integridad y disponibilidad.

Criterios de evaluación:

a) Se han identificado e interpretado las normativas y estándares internacionales más relevantes en ciberseguridad, como el RGPD (Reglamento General de Protección de Datos de la UE), ISO/IEC 2701 y ENS (Esquema Nacional de Seguridad), explicando su aplicación en distintos contextos.
b) Se han analizado escenarios prácticos para evaluar si las medidas de seguridad implementadas cumplen con los principios de confidencialidad, integridad y disponibilidad de la información.
c) Se han aplicado buenas prácticas de gestión de la seguridad de la información, como la clasificación de datos sensibles y la definición de políticas de acceso.
d) Se ha evaluado la efectividad de las políticas y procedimientos implementados, proponiendo mejoras basadas en los principios de gestión de riesgos.
e) Se ha elaborado documentación que describa los procedimientos utilizados para garantizar el cumplimiento normativo y las buenas prácticas, detallando los roles y responsabilidades asociados.

Contenidos:

1. Amenazas y vulnerabilidades informáticas.

a) Introducción a las amenazas y vulnerabilidades informáticas: conceptos básicos, diferencias entre amenazas activas y pasivas y su impacto, principios de confidencialidad, integridad y disponibilidad.
b) Clasificación y características de las principales amenazas informáticas: Tipos de *malware*. Técnicas de ingeniería social. Ataques a la red: (DoS y DDoS) y (Man-in-the-Middle). *Exploits* y ataques a aplicaciones web: Inyección SQL y Cross-Site Scripting (XSS).
c) Clasificación de vulnerabilidades en sistemas, redes y aplicaciones. Vulnerabilidades en sistemas operativos, aplicaciones y redes. Redes inalámbricas sin cifrar o con cifrados obsoletos.
d) Relación entre amenazas y vulnerabilidades. Mecánica de explotación: identificación de vulnerabilidades por los atacantes. Uso de *Exploits* y herramientas automatizadas. Ejemplos prácticos de explotación: ransomware en sistemas desactualizados e inyección SQL.
e) Evaluación de las consecuencias de las amenazas y vulnerabilidades. Impacto sobre la confidencialidad, la integridad y la disponibilidad.
f) Señales y síntomas de amenazas y vulnerabilidades activas. Detección de actividad sospechosa en sistemas. Señales de actividad maliciosa en redes.

2. Medidas de protección básicas.

a) Importancia de las configuraciones seguras en la ciberseguridad. Conceptos básicos: servicios innecesarios, actualizaciones y vulnerabilidades conocidas. Procedimientos para desactivar servicios innecesarios en sistemas operativos. Herramientas para gestionar actualizaciones y parches de seguridad.
b) Gestión de contraseñas robustas. Características de una contraseña segura. Políticas de gestión de contraseñas. Métodos de autenticación alternativos: autenticación Multifactor (MFA).

c) Control de accesos y permisos. Principios de control de acceso. Gestión de roles y permisos en sistemas operativos. Configuración de accesos en redes.
d) Implementación de reglas de firewall. Reglas básicas para controlar el tráfico: filtrado de puertos y protocolos y bloqueo de tráfico no autorizado. Configuración de cortafuegos en sistemas operativos y routers. Verificación y pruebas de las reglas implementadas.
e) Herramientas de monitoreo y auditoría. Importancia del monitoreo en la ciberseguridad. Métodos para analizar registros y detectar incidentes o anomalías. Automatización del monitoreo mediante herramientas específicas.
f) Corrección de configuraciones inseguras. Identificación de configuraciones inseguras o inconsistentes. Proceso de propuesta y ejecución de mejoras. Pruebas posteriores a la corrección para validar los cambios.
g) Documentación de medidas de protección implementadas. Importancia de la documentación en la seguridad informática. Estructura recomendada para documentar configuraciones y procedimientos. Uso de plantillas para la documentación eficiente.

3. Análisis de los incidentes de seguridad.

a) Concepto y clasificación de los incidentes de seguridad. Ciclo de vida de un incidente: detección, análisis, contención, erradicación, recuperación y aprendizaje. Elementos clave de un incidente: amenazas, vulnerabilidades y consecuencias.
b) Clasificación de incidentes de seguridad. Tipos de incidentes: internos, externos, dirigidos y masivos. Criterios para clasificar los incidentes: naturaleza, alcance y objetivo.
c) Indicadores de compromiso (IoC). Definición y tipos de IoC: basados en red, basados en sistema y basados en registros. Métodos para identificar IoC en sistemas y redes. Relación entre IoC y las técnicas de ataque utilizadas.
d) Estrategias proactivas para prevenir incidentes de seguridad: configuración de firewalls y herramientas de detección de intrusos e implementación de controles de acceso y gestión de contraseñas. Justificación de las medidas propuestas.
e) Evaluación del impacto de soluciones propuestas. Análisis de mitigación de riesgos. Consideraciones de coste-beneficio en las soluciones. Viabilidad técnica y operativa de las medidas implementadas.
f) Elaboración de informes sobre incidentes. Herramientas y formatos para la redacción de informes. Buenas prácticas en la comunicación de hallazgos técnicos.
g) Conceptos básicos del análisis forense: recopilación de evidencias digitales y preservación de la cadena de custodia. Técnicas fundamentales de análisis forense en sistemas y redes. Principios éticos y legales en la gestión de evidencias: cumplimiento normativo y privacidad y confidencialidad.

4. Herramientas y tecnologías de aplicación.

a) Introducción a las herramientas de ciberseguridad. Concepto y tipos. Funciones principales de cortafuegos, IDS/IPS, y software antivirus. Importancia de la configuración adecuada para la protección de sistemas.
b) Cortafuegos (firewalls). Tipos de cortafuegos: basados en red y cortafuegos basados en host. Instalación de cortafuegos: configuración básica y configuración avanzada. Pruebas funcionales.

c) Sistemas de detección y prevención de intrusos (IDS/IPS). Diferencias entre IDS y IPS. Instalación de IDS/IPS. Configuración de parámetros básicos. Ajustes avanzados. Verificación del funcionamiento.
d) Software antivirus y antimalware. Funciones y tipos de software antivirus. Instalación de software antivirus. Configuración inicial. Actualización de bases de datos y software. Validación del software antivirus: pruebas de detección y generación de informes.
e) Optimización de configuraciones y compatibilidad. Integración de herramientas de ciberseguridad con sistemas operativos y redes. Ajuste de configuraciones para maximizar el rendimiento. Resolución de conflictos entre herramientas y sistemas existentes.
f) Pruebas de efectividad de las herramientas configuradas. Métodos para simular escenarios de ataque. Evaluación de la respuesta de las herramientas ante amenazas simuladas. Identificación y resolución de configuraciones ineficientes o erróneas.
g) Documentación del proceso de configuración. Elementos básicos de la documentación técnica. Uso de plantillas para registrar procedimientos de instalación y configuración. Recomendaciones de mantenimiento y actualización.

5. Normativa y buenas prácticas de uso.

a) Concepto y objetivos de la seguridad de la información. Principios fundamentales: confidencialidad, integridad y disponibilidad. Importancia del cumplimiento normativo y las buenas prácticas en entornos profesionales.
b) Normativas y estándares internacionales en ciberseguridad. Reglamento General de Protección de Datos (RGPD). ISO/IEC 2701. Esquema Nacional de Seguridad (ENS).
c) Buenas prácticas en la gestión de la seguridad de la información. Clasificación de datos sensibles. Definición de políticas de acceso. Gestión del ciclo de vida de la información.
d) Evaluación de medidas de seguridad en escenarios prácticos. Análisis de casos. Uso de herramientas de auditoría. Diagnóstico de fallos. Propuestas de mejora.
e) Gestión de riesgos y mejora continua. Identificación de riesgos. Evaluación de riesgos. Desarrollo de planes de acción. Importancia de la revisión y actualización de las políticas de seguridad.
f) Documentación de la gestión de la seguridad de la información. Elaboración de procedimientos y políticas. Registro de incidencias y cumplimiento normativo. Uso de plantillas y formatos estándares para la documentación. Comunicación efectiva de las políticas y procedimientos a los usuarios.

Especialidades del Profesorado:

- Cuerpo/s: 0511/0590 Catedráticos/Profesores de enseñanza secundaria - Especialidad: 107 - Informática.
- Cuerpo/s: 0590/0591 Profesores de enseñanza secundaria/Profesores técnicos de formación profesional (a extinguir) - Especialidad: 227 - Sistemas y aplicaciones informáticas.
- Para la impartición del módulo optativo «Fundamentos de ciberseguridad (GS)» en centros de titularidad privada o de titularidad pública de otras administraciones distintas de las educativas, se exigirán las mismas condiciones de formación inicial que para

impartir cualquiera de los módulos que incluyan estándares de competencia adscritos a la misma familia profesional que el correspondiente título.