CVE-DOGC-B-22284035-2022

OTRAS DISPOSICIONES

DEPARTAMENTO DE EDUCACIÓN

RESOLUCIÓN EDU/3073/2022, de 3 de octubre, por la que se establece el currículo del curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información.

La ley orgánica 2/2006, de 3 de mayo, de educación, establece en el artículo 39.3, que los cursos de especialización forman parte de la formación profesional, en el artículo 42 que tienen carácter modular y cuya función es la de complementar o profundizar en las competencias de quienes ya dispongan de un título de formación profesional o cumplan las condiciones de acceso que para cada curso de especialización se determinen.

El Real decreto 479/2020, de 7 de abril, ha establecido el Curso de especialización en Ciberseguridad en Entornos de las Tecnologías de la Información y ha fijado los aspectos básicos del currículo.

Por tanto y para establecer el currículo del curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información.

Resuelvo:

-1 Detallar, en el anexo 1, la identificación del curso de especialización.

-2 Detallar, en el anexo 2, el acceso al curso de especialización.

-3 Establecer, en el anexo 3, la relación de módulos profesionales y unidades formativas que conforman el currículo del curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información.

-4 El resto de elementos que definen este curso de especialización (perfil profesional, entorno profesional, prospectiva en el sector o sectores, objetivos generales, espacios y equipamientos y profesorado), son los establecidos en el Real decreto 479/2020, de 7 de abril.

-5 De acuerdo con lo previsto en la disposición adicional segunda del Real decreto 479/2020, de 7 de abril, este curso de especialización no constituye una regulación del ejercicio de ninguna profesión regulada.

Contra esta Resolución, que pone fin a la vía administrativa, las personas interesadas pueden interponer recurso contencioso administrativo ante la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Cataluña, en el plazo de dos meses a contar desde el día siguiente de su publicación en el Diari Oficial de la Generalitat de Catalunya, de conformidad con lo previsto en el artículo 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa. También podrá interponer cualquier otro recurso que estime conveniente para la defensa de sus intereses.

Asimismo, previo al recurso contencioso administrativo, pueden interponer recurso de reposición ante el consejero de Educación, en el plazo de un mes a contar desde el día siguiente de su publicación en el DOGC, según lo dispuesto en el artículo 77 de la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña y los artículos 123 y 124 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, o cualquier otro recurso que consideren conveniente para la defensa de sus intereses.

CVE-DOGC-B-22284035-2022

Barcelona, 3 de octubre de 2022

Josep Gonzàlez Cambray

Consejero de Educación

Anexo 1

Identificación.

El curso de especialización en Ciberseguridad en Entornos de las Tecnologías de la Información queda identificado por los siguientes elementos:

Denominación: Ciberseguridad en Entornos de las Tecnologías de la Información.

Nivel: Formación Profesional de Grado Superior.

Duración: 720 horas.

Familia Profesional: Informática y Comunicaciones (únicamente a efectos de clasificación de las enseñanzas de formación profesional).

Ramas de conocimiento: Ingeniería y Arquitectura

Créditos ECTS: 43.

Referente a la Clasificación Internacional Normalizada de la Educación: P-5.5.4.

Anexo 2

Acceso al curso de especialización.

Los títulos que dan acceso a este curso de especialización son los siguientes:

Título de Técnico o Técnica superior en Administración de Sistemas Informáticos en Red, establecido por el Real decreto 1629/2009, de 30 de octubre.

Título de Técnico o Técnica superior en Desarrollo de Aplicaciones Multiplataforma, establecido por el Real decreto 450/2010, de 16 de abril.

Título de Técnico o Técnica superior en Desarrollo de Aplicaciones Web, establecido por el Real decreto 686/2010, de 20 de mayo.

Título de Técnico o Técnica Superior en Sistemas de Telecomunicaciones e Informáticos, establecido por el Real decreto 883/2011, de 24 de junio.

Título de Técnico o Técnica Superior en Mantenimiento Electrónico, establecido por Real decreto 1578/2011, de 4 de noviembre.

CVE-DOGC-B-22284035-2022

Anexo 3

Relación de módulos profesionales y unidades formativas.

Módulo profesional 1: Incidentes de Ciberseguridad

Duración: 99 horas

Equivalencia en créditos ECTS: 9

Unidades formativas que lo componen:

UF 1: incidentes de ciberseguridad. 99 horas

Módulo profesional 2: Bastionado de Redes y Sistemas

Duración: 132 horas

Equivalencia en créditos ECTS: 10

Unidades formativas que lo componen:

UF 1: bastionado de redes y sistemas. 132 horas

Módulo profesional 3: Puesta en Producción Segura

Duración: 99 horas

Equivalencia en créditos ECTS: 7

Unidades formativas que lo componen:

UF 1: puesta en producción segura. 99 horas

Módulo profesional 4: Análisis Forense Informático

Duración: 99 horas

Equivalencia en créditos ECTS: 7

Unidades formativas que lo componen:

UF 1: análisis forense informático. 99 horas

Módulo profesional 5: *Hacking* Ético

Duración: 99 horas

Equivalencia en créditos ECTS: 7

Unidades formativas que lo componen:

UF 1: *hacking* ético. 99 horas

Módulo profesional 6: Normativa de Ciberseguridad

Duración: 66 horas

Equivalencia en créditos ECTS: 3

Unidades formativas que lo componen:

CVE-DOGC-B-22284035-2022

UF 1: normativa de ciberseguridad. 66 horas

Módulo profesional 7: Formación en Centros de Trabajo

Duración: 126 horas

Descripción de los módulos profesionales y de las unidades formativas

Módulo profesional 1: Incidentes de Ciberseguridad

Duración: 99 horas

Equivalencia en créditos ECTS: 9

Unidades formativas que lo componen:

UF 1: incidentes de ciberseguridad. 99 horas

UF 1: incidentes de ciberseguridad

Duración: 99 horas

Resultados de aprendizaje y criterios de evaluación

1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.

Criterios de evaluación

1.1 Define los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección.

1.2 Establece una normativa de protección del puesto de trabajo.

1.3 Define un plan de concienciación de ciberseguridad dirigido a los empleados.

1.4 Desarrolla el material necesario para realizar las acciones de concienciación dirigidas a los empleados.

1.5 Realiza una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.

Criterios de evaluación

2.1 Clasifica y define la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.

2.2 Establece controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de

CVE-DOGC-B-22284035-2022

incidentes.

2.3 Establece controles y mecanismos de detección e identificación de incidentes de seguridad física.

2.4 Establece controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: *Open Source Intelligence*).

2.5 Realiza una clasificación, valoración, documentación y seguimiento de los incidentes detectados en la organización.

2.6 Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.

3. Recopila y almacena de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.

Criterios de evaluación

3.1 Realiza un análisis de evidencias.

3.2 Realiza la investigación de incidentes de ciberseguridad.

3.3 Intercambia información de incidentes, con proveedores y/u organismos competentes que podrían realizar aportaciones al respecto.

3.4 Inicia las primeras medidas de contención de los incidentes para limitar los posibles daños causados.

3.5 Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las adecuadas técnicas de protección.

4. Desarrolla procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.

Criterios de evaluación

4.1 Prepara respuestas ciberresilientes frente a incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.

4.2 Establece un flujo de toma de decisiones y escalado de incidentes interno y externo adecuados.

4.3 Lleva a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.

4.4 Documenta las acciones realizadas y las conclusiones que permitan mantener un registro de "lecciones aprendidas".

4.5 Realiza un adecuado seguimiento del incidente para evitar que una situación similar se vuelva a repetir.

4.6 Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.

5. Desarrolla un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.

Criterios de evaluación

CVE-DOGC-B-22284035-2022

5.1 Notifica el incidente de forma adecuada al personal interno de la organización responsable de la toma de decisiones.

5.2 Notifica el incidente de forma adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.

5.3 Notifica formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.

5.4 Notifica el incidente en los medios de comunicación en caso de ser necesario.

Contenidos

1. Desarrollo de planes de prevención y concienciación en ciberseguridad:

1.1 Principios generales en materia de ciberseguridad.

1.2 Normativa de protección del puesto de trabajo.

1.3 Plan de formación y concienciación en materia de ciberseguridad.

1.4 Materiales de formación y concienciación.

1.5 Auditorías internas de cumplimiento en materia de prevención.

2. Auditoría de incidentes de ciberseguridad:

2.1 Taxonomía de incidentes de ciberseguridad.

2.2 Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes.

2.3 Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física.

2.4 Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT).

2.5 Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.

3. Investigación de los incidentes de ciberseguridad:

3.1 Recopilación de evidencias.

3.2 Análisis de evidencias.

3.3 Investigación del incidente.

3.4 Intercambio de información del incidente con proveedores u organismos competentes.

3.5 Medidas de contención de incidentes.

4. Implementación de medidas de ciberseguridad:

4.1 Desarrollo de procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.

4.2 Implantación de capacidades de ciberresiliencia.

4.3 Establecimiento de flujos de toma de decisiones y escalado interno y/o externo adecuados.

4.4 Tareas para restablecer los servicios afectados por incidentes.

CVE-DOGC-B-22284035-2022

4.5 Documentación.

4.6 Seguimiento de incidentes para evitar una situación similar.

5. Detección y documentación de incidentes de ciberseguridad:

5.1 Desarrollo de procedimientos de actuación para la notificación de incidentes.

5.2 Notificación interna de incidentes.

5.3 Notificación de incidentes a los que corresponda.

Módulo profesional 2: Bastionado de Redes y Sistemas

Duración: 132 horas

Equivalencia en créditos ECTS: 10

Unidades formativas que lo componen:

UF 1: bastionado de redes y sistemas. 132 horas

UF 1: bastionado de redes y sistemas

Duración: 132 horas

Resultados de aprendizaje y criterios de evaluación

1. Diseña planes de securización incorporando buenas prácticas para el endurecimiento de sistemas y redes.

Criterios de evaluación

1.1 Identifica los activos, amenazas y vulnerabilidades de la organización.

1.2 Evalúa las medidas de seguridad actuales.

1.3 Elabora un análisis de riesgo de la situación actual en ciberseguridad de la organización.

1.4 Prioriza las medidas técnicas de seguridad a implantar en la organización teniendo en cuenta también los principios de la Economía Circular.

1.5 Diseña y elabora un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un adecuado nivel de seguridad en función de los riesgos de la organización.

1.6 Identifica las mejores prácticas en base a estándares, guías y políticas de seguridad adecuadas para el fortalecimiento de los sistemas y redes de la organización.

2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.

Criterios de evaluación

CVE-DOGC-B-22284035-2022

2.1 Define los mecanismos de autenticación en base a diferentes/múltiples factores (físicos, inherentes y basados en el conocimiento) existentes.

2.2 Define protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.

2.3 Define protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.

2.4 Define protocolos y políticas de autenticación basados en *tokens*, *OTPs*, etc., en base a las principales vulnerabilidades y tipos de ataques.

2.5 Define protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.

3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.

Criterios de evaluación

3.1 Identifica los tipos de credenciales más usados.

3.2 Genera y utiliza distintos certificados digitales como medio de acceso a un servidor remoto.

3.3 Comprueba la validez y autenticidad de un certificado digital de un servicio web.

3.4 Compara certificados digitales válidos e inválidos por distintos motivos.

3.5 Instala y configura un servidor seguro para la administración de credenciales (tipo *RADIUS - Remote Access Dial In User Service*).

4. Diseña redes de computadores contemplando los requisitos de seguridad.

Criterios de evaluación

4.1 Incrementa el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.

4.2 Optimiza una red local plana utilizando técnicas de segmentación lógica (*VLANs*).

4.3 Adapta un segmento de una red local ya operativo utilizando técnicas de *subnetting* para incrementar su segmentación respetando los direccionamientos existentes.

4.4 Configura las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (enrutadores, puntos de acceso, etc.).

4.5 Establece un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.

5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.

Criterios de evaluación

5.1 Configura dispositivos de seguridad perimetral de acuerdo con una serie de requisitos de seguridad.

CVE-DOGC-B-22284035-2022

5.2 Detecta errores de configuración de dispositivos de red mediante el análisis de tráfico.

5.3 Identifica comportamientos no deseados en una red a través del análisis de los registros (*Logs*), de un cortafuegos.

5.4 Implementa contramedidas frente a comportamientos no deseados en una red.

5.5 Caracteriza, instala y configura diferentes herramientas de monitorización.

6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación

6.1 Configura la *BIOS* para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.

6.2 Prepara un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.

6.3 Configura un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.

6.4 Instala un sistema informático utilizando sus capacidades de cifrado del sistema de archivos para evitar la extracción física de datos.

6.5 Realiza particiones del sistema de archivos de sistema informático para minimizar riesgos de seguridad.

7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación

7.1 Enumera y elimina los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.

7.2 Configura las características propias de sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.

7.3 Incrementa la seguridad de sistema de administración remoto *SSH* y otros.

7.4 Instala y configura un sistema de detección de intrusos en un *Host* (*HIDS*) en el sistema informático.

7.5 Instala y configura sistemas de copias de seguridad.

Contenidos

1. Diseño de planes de securización:

1.1 Análisis de riesgos.

1.2 Principios de la economía circular en la industria 4.0.

1.3 Plan de medidas técnicas de seguridad.

1.4 Políticas de securización más habituales.

CVE-DOGC-B-22284035-2022

1.5 Guías de buenas prácticas para la securización de sistemas y redes.

1.6 Estándares de securización de sistemas y redes.

1.7 Caracterización de procedimientos, instrucciones y recomendaciones.

1.8 Niveles, escalados y protocolos de atención a incidencias.

2. Configuración de sistemas de control de acceso y autenticación de personas:

2.1 Mecanismos de autenticación. Tipos de factores.

2.2 Autenticación basada en diferentes técnicas.

3. Administración de credenciales de acceso a sistemas informáticos:

3.1 Gestión de credenciales.

3.2 Infraestructuras de Clave Pública (*PKI*).

3.3 Acceso por medio de Firma electrónica.

3.4 Gestión de accesos. Sistemas *NAC* (*Network Access Control* , *Sistemas de Gestión de Acceso a la Red*).

3.5 Gestión de cuentas privilegiadas.

3.6 Protocolos *RADIVOS* y *MANCHAS*, servicio *Kerberos*, entre otros.

4. Diseño de redes de computadores seguras:

4.1 Segmentación de redes.

4.2 *Subnetting*.

4.3 Redes virtuales (*VLANs*).

4.4 Zona desmilitarizada (*DMZ*).

4.5 Seguridad en redes inalámbricas (*WPA2*, *WPA3*, etc.).

4.6 Protocolos de red segura (*IPSec*, etc.).

5. Configuración de dispositivos y sistemas informáticos:

5.1 Seguridad perimetral. Cortafuegos de Próxima Generación.

5.2 Seguridad de portales y aplicaciones web. Soluciones *WAF* (*Web Aplication Firewall*).

5.3 Seguridad del puesto de trabajo y *endpoint* fijo y móvil. *AntiAPT*, antimalware.

5.4 Seguridad de entornos *cloud*. Soluciones *CASB*.

5.5 Seguridad del correo electrónico.

5.6 Soluciones *DLP* (*Data Loss Prevention*).

5.7 Herramientas de almacenamiento de *logs*.

5.8 Protección ante ataques de denegación de servicio distribuido (*DDoS*).

5.9 Configuración segura de cortafuegos, routers y proxies.

5.10 Redes privadas virtuales (*VPNs*), y túneles (protocolo *IPSec*).

5.11 Monitorización de sistemas y dispositivos.

CVE-DOGC-B-22284035-2022

5.12 Herramientas de monitorización (*IDS*, *IPS*).

5.13 *SIEMs* (Gestores de Eventos e Información de Seguridad).

5.14 Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: *NOCs* y *SOCs*.

6. Configuración de dispositivos para la instalación de sistemas informáticos:

6.1 Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la *BIOS*, bloqueo del orden de arranque de los dispositivos, entre otros.

6.2 Seguridad en el arranque de sistema informático, configuración del arranque seguro.

6.3 Seguridad de los sistemas de archivos, cifrado, partición, entre otros.

7. Configuración de los sistemas informáticos:

7.1 Reducción del número de servicios, *Telnet*, *RSSH*, *TFTP*, entre otros.

7.2 *Hardening* de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar *exploits*, etc.).

7.3 Eliminación de protocolos de red innecesarios (*ICMP*, entre otros).

7.4 Securización de los sistemas de administración remota.

7.5 Sistemas de prevención y protección frente a virus e intrusiones (antivirus, *HIDS*, etc.).

7.6 Configuración de actualizaciones y parches automáticos.

7.7 Sistemas de copias de seguridad.

7.8 *Shadow IT* y políticas de seguridad en entornos *SaaS* .

Módulo profesional 3: Puesta en Producción Segura

Duración: 99 horas

Equivalencia en créditos ECTS: 7

Unidades formativas que lo componen:

UF 1: puesta en producción segura. 99 horas

UF 1: puesta en producción segura

Duración: 99 horas

Resultados de aprendizaje y criterios de evaluación

1. Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.

Criterios de evaluación

CVE-DOGC-B-22284035-2022

1.1 Compara distintos lenguajes de programación de acuerdo con sus características principales.

1.2 Describe los distintos modelos de ejecución de software.

1.3 Reconoce los elementos básicos de la fuente, dándoles significado.

1.4 Ejecuta distintos tipos de prueba de software.

1.5 Evalúa los lenguajes de programación de acuerdo con la infraestructura de seguridad que proporcionan.

2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.

Criterios de evaluación

2.1 Caracteriza los niveles de verificación de seguridad en aplicaciones establecidas por los estándares internacionales (*ASVS*, "*Application Security Verification Standard*").

2.2 Identifica el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo con estándares reconocidos.

2.3 Enumera los requisitos de verificación necesarios asociados al nivel de seguridad establecido.

2.4 Reconoce los principales riesgos de las aplicaciones desarrolladas en función de sus características.

3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.

Criterios de evaluación

3.1 Valida las entradas de los usuarios.

3.2 Detecta riesgos de inyección tanto en el servidor como en el cliente.

3.3 Gestiona correctamente la sesión del usuario durante el uso de la aplicación.

3.4 Utiliza roles para el control de acceso.

3.5 Usa algoritmos criptográficos seguros para almacenar las contraseñas de usuario.

3.6 Configura servidores web para reducir el riesgo de sufrir ataques conocidos.

3.7 Incorpora medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (*bots*).

4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando archivos y datos.

Criterios de evaluación

4.1 Compara los distintos modelos de permisos de las plataformas móviles.

4.2 Describe técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.

CVE-DOGC-B-22284035-2022

4.3 Implanta un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.

4.4 Utiliza herramientas de monitoreo de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.

4.5 Inspecciona binarios de aplicaciones móviles para buscar fugas de información sensible.

5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.

Criterios de evaluación

5.1 Identifica las características, principios y objetivos de la integración del desarrollo y la operación de software.

5.2 Implanta sistemas de control de versiones, administrando los roles y permisos solicitados.

5.3 Instala, configura y verifica sistemas de integración continua, conectándolos con sistemas de control de versiones.

5.4 Planifica, implementa y automatiza planes de desplegado de software.

5.5 Evalúa la capacidad del sistema desplegado para reaccionar de forma automática a fallos.

5.6 Documenta las tareas realizadas y los procedimientos a seguir para la recuperación frente a desastres.

5.7 Crea bucles de retroalimentación ágiles entre los miembros del equipo.

Contenidos

1. Prueba de aplicaciones web y para dispositivos móviles:

1.1 Fundamentos de la programación.

1.2 Lenguajes de programación interpretados y compilados.

1.3 Código fuente y entornos de desarrollo.

1.4 Ejecución de software.

1.5 Elementos principales de los programas.

1.6 Pruebas. Tipos.

1.7 Seguridad en los lenguajes de programación y sus entornos de ejecución (*Sandboxes*).

2. Determinación del nivel de seguridad requerido por aplicaciones:

2.1 Fuentes abiertas para desarrollo seguro.

2.2 Listas de riesgos de seguridad habituales: *OWASP Top Ten* (web y móvil).

2.3 Requisitos de verificación necesarios asociados al nivel de seguridad establecido.

2.4 Comprobaciones de seguridad a nivel de aplicación: *ASVS* (*Application Security Verification Standard*).

3. Detección y corrección de vulnerabilidades de aplicaciones web:

CVE-DOGC-B-22284035-2022

3.1 Desarrollo seguro de aplicaciones web.

3.2 Listas públicas de vulnerabilidades de aplicaciones web. *OWASP Top Ten*.

3.3 Entrada basada en formularios. Inyección. Validación de la entrada.

3.4 Estándares de autenticación y autorización.

3.5 Robo de sesión.

3.6 Vulnerabilidades web.

3.7 Almacenamiento seguro de contraseñas.

3.8 Contramedidas. *HSTS*, *CSP*, *CAPTCHAs*, entre otros.

3.9 Seguridad de portales y aplicaciones web. Soluciones *WAF* (*Web Application Firewall*).

4. Detección de problemas de seguridad en aplicaciones para dispositivos móviles:

4.1 Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.

4.2 Firma y verificación de aplicaciones.

4.3 Almacenamiento seguro de datos.

4.4 Validación de compras integradas en la aplicación.

4.5 Fuga de información en los ejecutables.

4.6 Soluciones *CASB*.

5. Implantación de sistemas seguros de desplegado de software:

5.1 Puesta segura en producción.

5.2 Prácticas unificadas para el desarrollo y operación de software (*devops*).

5.3 Sistemas de control de versiones.

5.4 Sistemas de automatización de construcción (*build*).

5.5 Integración continua y automatización de pruebas.

5.6 Escalado de servidores. Virtualización. Contenedores.

5.7 Gestión automatizada de configuración de sistemas.

5.8 Herramientas de simulación de fallos.

5.9 Orquestación de contenedores.

Módulo profesional 4: Análisis Forense Informático

Duración: 99 horas

Equivalencia en créditos ECTS: 7

Unidades formativas que lo componen:

UF 1: análisis forense informático. 99 horas

CVE-DOGC-B-22284035-2022

UF 1: análisis forense informático

Duración: 99 horas

Resultados de aprendizaje y criterios de evaluación

1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.

Criterios de evaluación

1.1 Identifica los dispositivos a analizar para garantizar la preservación de evidencias.

1.2 Utiliza los mecanismos y herramientas adecuadas para la adquisición y extracción de las evidencias.

1.3 Asegura la escena y conserva la cadena de custodia.

1.4 Documenta el proceso realizado de forma metódica.

1.5 Considera la línea temporal de las evidencias.

1.6 Elabora un informe de conclusiones a nivel técnico y ejecutivo.

1.7 Presenta y expone las conclusiones del análisis forense realizado.

2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación

2.1 Realiza el proceso de toma de evidencias en un dispositivo móvil.

2.2 Extrae, decodifica y analiza las pruebas conservando la cadena de custodia.

2.3 Genera informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.

2.4 Presenta y expone las conclusiones del análisis forense realizado a quien proceda.

3. Realiza análisis forenses en *Cloud*, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación

3.1 Desarrolla una estrategia de análisis forense en *Cloud*, asegurando la disponibilidad de los recursos y capacidades necesarios una vez pasado el incidente.

3.2 Consigue identificar las causas, el alcance y el impacto real causado por el incidente.

3.3 Realiza las fases del análisis forense en *Cloud*.

3.4 Identifica las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).

3.5 Cumple con los requerimientos legales en vigor, RGPD (Reglamento general de protección de datos) y

CVE-DOGC-B-22284035-2022

directiva *NIS* (Directiva de la UE sobre seguridad de redes y sistemas de información) o las que eventualmente puedan sustituirlas.

3.6 Presenta y expone las conclusiones del análisis forense realizado.

4. Realiza análisis forense en dispositivos del *IoT*, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación

4.1 Identifica a los dispositivos a analizar garantizando la preservación de las evidencias.

4.2 Utiliza mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias.

4.3 Garantiza la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.

4.4 Realiza análisis de evidencias de forma manual y mediante herramientas.

4.5 Documenta el proceso de forma metódica y detallada.

4.6 Considera la línea temporal de las evidencias.

4.7 Mantiene la cadena de custodia.

4.8 Elabora un informe de conclusiones a nivel técnico y ejecutivo.

4.9 Presenta y expone las conclusiones del análisis forense realizado.

5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.

Criterios de evaluación

5.1 Define el objetivo del informe pericial y su justificación.

5.2 Define el ámbito de aplicación del informe pericial.

5.3 Documenta los antecedentes.

5.4 Recopila las normas legales y reglamentos cumplidos en el análisis forense realizado.

5.5 Recoge los requisitos establecidos por el cliente.

5.6 Incluye conclusiones y justificación.

Contenidos

1. Aplicación de metodologías de análisis forenses:

1.1 Identificación de los dispositivos a analizar.

1.2 Recolección de evidencias (trabajar un escenario).

1.3 Análisis de la línea de tiempo (*TimeStamp*).

1.4 Análisis de volatilidad - Extracción de información (*volatility*).

1.5 Análisis de *Logs*, herramientas más usadas.

CVE-DOGC-B-22284035-2022

2. Realización de análisis forenses en dispositivos móviles:

2.1 Métodos para la extracción de evidencias.

2.2 Herramientas de mercado más comunes.

3. Realización de análisis forenses en *Cloud*:

3.1 Nube privada y nube pública o híbrida.

3.2 Retos legales, organizativos y técnicos particulares de un análisis en *Cloud*.

3.3 Estrategias de análisis forense en *Cloud*.

3.4 Realización de las fases relevantes del análisis forense en *Cloud*.

3.5 Utilización de herramientas de análisis en *Cloud* (*Celebrite UFED Cloud Analizer*, *Cloud Trail*, *Frost*, *OWADE*, ...).

4. Realización de análisis forenses en *IoT*:

4.1 Identificación de los dispositivos a analizar.

4.2 Adquisición y extracción de las evidencias.

4.3 Análisis de las evidencias de forma manual y automática.

4.4 Documentación del proceso realizado.

4.5 Establecimiento de la línea temporal.

4.6 Mantenimiento de la cadena de custodia.

4.7 Elaboración de las conclusiones.

4.8 Presentación y exposición de conclusiones.

5. Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe:

5.1 Hoja de identificación (título, razón social, nombre y apellidos, firma).

5.2 Índice de la memoria.

5.3 Objeto (objetivo del informe pericial y su justificación).

5.4 Alcance (ámbito de aplicación del informe pericial - resumen ejecutivo para una supervisión rápida del contenido y resultados).

5.5 Antecedentes (aspectos necesarios para la comprensión de las alternativas estudiadas y las conclusiones finales).

5.6 Normas y referencias (documentos y normas legales y reglamentos mencionados en los distintos apartados).

5.7 Definiciones y abreviaturas (definiciones, abreviaturas y expresiones técnicas que se han utilizado a lo largo del informe).

5.8 Requisitos (bases y datos de partida establecidos por el cliente, legislación, reglamentación y normativa aplicables).

5.9 Análisis de soluciones – resumen de conclusiones del informe pericial (alternativas estudiadas, qué caminos se han seguido para llegar, ventajas e inconvenientes de cada una y cuál es la solución finalmente elegida y su justificación).

5.10 Anexos.

CVE-DOGC-B-22284035-2022

Módulo profesional 5: *Hacking* Ético

Duración: 99 horas

Equivalencia en créditos ECTS: 7

Unidades formativas que lo componen:

UF 1: *hacking* ético. 99 horas

UF 1:* hacking *ético

Duración: 99 horas

Resultados de aprendizaje y criterios de evaluación

1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de *hacking* ético.

Criterios de evaluación

1.1 Define la terminología esencial del *hacking* ético.

1.2 Identifica los conceptos éticos y legales frente al ciberdelito.

1.3 Define el alcance y las condiciones de un test de intrusión.

1.4 Identifica los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.

1.5 Identifica las fases de un ataque seguidas por un atacante.

1.6 Analiza y define los tipos de vulnerabilidades.

1.7 Analiza y define los tipos de ataque.

1.8 Determina y caracteriza las distintas vulnerabilidades existentes.

1.9 Determina las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.

2. Ataca y defensa en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.

Criterios de evaluación

2.1 Configura los distintos modos de funcionamiento de la tarjeta de red inalámbrica.

2.2 Describe las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.

2.3 Detecta redes inalámbricas y captura tráfico de red como paso previo a su ataque.

2.4 Accede a redes inalámbricas vulnerables.

CVE-DOGC-B-22284035-2022

2.5 Caracteriza otros sistemas de comunicación inalámbrico y sus vulnerabilidades.

2.6 Utiliza técnicas de "Equipo Rojo y Azul".

2.7 Realiza informes sobre las vulnerabilidades detectadas.

3. Ataca y defensa en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.

Criterios de evaluación

3.1 Recopila información sobre la red y sistemas objetivo mediante técnicas pasivas.

3.2 Crea un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.

3.3 Intercepta tráfico de red de terceros para buscar información sensible.

3.4 Realiza un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.

3.5 Compromete sistemas remotos explotando sus vulnerabilidades.

4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

Criterios de evaluación

4.1 Administra sistemas remotos a través de herramientas de línea de órdenes.

4.2 Compromete contraseñas a través de ataques de diccionario, tablas *rainbow* y fuerza bruta contra sus versiones encriptadas.

4.3 Accede a sistemas adicionales a través de sistemas comprometidos.

4.4 Instala puertas traseras para garantizar accesos futuros a los sistemas comprometidos.

5. Ataca y defensa en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.

Criterios de evaluación

5.1 Identifica los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas.

5.2 Realiza un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación Web.

5.3 Analiza el flujo de las interacciones realizadas entre el navegador y la aplicación Web durante su uso normal.

5.4 Examina manualmente aplicaciones web en busca de las vulnerabilidades más habituales.

5.5 Utiliza herramientas de búsqueda y explotación de vulnerabilidades web.

5.6 Realiza la búsqueda y explotación de vulnerabilidades web mediante herramientas software.

CVE-DOGC-B-22284035-2022

Contenidos

1. Determinación de las herramientas de monitorización para detectar vulnerabilidades:

1.1 Elementos esenciales del *hacking* ético.

1.2 Diferencias entre *hacking*, *hacking* ético, test de penetración y hacktivismo.

1.3 Recogida de permisos y autorizaciones previos a un test de intrusión.

1.4 Fases del *hacking*.

1.5 Auditorías de caja negra y de caja blanca.

1.6 Documentación de vulnerabilidades.

1.7 Clasificación de herramientas de seguridad y *hacking*.

1.8 *Clearnet*, *Deep Web*, *Dark web*, *Darknets*. Conocimiento, diferencias y herramientas de acceso: *Tor, ZeroNet*, *freenet*.

2. Ataque y defensa en torno a pruebas, de las comunicaciones inalámbricas:

2.1 Comunicación inalámbrica.

2.2 Modo infraestructura, ad hoc y monitor.

2.3 Análisis y recogida de datos en redes inalámbricas.

2.4 Técnicas de ataques y exploración de redes inalámbricas.

2.5 Ataques a otros sistemas inalámbricos.

2.6 Realización de informes de auditoría y presentación de resultados.

3. Ataque y defensa en torno a pruebas, de redes y sistemas para acceder a sistemas de terceros:

3.1 Fase de reconocimiento (*footprinting*).

3.2 Fase de escaneo (*fingerprinting*).

3.3 Monitorización de tráfico.

3.4 Intercepción de comunicaciones utilizando distintas técnicas.

3.5 Manipulación e inyección de tráfico.

3.6 Herramientas de búsqueda y explotación de vulnerabilidades.

3.7 Ingeniería social. *Phising*.

3.8 Escalada de privilegios.

4. Consolidación y utilización de sistemas comprometidos:

4.1 Administración de sistemas de forma remota.

4.2 Ataques y auditorías de contraseñas.

4.3 Pivotaje en la red.

4.4 Instalación de puertas traseras con troyanos (*RAT*, *Remote Access Trojan*).

CVE-DOGC-B-22284035-2022

5. Ataque y defensa en entorno de pruebas, a aplicaciones web:

5.1 Negación de credenciales en aplicaciones web.

5.2 Recogida de datos.

5.3 Automatización de conexiones a servidores web (ejemplo: *Selenium*).

5.4 Análisis de tráfico a través de proxies de intercepción.

5.5 Búsqueda de vulnerabilidades habituales en aplicaciones web.

5.6 Herramientas para la explotación de vulnerabilidades web.

Módulo profesional 6: Normativa de Ciberseguridad

Duración: 66 horas

Equivalencia en créditos ECTS: 3

Unidades formativas que lo componen:

UF 1: normativa de ciberseguridad. 66 horas

UF 1: normativa de ciberseguridad

Duración: 66 horas

Resultados de aprendizaje y criterios de evaluación

1. Identifica los principales puntos de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.

Criterios de evaluación

1.1 Identifica las bases de cumplimiento normativo a tener en cuenta en las organizaciones.

1.2 Describe y aplica los principios de un buen gobierno y su relación con la ética profesional.

1.3 Define las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del desempeño normativo dentro de las organizaciones.

1.4 Describe las funciones o competencias del responsable del desempeño normativo dentro de las organizaciones.

1.5 Establece las relaciones con terceros para un correcto cumplimiento normativo.

2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.

Criterios de evaluación

CVE-DOGC-B-22284035-2022

2.1 Recoge las principales normativas que afectan a los distintos tipos de organizaciones.

2.2 Establece las recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 19.600 entre otras).

2.3 Realiza análisis y evaluaciones de los riesgos de distintos tipos de organizaciones de acuerdo con la normativa vigente (ISO 31.000 entre otros).

2.4 Documenta el sistema de cumplimiento normativo diseñado.

3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.

Criterios de evaluación

3.1 Identifica los riesgos penales aplicables a distintas organizaciones.

3.2 Implanta las medidas necesarias para eliminar o minimizar los riesgos identificados.

3.3 Establece un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros).

3.4 Determina los principios básicos dentro de las organizaciones para combatir el cohecho y promover una cultura empresarial ética acorde con la legislación y normativa vigente (ISO 37.001 entre otros).

4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.

Criterios de evaluación

4.1 Reconoce las fuentes del Derecho de acuerdo con el ordenamiento jurídico en materia de protección de datos de carácter personal.

4.2 Aplica los principios relacionados con la protección de datos de carácter personal, tanto a nivel nacional como internacional.

4.3 Establece los requisitos necesarios para hacer frente a la privacidad desde las bases del diseño.

4.4 Configura las herramientas corporativas contemplando el cumplimiento normativo por defecto.

4.5 Realiza un análisis de riesgos para el tratamiento de los derechos en la protección de datos.

4.6 Implanta las medidas necesarias para eliminar o minimizar los riesgos identificados en la protección de datos.

4.7 Describe las funciones o competencias del delegado de protección de datos dentro de las organizaciones.

5. Recoge y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.

Criterios de evaluación

5.1 Establece el plan de revisiones de normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.

CVE-DOGC-B-22284035-2022

5.2 Detecta nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.

5.3 Analiza la nueva normativa para determinar si se aplica en la actividad de la organización.

5.4 Incluye en el plan de revisiones las modificaciones necesarias sobre la nueva normativa aplicable a la organización para un correcto cumplimiento normativo.

5.5 Determina e implementa los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones.

Contenidos

1. Puntos principales de aplicación para un correcto cumplimiento normativo:

1.1 Introducción al desempeño normativo (*Compliance*: objetivo, definición y conceptos principales).

1.2 Principios del buen gobierno y ética empresarial.

1.3 *Compliance Officer*: funciones y responsabilidades.

1.4 Relaciones con terceras partes dentro del *Compliance*.

2. Diseño de sistemas de cumplimiento normativo:

2.1 Sistemas de Gestión de *Compliance*.

2.2 Entorno regulador de aplicación.

2.3 Análisis y gestión de riesgos, mapas de riesgos.

2.4 Documentación del sistema de cumplimiento normativo diseñado.

3. Legislación para el cumplimiento de la responsabilidad penal:

3.1. Riesgos penales que afectan a la organización.

3.2. Sistemas de gestión de *Compliance* penal.

3.3. Sistemas de gestión anticorrupción.

4. Legislación y jurisprudencia en materia de protección de datos:

4.1 Principios de protección de datos.

4.2 Novedades del RGPD de la Unión Europea.

4.3 Privacidad por Diseño y por defecto.

4.4 Análisis de Impacto en Privacidad (*PIA*), y medidas de seguridad.

4.5 Delegado de Protección de Datos (DPO).

5. Normativa vigente de ciberseguridad de ámbito nacional e internacional:

5.1 Normas nacionales e internacionales.

5.2 Sistema de Gestión de Seguridad de la Información (estándares internacionales) (ISO 27.001).

5.3 Acceso electrónico de los ciudadanos a los Servicios Públicos. Esquema Nacional de Seguridad (ENS).

5.4 Planes de Continuidad de Negocio (estándares internacionales) (ISO 22.301).

CVE-DOGC-B-22284035-2022

5.5 Directiva *NIS*.

5.6 Legislación sobre la protección de infraestructuras críticas. Ley PIC (Protección de infraestructuras críticas).

Módulo Profesional 7: Formación en Centros de Trabajo

Duración: 126 horas

Resultados de aprendizaje y criterios de evaluación

1. Identifica la estructura, organización y condiciones de trabajo de la empresa, centro o servicio, relacionándolo con las actividades que realiza.

Criterios de evaluación

1.1 Identifica las características generales de la empresa, centro o servicio y el organigrama y funciones de cada área.

1.2 Identifica los procedimientos de trabajo en el desarrollo de la actividad.

1.3 Identifica las competencias de los puestos de trabajo en el desarrollo de la actividad

1.4 Identifica las características del mercado o entorno, tipos de usuarios y proveedores.

1.5 Identifica las actividades de responsabilidad social de la empresa, centro o servicio hacia el entorno.

1.6 Identifica el flujo de servicios o canales de comercialización más frecuentes en esta actividad.

1.7 Relaciona ventajas e inconvenientes de la estructura de la empresa, centro o servicio, frente a otros tipos de organizaciones relacionadas.

1.8 Identifica el convenio colectivo o el sistema de relaciones laborales al que está acogida la empresa, centro o servicio.

1.9 Identifica los incentivos laborales, las actividades de integración o formación y las medidas de conciliación en relación con la actividad.

1.10 Valora las condiciones de trabajo en el clima laboral de la empresa, centro o servicio.

1.11 Valora la importancia de trabajar en grupo para conseguir con eficacia los objetivos establecidos en la actividad y resolver los problemas planteados.

2. Desarrolla actitudes éticas y laborales propias de la actividad profesional de acuerdo con las características del puesto de trabajo y los procedimientos establecidos por el centro de trabajo.

Criterios de evaluación

2.1 Cumple el horario establecido.

2.2 Muestra una presentación personal adecuada.

2.3 Es responsable en la ejecución de las tareas asignadas.

CVE-DOGC-B-22284035-2022

2.4 Se adapta a los cambios de las tareas asignadas.

2.5 Manifiesta iniciativa en la resolución de problemas.

2.6 Valora la importancia de su actividad profesional.

2.7 Mantiene organizada su área de trabajo.

2.8 Cuida los materiales, equipos o herramientas que utiliza en su actividad.

2.9 Mantiene una actitud clara de respeto al medio ambiente.

2.10 Establece una comunicación y una relación eficaz con el personal de la empresa.

2.11 Se coordina con los miembros de su equipo de trabajo.

3. Realiza las actividades formativas de referencia siguiendo protocolos establecidos por el centro de trabajo.

Criterios de evaluación

3.1 Ejecuta las tareas según los procedimientos establecidos.

3.2 Identifica las características particulares de los medios de producción, equipos y herramientas.

3.3 Aplica las normas de prevención de riesgos laborales en su actividad profesional.

3.4 Utiliza los equipos de protección individual según riesgos de la actividad profesional y las normas para el centro de trabajo.

3.5 Aplica las normas internas y externas vinculadas a la actividad.

3.6 Obtiene la información y los medios necesarios para realizar la actividad asignada.

3.7 Interpreta y expresa la información con la terminología o simbología y los medios propios de la actividad.

3.8 Detecta anomalías o desviaciones en el ámbito de la actividad asignada, identifica sus causas y propone posibles soluciones.

Actividades formativas de referencia

1. Actividades formativas de referencia relacionadas con el desarrollo de planes de prevención y concienciación en ciberseguridad.

1.1 Identificación de los principios generales en materia de ciberseguridad.

1.2 Aplicación de la normativa de protección del puesto de trabajo.

1.3 Desarrollo de un plan de formación y concienciación en materia de ciberseguridad.

1.4 Desarrollo de materiales de formación y concienciación.

1.5 Realización de auditorías internas de cumplimiento en materia de prevención.

2. Actividades formativas de referencia relacionadas con el análisis de incidentes de ciberseguridad y con el desarrollo de procedimientos de actuación para darles respuesta.

2.1 Aplicación de la taxonomía de incidentes de ciberseguridad.

2.2 Utilización de controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes.

CVE-DOGC-B-22284035-2022

2.3 Recogida de evidencias, análisis, investigación de incidentes y aplicación de medidas de contención.

2.4 Desarrollo de procedimientos de actuación para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.

2.5 Restablecimiento de los servicios afectados por incidentes.

2.6 Seguimiento de incidentes para evitar una situación similar.

2.7 Notificación de incidentes.

2.8 Realización del análisis de riesgos.

2.9 Realización de guías de buenas prácticas para la securización de sistemas y redes.

3. Actividades formativas de referencia relacionadas con la configuración de sistemas de control de acceso y autenticación de personas.

3.1 Aplicación de mecanismos de autenticación y gestión de credenciales basados en diferentes técnicas.

3.2 Desarrollo de infraestructuras de Clave Pública (*PKI*).

3.3 Aplicación de acceso mediante firma electrónica.

3.4 Administración de la gestión de accesos.

3.5 Administración de la gestión de cuentas privilegiadas.

3.6 Aplicación de protocolos para la administración de credenciales.

4. Actividades formativas de referencia relacionadas con el diseño de redes de computadores.

4.1 Diseño de la segmentación de redes.

4.2 Diseño de *subnetting*.

4.3 Diseño de redes virtuales (*VLANs*).

4.4 Diseño de la zona desmilitarizada (*DMZ*).

4.5 Aplicación de seguridad en redes inalámbricas (*WPA2*, *WPA3*, etc.).

4.6 Aplicación de protocolos de red segura (*IPSec*, etc.).

5. Actividades formativas de referencia relacionadas con la configuración de dispositivos y sistemas informáticos.

5.1 Configuración de seguridad perimetral. Configuración de firewall de Próxima Generación.

5.2. Configuración de seguridad de portales y aplicaciones web.

5.3 Configuración de seguridad del puesto de trabajo.

5.4 Configuración de seguridad de entornos *cloud*.

5.5 Configuración de la seguridad del correo electrónico.

5.6 Configuración de soluciones DLP (*Data Loss Prevention*).

5.7 Configuración de herramientas de almacenamiento de logs.

5.8 Configuración de protección frente a ataques de denegación de servicio distribuido (*DDoS*).

5.9 Configuración de forma segura de cortafuegos, routers y proxies.

5.10 Configuración de redes privadas virtuales (*VPNs*), y túneles (*protocolo IPSec*).

5.11 Configuración de herramientas de monitorización (IDS, IPS).

CVE-DOGC-B-22284035-2022

5.12 Configuración de SIEMs (Gestores de Eventos e Información de Seguridad).

5.13 Configuración de soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs.

5.14 Aplicación de precauciones previas a la instalación de un sistema informático.

5.15 Configuración de seguridad en el arranque de sistema informático.

5.16 Configuración de seguridad de los sistemas de archivos, cifrado, partición, entre otros.

6. Actividades formativas de referencia relacionadas con la configuración de sistemas informáticos, aplicaciones web y aplicaciones para dispositivos móviles.

6.1 Reducción del número de servicios, realización de *hardening* de procesos, eliminación de protocolos de red innecesarios, securización de los sistemas de administración remota, configuración de sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.), configuración de actualizaciones y parches automáticos, configuración de sistemas de copias de seguridad y configuración Shadow IT y políticas de seguridad en entornos SaaS.

6.2 Prueba de la seguridad en los lenguajes de programación y sus entornos de ejecución, análisis de las fuentes abiertas y elaboración de listas de riesgos.

6.3 Establecimiento de los requisitos de verificación a nivel de aplicación y aplicación web.

6.4 Análisis de la entrada de datos.

6.5 Detección y corrección de vulnerabilidades y aplicación de contramedidas.

6.6 Análisis de la firma y la verificación de aplicaciones.

6.7 Ataque y defensa, identificación de vulnerabilidades, análisis y recogida de datos.

7. Actividades formativas de referencia relacionadas con la aplicación de metodologías de análisis forense.

7.1 Identificación de los dispositivos a analizar.

7.2 Recogida de evidencias.

7.3 Análisis de la línea de tiempo.

7.4 Análisis de la volatilidad de información.

7.5 Análisis de *Logs* utilizando las herramientas más utilizadas.

7.6 Documentación del proceso realizado.

7.7 Establecimiento de la línea temporal.

7.8 Mantenimiento de la cadena de custodia.

7.9 Elaboración de las conclusiones.

7.10 Presentación y exposición de conclusiones.

8. Actividades formativas de referencia relacionadas con la normativa de ciberseguridad.

8.1 Diseño de un sistema de Gestión de *Compliance*.

8.. Realización del análisis y gestión de riesgos, mapas de riesgos.

8.3 Documentación del sistema.

8.4 Identificación de los riesgos penales que afectan a la organización.

8.5 Estudio de los sistemas de gestión de *Compliance* penal.

CVE-DOGC-B-22284035-2022

8.7 Conocimiento de los sistemas de gestión anticorrupción.

8.8 Aplicación de los principios de protección de datos.

8.9 Aplicación de privacidad por diseño y por defecto.

8.10 Realización del análisis de Impacto en Privacidad (PIA), y medidas de seguridad.

(22.284.035)