# CUALIFICACIÓN PROFESIONAL:
## Gestión de la ciberseguridad

| | |
|---|---|
| *Familia Profesional:* | ***Informática y Comunicaciones*** |
| *Nivel:* | ***3*** |
| *Código:* | ***IFC153_3*** |
| *Estado:* | ***BOE*** |
| *Publicación:* | ***RD 917/2024*** |
| *Referencia Normativa:* | ***Orden PRE/1636/2015, RD 1087/2005, RD 616/2020*** |

## Competencia general

Garantizar la seguridad en el almacenamiento y transmisión de la información, verificando los accesos y usos en equipos informáticos, redes de comunicación y sitios web, previniendo y reaccionando ante ataques, identificando vulnerabilidades y aplicando contramedidas para garantizar la confidencialidad, disponibilidad, integridad y autenticidad, cumpliendo la normativa aplicable sobre protección de datos, propiedad intelectual e industrial, seguridad informática y servicios de las comunicaciones.

## Unidades de competencia

**UC0486_3:** ASEGURAR EQUIPOS INFORMÁTICOS
**UC0487_3:** Auditar redes de comunicación y sistemas informáticos
**UC0488_3:** Gestionar incidentes de ciberseguridad
**UC0489_3:** Implementar sistemas seguros de acceso y transmisión de datos

## Entorno Profesional

### Ámbito Profesional

Desarrolla su actividad profesional en el área de sistemas informáticos y/o telemáticos dedicado a la seguridad informática (ciberseguridad), en entidades de naturaleza pública o privada, empresas de tamaño pequeño/mediano/grande o microempresas, tanto por cuenta propia como ajena, con independencia de su forma jurídica. Desarrolla su actividad dependiendo, en su caso, funcional y/o jerárquicamente de un superior. Puede tener personal a su cargo en ocasiones, por temporadas o de forma estable. En el desarrollo de la actividad profesional se aplican los principios de accesibilidad universal y diseño universal o diseño para todas las personas de acuerdo con la normativa aplicable.

### Sectores Productivos

Se ubica principalmente en el sector servicios, en el subsector de los servicios de instalación, mantenimiento, gestión y asistencia técnica de sistemas informáticos y telemáticos, y en cualquier sector productivo que requiera los servicios anteriores

### Ocupaciones y puestos de trabajo relevantes

*Los términos de la siguiente relación de ocupaciones y puestos de trabajo se utilizan con carácter genérico y omnicomprensivo de mujeres y hombres.*

- Técnicos en seguridad informática
- Técnicos de gestión de incidentes de ciberseguridad
- Técnicos en auditoría de ciberseguridad

- Técnicos en ciberseguridad

## Formación Asociada (600 horas)

### Módulos Formativos

**MF0486_3:** SEGURIDAD EN EQUIPOS INFORMÁTICOS (120 horas)
**MF0487_3:** Auditoría de redes de comunicación y sistemas informáticos (180 horas)
**MF0488_3:** Gestión de incidentes de ciberseguridad (120 horas)
**MF0489_3:** Implementación de sistemas seguros de acceso y transmisión de datos (180 horas)

## UNIDAD DE COMPETENCIA 1
ASEGURAR EQUIPOS INFORMÁTICOS

*Nivel:* *3*
*Código:* *UC0486_3*
*Estado:* *BOE*

### Realizaciones profesionales y criterios de realización

**RP1:** Configurar equipos informáticos siguiendo los procedimientos establecidos en el plan de seguridad de la organización para protegerlos de la pérdida, manipulación y sustracción de información no autorizada.

**CR1.1** Los tipos de usuarios se definen, estableciendo los privilegios de acceso a los recursos (aplicaciones "software", carpetas, entre otros), según las funciones desempeñadas dentro de la organización.

**CR1.2** Las cuentas de usuario se crean, utilizando las herramientas específicas del sistema operativo, dándoles un nombre de usuario, una contraseña y asignándolas a los tipos de usuarios definidos en el sistema informático.

**CR1.3** La política de contraseñas se configura, estableciendo parámetros tales como complejidad, caducidad, revocación, bloqueo, reutilización, entre otros.

**CR1.4** El control de acceso al equipo informático se establece, configurando parámetros tales como el número de intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros.

**CR1.5** La seguridad del equipo informático ante ataques externos se refuerza, configurando un cortafuegos según las necesidades de uso del equipo, estableciendo reglas de filtrado de las conexiones entrantes y salientes.

**CR1.6** La seguridad de la información del equipo informático (integridad, accesos, entre otros) frente a riesgos de ataque malicioso se revisa, comprobando la instalación y configuración del "software" de protección adecuado (EDP -"EndPoint Detection and Response"-, "anti-ransomware", "anti-malware", entre otros).

**CR1.7** La recopilación, tratamiento y eliminación de la información por parte de los usuarios se revisa, documentando detalladamente los protocolos a seguir según el grado de confidencialidad de la información.

**CR1.8** La política de seguridad de la organización se transmite a los usuarios, publicando informaciones tales como restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos, ámbitos de responsabilidades relativos a la utilización de los equipos informáticos.

**RP2:** Configurar equipos servidores, aplicando los mecanismos de protección establecidos en el plan de seguridad de la organización para protegerlos de accesos indebidos.

**CR2.1** Los servicios que ofrece el servidor (correo, web, servicio de impresión, entre otros) se configuran, haciendo uso de los entornos específicos de cada servicio, estableciendo valores a sus parámetros de configuración, conforme a las medidas de bastionado establecidas por la organización, si procede.

**CR2.2** Los servicios del sistema operativo preinstalados no necesarios (NFS, DNS, entre otros) en el servidor se desactivan, borrándolos del sistema, garantizando así que no pueden ser activados.

**CR2.3** La comunicación con el servidor (autentificación de usuarios, intercambio de información) se asegura, activando y configurando protocolos de seguridad tales como TLS (TLS, SSH, entre otros).

**CR2.4** Los mecanismos de registro de actividad e incidencias del servidor se activan, configurando el registro de eventos del sistema y parametrizando valores tales como periodicidad, nivel de detalle (fecha, usuario, entre otros).

**CR2.5** Los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor se activan, configurando y parametrizando, según el servicio, valores tales como tamaño de los ficheros logs, rotación, nivel de detalle (dirección IP, fecha, usuario, entre otros).

**CR2.6** Las configuraciones realizadas e incidencias producidas se documentan, detallando el procedimiento llevado a cabo, las incidencias ocurridas (descripción, tipo, entre otros) y el correctivo aplicado para solventarlas, según procedimiento interno de la organización (plantillas, herramientas "software", entre otros).

**RP3:** Eliminar información en soportes y sistemas de almacenamiento de equipos informáticos, de forma segura, aplicando procedimientos de borrado seguro y destrucción física de información, siguiendo los procedimientos establecidos en la política de seguridad de la organización para prevenir la fuga de información confidencial.

**CR3.1** Los métodos de destrucción física (trituración, desintegración, incineración, entre otros) se revisan, comprobando que el método utilizado se corresponde con el tipo de soporte de información.

**CR3.2** El protocolo de retención de datos se interpreta, teniendo en cuenta la organización, búsqueda, acceso y eliminación de la información.

**CR3.3** La información almacenada en los equipos informáticos y en los soportes de información se borran, utilizando herramientas "software" de borrado seguro de datos.

**CR3.4** El procedimiento realizado se registra, generando un documento de certificación que detalle informaciones tales como, evidencias lógicas o gráficas del proceso, cuándo y cómo se ha realizado el proceso de destrucción o reutilización, especificaciones técnicas del "hardware", entre otras.

**RP4:** Aplicar medidas de seguridad física a equipos servidores, comprobando que su ubicación dispone de protección de acceso y condiciones ambientales específicas, entre otras, siguiendo el plan de seguridad de la organización para evitar interrupciones en la prestación de servicios del sistema.

**CR4.1** La ubicación física de los servidores se revisa, comprobando que se encuentran situados en un espacio con acceso físico controlado y protegido.

**CR4.2** Las condiciones ambientales (temperatura, humedad) de la ubicación física de equipos servidores se comprueban, verificando que se encuentran dentro del rango de trabajo óptimo considerado entre 17 y 21 grados.

**CR4.3** El Sistema de Alimentación Ininterrumpida (SAI) se revisa, comprobando que está operativo a través de su sistema de alertas y reportando su estado en caso de anomalías de funcionamiento.

**RP5:** Verificar la realización de copias de seguridad, comprobando la información a respaldar, la frecuencia de respaldo, entre otros, para mantener la seguridad y disponibilidad de la información.

**CR5.1** La información del equipo informático se comprueba, verificando que su clasificación en función de su criticidad y de su tipo (datos de sistema o datos de la organización) es acorde al plan de copias de seguridad.

**CR5.2** El plan de copias de seguridad se verifica, comprobando que contempla los datos a guardar, su criticidad, tipo de salvaguarda, frecuencia de respaldo, entre otros.

**CR5.3** Los dispositivos de almacenamiento de copias de seguridad (cintas, discos externos, entre otros) se comprueban, verificando que la información (fecha de la copia, información respaldada, entre otros) contenida en ellos se encuentra registrada en el plan de copias de seguridad.

**CR5.4** Los procedimientos de obtención y verificación de copias de seguridad se verifican, realizando pruebas de funcionamiento de los mismos.

## Contexto profesional

### Medios de producción

Aplicaciones ofimáticas corporativas. Verificadores de fortaleza de contraseñas. Analizadores de puertos. Analizadores de ficheros de registro del sistema. Cortafuegos. Equipos específicos y/o de propósito general. Cortafuegos personales o de servidor. Sistemas de autenticación: débiles: basados en usuario y contraseña y robustos: basados en dispositivos físicos y medidas biométricas. Programas de comunicación con capacidades criptográficas. Herramientas de administración remota segura. IDS Sistemas de Detección de Intrusión (IDS), Sistemas de Prevención de Intrusión (IPS), equipos trampa ("Honeypots"). Herramientas de borrado seguro de información.

### Productos y resultados

Equipos informáticos con control de acceso seguro, cortafuegos y "software" de protección configurado. Equipos servidores con mecanismos de protección establecidos. Documentos de configuración e incidencias producidas. Equipos informáticos reutilizables. Equipos servidores en ubicaciones protegidas y seguras.

### Información utilizada o generada

Política de seguridad de infraestructuras telemáticas. Normativa aplicable, reglamentación y estándares. Registro inventariado del "hardware". Registro de comprobación con las medidas de seguridad aplicadas a cada sistema informático. Topología del sistema informático a proteger. Normativa sobre protección de datos. Normativa sobre servicios de la sociedad de información. Normativa sobre prevención de riesgos laborales. Normativa medioambiental, en especial sobre producción y gestión de residuos y suelos contaminados.

## UNIDAD DE COMPETENCIA 2

Auditar redes de comunicación y sistemas informáticos

*Nivel:* *3*
*Código:* *UC0487_3*
*Estado:* *Tramitación BOE*

### Realizaciones profesionales y criterios de realización

**RP1:** Comprobar la seguridad de los sistemas informáticos, revisando el bastionado de las instalaciones, equipos y "software", para verificar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la información gestionada, según indicaciones del plan de seguridad de la organización auditada.

**CR1.1** El inventariado de activos se revisa, verificando los equipos existentes y sus características, comprobando las versiones de los programas que se ejecutan, para confirmar que está actualizado y no hay equipos ni programas que no aparezcan en el mismo.

**CR1.2** La instalación y configuración de los sistemas operativos se revisa, confirmando que el "software" instalado es legítimo, está actualizado y tanto los usuarios como las aplicaciones cuentan con los permisos de "mínimo privilegio" para desempeñar sus funciones en el sistema.

**CR1.3** La instalación y configuración de "software" de seguridad contra programas maliciosos tales como antivirus/"antimalware", EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection and Response"), entre otros, se comprueba, verificando que dicho "software" es legítimo, está actualizado y tiene activas las funciones que indique el responsable de seguridad.

**CR1.4** Las aplicaciones empleadas en la organización se revisan, comprobando licencias y versiones para confirmar que son legítimas, están actualizadas y que únicamente pueden ser accedidas por el personal autorizado, y que ese acceso tenga las limitaciones que indique el responsable de seguridad, basadas en el principio de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know").

**CR1.5** Las cuentas de usuario de la organización se comprueban que son individuales, cuentan con una política de contraseñas robusta y han sido elaboradas bajo el principio de "mínimo privilegio" y segregación de funciones, modificando aquellas que no cumplen los criterios y eliminando las cuentas obsoletas o que no pertenecen a personas autorizadas.

**CR1.6** Las instalaciones se comprueban de manera presencial para asegurarse de que los equipos y la información están protegidos contra accesos físicos no autorizados, usando elementos al efecto de manera separada o combinada tales como mecanismos de apertura por usuario y contraseña, llave física, detectores biométricos entre otros, aplicando un sistema de aviso previo y bloqueando sesiones por inactividad y usando políticas de "mesas limpias".

**CR1.7** Las instalaciones se comprueban, verificando las condiciones ambientales de temperatura y humedad requeridas por el fabricante para su funcionamiento y la protección frente a desastres naturales que pueden afectar físicamente en el emplazamiento y previniendo posibles alteraciones del entorno tales como picos de electricidad o ruido eléctrico, entre otros.

**CR1.8** Las pruebas realizadas durante la auditoría se documentan, incluyendo referencias a los activos del sistema, los parches y actualizaciones instalados en los sistemas operativos y aplicaciones, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

**RP2:** Comprobar la seguridad de la red de la organización auditada, verificando los elementos relativos indicados en el plan de seguridad, para prevenir posibles intrusiones, ataques y fugas de información.

**CR2.1** El diseño de arquitectura de la red se revisa, mediante auditoría de caja blanca, comprobando que la red está configurada de forma que se minimice el impacto de posibles ataques del exterior: utilizando VLAN ("Virtual Local Área Networks"), cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), "routers" y otros dispositivo de red e instalado todos los recursos de la empresa que deben ser accesibles desde Internet tales como páginas web y correo electrónico, en una zona aislada o desmilitarizada (DMZ).

**CR2.2** Los dispositivos que controlan y gestionan el tráfico de la red tales como "router", "switch", "hub", cortafuegos, IDS, IPS, SIEM ("Security Information and Event Management"), entre otros, se revisan, usando técnicas de caja blanca: de manera física y comprobando su configuración para verificar que únicamente aceptan el tráfico permitido y están actualizados.

**CR2.3** Los mensajes de error generados por los dispositivos de red, "routers", "switch", "hub" cortafuegos, IDS, IPS, SIEM y cualquier otro, se revisan en forma de auditoría de caja blanca para asegurar que, de forma interna, registran cualquier anomalía para facilitar la gestión de incidentes y, de forma externa en modo auditoría de caja negra, para confirmar que no aportan información que permita a un posible atacante remoto obtener información de los puertos abiertos en el sistema.

**CR2.4** Los elementos de la red se comprueban que únicamente son accedidos de forma remota por personal y bajo las condiciones de tiempo y lugar de origen, previamente autorizados en la política de seguridad y sólo a través de las VPN (Redes privadas Virtuales).

**CR2.5** El uso de programas o herramientas en la nube se revisa, verificando que se lleva a cabo de la forma acordada con el proveedor del servicio y permitida dentro de la política de seguridad de la organización.

**CR2.6** Las redes Wifi se comprueban, verificando que utilizan protocolos seguros de cifrado y que únicamente acceden a ellas las personas autorizadas en la política de seguridad.

**CR2.7** La conexión a Internet por parte de los usuarios de la organización se comprueba, verificando que únicamente pueden acceder a los servicios y contenidos previamente autorizados en la política de seguridad.

**CR2.8** Los sistemas anti DDoS (Denegación de servicio) de la organización se verifica que están habilitados y funcionales, comprobando si se han configurado sistemas al efecto tales como reglas de cortafuegos, sistemas de monitorización y/o servicios externos de protección, entre otros.

**CR2.9** Las pruebas realizadas durante la auditoría se documentan, incluyendo referencias a los activos inspeccionados, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

**RP3:** Comprobar la seguridad del sitio web, realizando pruebas de simulación de ataques para detectar posibles fallos de seguridad.

**CR3.1** La instalación y configuración de los sistemas de gestión de contenidos (CMS) y servidores web se verifica, comprobando que están instaladas las últimas versiones estables y que únicamente tienen instalados los módulos imprescindibles para su funcionamiento, revisando la documentación asociada.

**CR3.2** Las cuentas de usuario del sitio web se comprueban, verificando que son generadas bajo el principio de "mínimo privilegio" y cuentan con una política de acceso segura.

**CR3.3** La información generada de forma pública por el servidor web y/o el sistema de gestión de contenidos (CMS) se verifica, comprobando que no muestre ninguna información que permita obtener fácilmente información relacionada con la configuración del sistema tal como tipo de programa empleado, versión, entre otros.

**CR3.4** La gestión de sesiones en el sistema se comprueba, verificando que tanto las "cookies" como los "tokens" de sesión se generan de forma segura y no predecible, tal como evitando la numeración secuencial para la identificación de usuarios, para impedir que un atacante externo pueda aprovecharse de ellas para acceder al sistema de forma no autorizada.

**CR3.5** Los formularios y puntos de acceso de información por parte del usuario se comprueban, verificando que cuentan con mecanismos que impidan la entrada de caracteres que provoquen un comportamiento no deseado del sistema como la introducción de código (por inyección de SQL o XSS -"Cross-site scripting"-, entre otros) o la generación de errores en el sistema tales como desbordamiento de "buffer" por introducción de cadenas largas.

**CR3.6** La gestión de errores y excepciones del sistema se comprueba, verificando que éstos son registrados y la información mostrada en el lado del cliente no revela información que pueda permitir a los usuarios una posterior explotación del fallo.

**CR3.7** La información entre el cliente y el servidor se comprueba que se envía de forma segura, verificando que se realiza a través de protocolos tales como HTTPS y TLS, que la información enviada se cifra, siguiendo estándares actualizados.

**CR3.8** Las pruebas realizadas durante la auditoría se documentan, incluyendo referencias a los activos inspeccionados, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

**RP4:** Comprobar la seguridad de la información tratada por la organización auditada, verificando y asegurando los elementos relativos indicados en el plan de seguridad, para garantizar la integridad, disponibilidad, confidencialidad, autenticidad y el "no repudio" y el cumplimiento de la normativa aplicable de protección de datos.

**CR4.1** La asignación de los roles del personal responsable de la gestión, tratamiento y almacenamiento de los datos se comprueba, verificando que se accede a la información requerida en cada caso y su alineación con el principio de "mínimo privilegio" y "necesidad de saber".

**CR4.2** Las medidas de seguridad físicas y lógicas implantadas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos se comprueban, verificando que se cumple con los principios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio.

**CR4.3** El intercambio de información se comprueba, verificando que se realiza únicamente a través de los canales autorizados, de la forma convenida y por las personas definidas en la normativa de la organización.

**CR4.4** El registro de actividades del tratamiento de los datos se revisa, verificando que está completo y actualizado, comprobando que el tratamiento únicamente se efectúa por personas autorizadas en la normativa de seguridad de la organización.

**CR4.5** Los protocolos de eliminación de información se revisan, confirmando que garantizan el borrado seguro de la información, destruyendo el papel en máquinas y contenedores específicos que no permitan la recuperación de la información y, en caso de cesión de

dispositivos digitales a terceros, que no se pueda acceder a la información contenida previamente en él.

**CR4.6** La realización de copias de seguridad se verifica, comprobando que está alineado con la política de seguridad de la organización de forma que, ante una eliminación de datos por un desastre natural, o por personas de modo accidental o intencionado, es posible recuperar la información en los plazos de tiempo convenidos.

**CR4.7** La aplicación de la normativa de seguridad por parte de los usuarios se revisa, verificando que saben cómo y dónde reportar los incidentes informáticos, no hacen uso de dispositivos no autorizados o de origen desconocido, aplican la política de "mesas limpias", bloquean el equipo si van a estar ausentes y no divulgan información asociada con su trabajo.

**CR4.8** El informe de la auditoría se elabora, incluyendo el alcance de la misma, la documentación revisada, las pruebas y entrevistas realizadas, los posibles obstáculos encontrados y las evidencias obtenidas, presentando especial atención a los hallazgos clasificados y no conformidades de las que también se indicará su criticidad, detallando el grado de cumplimiento legal y las medidas de mejora convenientes.

## Contexto profesional

### Medios de producción

Equipos informáticos tales como ordenadores de sobremesa, portátiles y servidores. Redes Wifi. Navegadores. Buscadores. Aplicaciones ofimáticas. Analizadores de vulnerabilidades. Herramientas de prueba de penetración. "Software" de auditorías de PC. Programas de análisis de contraseñas.

### Productos y resultados

Sistemas informáticos seguros y comprobados. Red asegurada y verificada. Sitios web asegurados y verificados. Información usada, almacenada y accedida bajo criterios de integridad, disponibilidad, confidencialidad. Control de acceso a la información y "no repudio" garantizados.

### Información utilizada o generada

Normas externas de trabajo (normativa aplicable de propiedad intelectual e industrial; normativa aplicable de protección de datos y seguridad informática; normativa aplicable sobre prevención de riesgos laborales - ergonomía -). Normas internas de trabajo (plan de seguridad, metodologías de análisis de seguridad, histórico de incidencias, registro de ficheros de datos de carácter personal, informes de análisis de vulnerabilidades, relación de contraseñas débiles, informe de auditoría de servicios y puntos de acceso al sistema informático). Documentación técnica (boletines de seguridad externos, documentación técnica del fabricante de los equipos, sistemas y "software" utilizado, documentación técnica de la red, bibliografía especializada, tutoriales y cursos).

## UNIDAD DE COMPETENCIA 3

Gestionar incidentes de ciberseguridad

*Nivel:* *3*
*Código:* *UC0488_3*
*Estado:* *Tramitación BOE*

### Realizaciones profesionales y criterios de realización

**RP1:** Implantar procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos en los sistemas de una entidad u organización según directrices ante incidentes nacionales e internacionales para los equipos de respuesta.

**CR1.1** Los procedimientos de detección y respuesta de incidentes se localizan, verificando que están documentados, que indican los roles y responsabilidades de seguridad y que implementan los requerimientos de la política de seguridad de la entidad, así como la determinación de la cadena de mando ante la detección de un incidente de seguridad.

**CR1.2** La modelización de los sistemas se efectúa, seleccionando los mecanismos de registro a activar, observando las alertas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones y signos de comportamiento sospechoso a partir de indicadores de compromiso (IOC: "Indicator of Compromise") facilitados por equipos de respuesta ante incidentes nacionales e internacionales.

**CR1.3** La activación de los mecanismos de registro del sistema se verifica, contrastándolos con las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.

**CR1.4** La planificación de los mecanismos de análisis de registros se verifica, de forma que se garantice la detección de los comportamientos sospechosos, mediante un sistema de indicadores y métricas.

**CR1.5** La instalación, configuración y actualización de los sistemas de detección de intrusos (IDS) se verifica en función de las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.

**CR1.6** Los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan") definido por la organización, se verifican, comprobando que pueden ser recuperados en tiempo y forma ante un incidente grave.

**RP2:** Detectar incidentes de seguridad de forma activa y preventiva para minimizar el riesgo según directrices de los equipos de respuesta ante incidentes nacionales e internacionales y de la entidad responsable del sistema.

**CR2.1** Las herramientas utilizadas para detectar intrusiones se comprueba que no han sido comprometidas ni afectadas por programas maliciosos analizándolas, siguiendo las guías y directrices de los equipos de respuesta nacionales e internacionales.

**CR2.2** Los funcionamientos sospechosos se detectan, analizando parámetros de funcionamiento tales como conexiones no autorizadas, mensajes de alerta de los sistemas de detección de intrusiones (IDS: "Intrusion Detection System") o "antimalware" entre otros,

usando herramientas específicas tales como sistemas de Gestión de información y eventos de seguridad (SIEM: "Security information and event management") e IDS, entre otras y estableciendo procedimientos para recoger denuncias de los usuarios acerca de ataques tales como "phising" o comportamientos anómalos en equipos según directrices de la entidad responsable del sistema.

**CR2.3** Los componentes "software" del sistema se verifican periódicamente en lo que respecta a su integridad usando programas específicos.

**CR2.4** El funcionamiento de los dispositivos de protección física se verifica por medio de los registros de cada sistema, pruebas específicas, pruebas de estrés, entre otras según las normas de la organización y/o normativa aplicable de seguridad.

**CR2.5** Los sucesos y signos extraños que pudieran considerarse una alerta se recogen en el informe para su posterior análisis, en función de la gravedad de los mismos y la política de la organización, especificando para cada uno ítems tales como día y hora de la detección, persona que lo comunicó, sistemas implicados y acciones realizadas, entre otros.

**CR2.6** La exposición o filtración de los datos de la organización se verifica periódicamente en función del riesgo que haya determinado la entidad responsable del sistema, consultando fuentes abiertas (OSINT: "Open Source Intelligence") según las características de la organización.

**CR2.7** La información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales se comprueba, verificándola de manera periódica para establecer en su caso los mecanismos de seguridad recomendados en caso de exposición a las amenazas publicadas.

**RP3:** Coordinar la respuesta ante incidentes de seguridad entre las áreas implicadas, aplicando el procedimiento recogido en los protocolos de seguridad para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la entidad u organización a proteger.

**CR3.1** Los procedimientos se activan ante la detección de un incidente de seguridad, dando aviso a los responsables de cada subsistema y aplicando los pasos recogidos en los protocolos de la normativa de seguridad de la organización.

**CR3.2** La información para el análisis forense del sistema vulnerado se recoge, una vez aislado el sistema, capturando una imagen tan precisa como sea posible, realizando notas detalladas (incluyendo fechas y horas indicando si se utiliza horario local o UTC), recogiendo la información según el orden de volatilidad (de mayor a menor) entre otras, según los procedimientos de las normas de seguridad de la entidad.

**CR3.3** Las características de la intrusión se determinan, analizando el sistema atacado mediante herramientas de detección de intrusos (IDS), usando las facilidades específicas de cada herramienta y según los procedimientos de seguridad de la organización.

**CR3.4** La intrusión se contiene mediante la aplicación de las medidas establecidas en las normas de seguridad de la organización tales como desconexión de equipos y/o segmentos de red o cierre de puertos de comunicaciones, entre otras, y aquellas extraordinarias, que indique la persona responsable de la seguridad, aunque no estén previamente planificadas.

**CR3.5** La documentación del incidente, así como todas las acciones realizadas y las conclusiones obtenidas se realiza para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido, manteniendo de esta forma un registro de lecciones aprendidas ("Lessons Learned").

**CR3.6** Las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado se planifican a partir de la determinación de los daños causados, cumpliendo los criterios de calidad de servicio y el plan de explotación de la entidad a proteger.

**RP4:** Implantar planes de prevención y concienciación en ciberseguridad, para facilitar la previsión de ciberincidentes y su respuesta, en caso de producirse, según los requisitos de servicio y dentro de las directivas de la organización o entidad a proteger.

**CR4.1** Las medidas de ciberseguridad definidas por la organización se difunden, usando medios tales como correo electrónico, intranet corporativa y sesiones específicas, entre otros.

**CR4.2** La normativa de protección del puesto de trabajo se establece, incluyendo ítems tales como escenarios y ejemplos de riesgo y medidas de seguridad, entre otros.

**CR4.3** El plan de concienciación de ciberseguridad dirigido a los empleados se define, elaborando material y cursos o tutoriales para su difusión o impartición y las evaluaciones a realizar y su periodicidad.

**CR4.4** El material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados se difunde o en su caso se imparte de forma periódica, usando los mecanismos disponibles en la entidad, tales como correo electrónico, plataformas web de difusión, aulas y canales de vídeo para cursos, entre otros, capacitando a los empleados ante ciberataques, para detectar los métodos y vectores más habituales.

## Contexto profesional

### Medios de producción

Equipos informáticos tales como ordenadores de sobremesa, portátiles y servidores. Aplicaciones ofimáticas corporativas. Analizadores de vulnerabilidades tales como antivirus/"antimalware" o EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection" and "Response"). Herramientas para garantizar la confidencialidad de la información tales como sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS). "Software" de monitorización de redes. Sistemas de monitorización SIEM ("Security Information and Event Management"). "Software" para garantizar la confidencialidad e integridad de las comunicaciones. Programas de análisis de contraseñas. "Software" de flujo de trabajo para envío de alarmas e incidencias a responsables. Consola de SNMP. Herramientas de análisis forense (creación de líneas de tiempo, recuperación de ficheros borrados, clonado de discos, entre otros).

### Productos y resultados

Procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos implantados. Incidentes de seguridad detectados y prevenidos. Riesgos minimizados. Respuesta ante incidentes de seguridad coordinada. Incidentes solucionados y contenidos. Planes de prevención y concienciación en ciberseguridad implantados.

### Información utilizada o generada

Normas externas de trabajo (normativa aplicable de propiedad intelectual e industrial; normativa aplicable de protección de datos y seguridad informática; normativa aplicable sobre prevención de riesgos laborales -ergonomía-). Normas internas de trabajo (plan de seguridad, metodologías de análisis de seguridad, histórico de incidencias, registro de ficheros de datos de carácter personal, informes de análisis de vulnerabilidades, relación de contraseñas débiles, informe de auditoría de servicios y puntos de acceso al sistema informático, normas internas de detección de intrusos y de prevención de amenazas de seguridad). Documentación técnica (boletines de seguridad externos y avisos de vulnerabilidades, documentación técnica del fabricante de los equipos, sistemas y "software" utilizado, documentación técnica de la red, bibliografía especializada, tutoriales y cursos).

## UNIDAD DE COMPETENCIA 4

Implementar sistemas seguros de acceso y transmisión de datos

*Nivel:* *3*
*Código:* *UC0489_3*
*Estado:* *Tramitación BOE*

### Realizaciones profesionales y criterios de realización

**RP1:** Implantar protocolos y herramientas en operaciones de intercambio de datos según las necesidades de uso, garantizando la integridad y confidencialidad de la información, así como el control de acceso, para obtener comunicaciones o canales de comunicación seguros, cumpliendo las directivas del departamento responsable de la seguridad del sistema informático.

**CR1.1** La confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas se garantiza, haciendo uso de redes privadas virtuales, comunicándolos al proveedor del servicio para lograr soluciones ajustadas al plan de seguridad.

**CR1.2** Las técnicas de protección de conexiones inalámbricas disponibles en el mercado se aplican, seleccionando aquellas basadas en estándares reconocidos como confiables en el sector, para cubrir vulnerabilidades, teniendo en cuenta el principio de proporcionalidad.

**CR1.3** Los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones se implantan, diferenciando usuarios por perfiles y asignándoles permisos según ese perfil.

**CR1.4** Los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas se protegen, usando herramientas disponibles para el cifrado extremo a extremo, para garantizar la seguridad de las comunicaciones.

**CR1.5** La identidad de los servidores se garantiza en aquellos servicios que lo soportan, usando certificados digitales, configurando las aplicaciones cliente con el certificado raíz de confianza que garantice al usuario la autenticidad del servidor.

**CR1.6** Las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas se documentan, incluyendo las características de las configuraciones aplicadas, ajustándolo a estándares y/o en el formato establecido en la organización.

**CR1.7** Los servicios, cuyo nivel riesgo estime el departamento entidad responsable de la gestión de la seguridad del sistema informático que lo requieran, se aseguran incorporando una autenticación de doble o triple factor basada en certificados de usuario, DNI electrónico, "token", biométricos u otros mecanismos.

**CR1.8** Los servicios en los que se utiliza autenticación basada en contraseñas, se configuran, estableciendo políticas de complejidad, renovación, bloqueo, almacenamiento y/o recuperaciones.

**RP2:** Implantar el uso de sistemas de firma y certificados de persona para asegurar la autenticidad, integridad, confidencialidad y "no repudio" de los datos que intervienen en una transferencia de información personal según las necesidades de uso y dentro de las directivas del departamento responsable de la seguridad del sistema informático.

**CR2.1** El acceso a servicios a través de la red telemática se implanta de forma que asegure la autenticación mutua de cliente y servidor, utilizando autenticación de la clientela basada en certificados digitales de identidad personal cuando la política de seguridad de la organización así lo requiera.

**CR2.2** El proceso de obtención y verificación de certificados digitales de identidad personal se aplica, siguiendo los pasos establecidos por la entidad certificadora y con la periodicidad indicada por el departamento responsable de la seguridad del sistema.

**CR2.3** Los mecanismos para la transmisión cifrada del correo electrónico y otras comunicaciones, ya sea interpersonales o entre procesos y/o componentes, se implementan empleando certificados digitales para firmar y cifrar extremo a extremo el contenido de dichos mensajes, en los casos que indique la política de seguridad de la organización.

**CR2.4** Los mecanismos de firma digital de documentos seleccionados de acuerdo con la política de seguridad del departamento responsable se aplican, incluyendo dicha firma en el momento del envío o, en su caso, al almacenar cada documento.

**CR2.5** Los sistemas de sellado digital de tiempo se implantan, aplicándolos a los documentos que requiera la seguridad de la organización, para garantizar la existencia de un documento electrónico en un instante concreto, garantizando que la información contenida no ha sido alterada por terceros.

**CR2.6** La integridad de los componentes en sitios web y del "software" interno se garantiza, firmándolos mediante firma digital, según el procedimiento del sistema o herramientas de firmado.

**CR2.7** Los sistemas de firma digital implantados se documentan indicando su ámbito de aplicación, el procedimiento para su uso, la tipología de documentos, aplicaciones a firmar y el sistema de firma aplicado, entre otros, siguiendo estándares y de acuerdo con el formato establecido en la organización.

**RP3:** Implementar infraestructuras de clave pública, siguiendo instrucciones del fabricante y en función de las condiciones de uso, para garantizar la seguridad, según los estándares del sistema y dentro de las directivas de la organización.

**CR3.1** La jerarquía de certificación se instala configurando la herramienta que la implementa, siguiendo las instrucciones del proveedor, en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.

**CR3.2** La declaración de prácticas de certificación y la política de certificación se redacta, definiendo los procedimientos, derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.

**CR3.3** El sistema de autoridad de certificación se instala, siguiendo las indicaciones del fabricante, las prácticas recomendadas del sector y la política de seguridad de la organización.

**CR3.4** El certificado digital de la autoridad de certificación y su política asociada se ponen a disposición de los usuarios, siguiendo las directrices contenidas en la declaración de prácticas de certificación.

**CR3.5** La clave privada de la autoridad de certificación se almacena, manteniéndola segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.

**CR3.6** Los certificados digitales se emiten según los usos que van a recibir los certificados y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.

**CR3.7** La validez de los certificados emitidos por la autoridad de certificación se comprueba, verificando que es mantenido por el servicio de revocación de certificados, según lo indicado en la declaración de prácticas de certificación.

**CR3.8** Las infraestructuras de clave pública implantadas se documentan recogiendo sus datos de configuración, ajustándose a estándares y según el formato establecido en la organización.

**RP4:** Revisar el "hardware" y el diseño de la red de área local, aplicando adaptaciones para garantizar la seguridad de las comunicaciones y la protección de los datos según las directrices de la entidad responsable de la gestión de la red.

**CR4.1** La topología de la red se adapta según las necesidades de seguridad, valorando su idoneidad mediante el análisis de modelos de referencia estándar, seleccionando una nueva topología y añadiendo o suprimiendo dispositivos de comunicaciones para minimizar posibles riesgos.

**CR4.2** La red de la organización se segmenta de acuerdo con la compartimentación organizativa, la identidad de los equipos o usuarios y la política de seguridad de la entidad responsable, ya sea de forma física, mediante equipos tales como "routers", o de forma lógica utilizando VLAN ("Virtual Local Área Networks").

**CR4.3** Las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, se establecen de acuerdo con la segmentación establecida y la política de seguridad de la organización.

**CR4.4** Los mecanismos de protección para las redes de acceso, ante elementos que rompen con el perímetro tradicional de la red corporativa, tales como redes inalámbricas, dispositivos móviles y portátiles, particulares o corporativos, con conexión a las redes de la organización se establecen identificando los dispositivos empleados, delimitando su alcance y protegiendo el acceso mediante cifrado seguro, de acuerdo con la política de seguridad de la organización.

**CR4.5** Los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention") se implementan mediante "hardware" o "software" al efecto, en virtud de los requisitos de seguridad de la organización, para detectar potenciales brechas en el acceso y/o transmisión de datos y prevenirlas a través del monitoreo, detección y bloqueo de información sensible.

**CR4.6** El diseño de la red se modifica en su caso, introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, bien duplicando la red física, equipos y "software", bien mediante la virtualización de sistemas.

**CR4.7** Los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal se configuran, asegurando una transmisión de datos confiable y segura entre los distintos nodos que la conforman.

**CR4.8** Los procedimientos de salvaguarda de configuraciones se revisan modificando, en su caso, la programación de sus copias de seguridad mediante la funcionalidad habilitada en el sistema, almacenándolas en condiciones de seguridad y permitiendo una eficaz recuperación.

**CR4.9** La documentación de configuración de seguridad se elabora incluyendo todos los valores de configuración implantados, ajustándolo a estándares y según el formato establecido en la organización.

**RP5:** Revisar el "software" de comunicaciones en red y el control de acceso de manera periódica, actualizándolo, añadiendo o suprimiendo elementos y/o modificando configuraciones, para garantizar la seguridad de las comunicaciones y la protección de los datos, según las directrices de la organización.

**CR5.1** El "software" de comunicaciones que se ejecuta en los dispositivos de red se evalúa, valorando su compatibilidad, teniendo en cuenta su funcionalidad y su idoneidad para el diseño a corto y medio plazo, comprobando su integridad, legitimidad y grado de actualización para corregir problemas de seguridad.

**CR5.2** Los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies" se incluyen en el diseño de la red, comparando prestaciones y características e interpretando la documentación técnica asociada.

**CR5.3** Los procedimientos de salvaguarda del "software" se revisan, modificando en su caso la programación de los "backup", almacenándolos en condiciones de seguridad y permitiendo una eficaz recuperación.

**CR5.4** Los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros se revisan, ajustándolos de forma que garanticen la seguridad, la trazabilidad de los parámetros y las definiciones de configuración, estableciendo protocolos para el cambio cíclico de contraseñas fijas que no caducan, estableciendo mecanismos de control de acceso del equipo de red de forma que sólo puedan ser modificados desde puntos permitidos y por administradores autorizados.

**CR5.5** La configuración de seguridad en el ámbito de red se aplica garantizando el funcionamiento de puntos críticos, tales como la seguridad de puerto y configurando los mecanismos de control de tormentas de difusión, tales como el protocolo de árbol de expansión ("spanning-tree"), protocolos de redundancia ("Parallel Redundancy Protocol" -PRP-) y "Highly-available Seamless Redundancy" (HSR), entre otros.

**CR5.6** La documentación del "software" de seguridad se elabora incluyendo productos, referencias y todos los valores de configuración implantados, ajustándolo a estándares y según el formato establecido en la organización.

## Contexto profesional

### Medios de producción

Equipos informáticos tales como ordenadores de sobremesa, portátiles y servidores. Aplicaciones ofimáticas corporativas. "Software" para garantizar la confidencialidad e integridad de las comunicaciones. Programas de análisis de contraseñas. Sistemas para implantar autoridades de certificación digital. Servidores y clientes de redes privadas virtuales (VPN). Soportes seguros para certificados digitales. Servidores web con soporte SSL/TLS. Encapsuladores de tráfico con soporte criptográfico ("hardware" y "software"). Programas de conexión segura a servicios telemáticos. Interfaces de correo electrónico con soporte para correo seguro. Infraestructuras de Clave Pública (PKI) y dispositivos seguros de creación de firma (DNI electrónico, módulos PKCS y CSP, entre otros). Soluciones de prevención de fuga de datos (DLP).

### Productos y resultados

Protocolos y herramientas en operaciones de intercambio de datos implantados. Sistemas de firma y certificados de persona implantados. Infraestructuras de clave pública implementadas. "Hardware", "software" y diseño de la red de área local revisados y, en su caso, modificados para garantizar la seguridad de las comunicaciones y datos.

### Información utilizada o generada

Normas externas de trabajo (normativa aplicable de propiedad intelectual e industrial; normativa aplicable de protección de datos, seguridad informática y servicios de comunicaciones; estándares y recomendaciones de seguridad, normativa aplicable sobre prevención de riesgos laborales -ergonomía-). Normas internas de trabajo (plan de seguridad, metodologías de análisis de seguridad, relación de contraseñas débiles, informe de auditoría de servicios y puntos de acceso al sistema informático, normas internas de prevención de amenazas de seguridad, historial de ataques y vulnerabilidades). Documentación técnica (manuales de instalación de infraestructuras de clave pública (PKI), Entidades de certificación (CA), DNI electrónico, certificados digitales, "token"; boletines de seguridad externos y

avisos de vulnerabilidades; documentación técnica del fabricante de los equipos, sistemas y "software" utilizado; documentación técnica de la red, bibliografía especializada, tutoriales y cursos).

## MÓDULO FORMATIVO 1
SEGURIDAD EN EQUIPOS INFORMÁTICOS

*Nivel:* *3*
*Código:* *MF0486_3*
*Asociado a la UC:* *UC0486_3 - ASEGURAR EQUIPOS INFORMÁTICOS*
*Duración (horas):* *120*
*Estado:* *BOE*

### Capacidades y criterios de evaluación

**C1:** Aplicar procedimientos de configuración de seguridad de equipos informáticos instalando "software", configurando opciones del sistema operativo, entre otros, para protegerlos ante el riesgo de pérdida, manipulación y/o sustracción de información no autorizada.

**CE1.1** Definir tipos de usuario o roles, estableciendo los privilegios de acceso a los recursos (aplicaciones "software", carpetas, entre otros), según las funciones desempeñadas dentro de la organización.

**CE1.2** Crear cuentas de usuario, asignándolas a los tipos de usuarios definidos en el sistema informático.

**CE1.3** Configurar la política de contraseñas, estableciendo parámetros tales como complejidad, caducidad, revocación, bloqueo, reutilización, entre otros.

**CE1.4** Configurar el control de acceso al equipo informático, estableciendo parámetros tales como el número de intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros.

**CE1.5** Configurar un cortafuegos en el equipo informático, según las necesidades de uso del equipo, estableciendo reglas de filtrado de las conexiones entrantes y salientes.

**CE1.6** Aplicar medidas de seguridad a la información del equipo informático (integridad, accesos, entre otros), frente a riesgos de ataque malicioso, revisando la instalación y configuración del "software" de protección adecuado (EDP -"Endpoint Detection and Response"-, "anti-ransomware", "anti-malware", entre otros).

**CE1.7** Contrastar los procesos de recopilación, tratamiento y eliminación de la información por parte de los usuarios, comprobando que cumplen protocolos a seguir según el grado de confidencialidad de la información.

**CE1.8** Crear documentación informativa sobre la política de seguridad de la organización tal como, restricciones asignadas a equipos y usuarios, ámbitos de responsabilidades relativos a la utilización de los equipos informáticos, entre otros.

**C2:** Aplicar procedimientos de configuración de seguridad a equipos servidores, estableciendo mecanismos de registro de la actividad del servidor, deshabilitando los servicios no prestados, haciendo uso de protocolos de seguridad, entre otros.

**CE2.1** Identificar tipos de servicios (correo, web, entre otros) que puede ofrecer un servidor, describiendo su función y características.

**CE2.2** Identificar las amenazas existentes para cada tipo de servicio, describiendo las configuraciones a realizar para minimizar/proteger dicho servicio.

**CE2.3** Configurar un servicio (correo, web, entre otros) en un servidor, haciendo uso del entorno específico del servicio, estableciendo sus parámetros de configuración según unos valores dados.

**CE2.4** En un supuesto práctico de aseguramiento de un tipo de servidor, configurando los servicios necesarios para prestar su función (web, correo, entre otros) y deshabilitando los innecesarios:

- Identificar qué servicios están activos en el servidor, haciendo uso de la directiva correspondiente de sistema operativo específico y verificando su estado.
- Identificar los servicios que están activos que no se van a utilizar, deshabilitándolos del sistema operativo.
- Eliminar el "software" de los servicios deshabilitados, borrándolos del sistema operativo.

**CE2.5** Identificar los protocolos de seguridad (TLS -Transport Layer Security, Seguridad de la Capa de Transporte-, SSH -Secure Shell-, entre otros) utilizados en las comunicaciones con un tipo de servidor, describiendo sus características e indicando cómo se activan y configuran para un sistema operativo específico.

**CE2.6** Activar mecanismos de auditoría de la actividad e incidencias del servidor, configurando el registro de eventos del sistema y parametrizando valores tales como periodicidad, nivel de detalle (fecha, usuario, entre otros).

**CE2.7** Documentar las configuraciones realizadas e incidencias producidas, detallando el procedimiento llevado a cabo, las incidencias ocurridas (descripción, tipo, entre otros) y el correctivo aplicado para solventarlas, según procedimiento interno de la organización (plantillas, herramientas "software", entre otros).

**C3:** Aplicar procedimientos de borrado seguro y destrucción física de información en soportes y sistemas de almacenamiento de un equipo informático, haciendo uso de las técnicas de borrado y destrucción específicas al tipo de soporte de información.

**CE3.1** Identificar las técnicas de borrado o destrucción apropiadas para cada tipo de soporte (lógico, óptico, magnético o memorias de estado sólido), describiendo sus características y función.

**CE3.2** Redactar un protocolo de retención de datos, teniendo en cuenta la organización, búsqueda, acceso y eliminación de la información.

**CE3.3** Revisar los métodos de borrado o destrucción física aplicado en soportes de información, comprobando que el método o técnica utilizados se corresponde con el tipo de soporte [magnético, óptico, electrónico (SSD -"Solid State Drive", Unidad de Estado Sólido-)].

**CE3.4** En un supuesto práctico de borrado seguro de información de soporte de información de datos (IDE -"Integrated Drive Electronics"-, SATA -"Serial Advanced Technology Attachment"-, SCSI -"Small Computer System Interface"- y USB -"Universal Serial Bus"-), utilizando una herramienta "software" de borrado seguro:

- Comprobar que el equipo informático donde se va a instalar o utilizar la herramienta "software" de borrado seguro cumple los requisitos (tipo de procesador, tamaño de memoria, puerto USB, entre otros) para su instalación o uso y verificando que se encuentra aislado (sin conexión a red) y libre de "malware".
- Configurar el equipo informático para que permita el arranque desde USB, configurando la BIOS (Sistema básico de entrada/salida).

- Reinicia el equipo, introduciendo el dispositivo USB con la herramienta de borrado seguro antes de que comience el proceso de arranque.
- Hacer uso de la herramienta de borrado seguro, seleccionando los soportes con la información a borrar y el método de borrado a aplicar.
- Realizar el proceso de borrado seguro de los soportes de información seleccionados, obteniendo un informe de proceso terminado y guardándolo en el lugar indicado.
- Verificar que la información en los dispositivos de almacenamiento seleccionados ha sido borrada de forma segura, visualizando en el informe generado que el borrado se ha realizado sin ningún error.
- Documentar el trabajo realizado, indicando los dispositivos de almacenamiento, método de borrado y evidencias del proceso de borrado seguro.

**CE3.5** Registrar un procedimiento realizado de borrado o destrucción, generando un documento de certificación que detalle informaciones tales como, evidencias lógicas o gráficas del proceso, cuándo y cómo se ha realizado el proceso de destrucción o reutilización, especificaciones técnicas del "hardware", entre otras.

**C4:** Comprobar medidas de seguridad física a equipos servidores, verificando que su ubicación dispone de protección de acceso y condiciones ambientales específicas, entre otras.

**CE4.1** Revisar la ubicación física de servidores, comprobando que se encuentran situados en un espacio con acceso físico controlado y protegido.

**CE4.2** Comprobar las condiciones ambientales (temperatura, humedad) de la ubicación física de equipos servidores, verificando que se encuentran dentro del rango de trabajo óptimo considerado entre 17 y 21 grados.

**CE4.3** Revisar el sistema de alimentación ininterrumpida (SAI), comprobando que está operativo a través de su sistema de alertas.

**C5:** Aplicar técnicas de verificación de copias de seguridad, comprobando que la información a respaldar, la frecuencia de respaldo, entre otros, permite mantener la seguridad y disponibilidad de la información.

**CE5.1** Comprobar la información de un equipo informático, verificando que su clasificación en función de su criticidad y de su tipo (datos de sistema o datos de la organización) es acorde a un plan de copias de seguridad.

**CE5.2** Verificar un plan de copias de seguridad, comprobando que contempla los datos a guardar, su criticidad, tipo de salvaguarda, frecuencia de respaldo, entre otros.

**CE5.3** Comprobar dispositivos de almacenamiento de copias de respaldo (cintas, discos externos, entre otros), verificando que la información (fecha de la copia, información respaldada, entre otros) contenida en ellos se encuentra registrada en un plan de copias de seguridad.

**CE5.4** Verificar procedimientos de obtención y verificación de copias de seguridad, realizando pruebas de funcionamiento de los mismos.

## Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C2 respecto a CE2.4 y C3 respecto a CE3.4.

Otras Capacidades:

Mantener el área de trabajo con el grado apropiado de orden y limpieza.
Demostrar creatividad en el desarrollo del trabajo que realiza.
Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.
Interpretar y ejecutar instrucciones de trabajo.
Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

## Contenidos

### 1 Gestión de la seguridad y riesgos de un sistema informático

Seguridad: objetivo de la seguridad; amenazas; atacante externo e interno; tipos de ataque; mecanismos de protección. Riesgos: proceso de gestión de riesgos; métodos de identificación y análisis de riesgos; reducción del riesgo. Normativa de protección medioambiental (CO2, producción y gestión de residuos, entre otros).

### 2 Seguridad física en el sistema informático

Protección del sistema informático. Protección de los datos. Técnicas de borrado seguro y destrucción de información. Herramientas "software" de borrado seguro de información.

### 3 Seguridad lógica del sistema informático

Sistemas de ficheros. Permisos de archivos. Listas de control de acceso (ACLs) a ficheros. Registros de actividad del sistema. Autenticación de usuarios: sistemas de autenticación débiles; sistemas de autenticación fuertes; sistemas de autenticación biométricos. Introducción a la Criptografía y Establecimiento de Políticas de Contraseñas. Arquitectura del servicio de copias de respaldo: sistemas centralizados, sistemas distribuidos, copias locales. Planificación del servicio de copias de respaldo: niveles de copia de respaldo, dimensionamiento del servicio de copias de respaldo. Soportes para copias de respaldo: soportes tradicionales, jerarquías de almacenamiento.

### 4 Acceso remoto al sistema informático

Mecanismos del sistema operativo para control de accesos. Cortafuegos de servidor: filtrado de paquetes; cortafuegos de nivel de aplicación; registros de actividad del cortafuegos.

## Parámetros de contexto de la formación

### Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Taller de 4 m² por alumno o alumna.

- Instalación de 2 m² por alumno o alumna.

### Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con el aseguramiento de equipos informáticos, que se acreditará mediante una de las dos formas siguientes:

- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.

2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

## MÓDULO FORMATIVO 2

Auditoría de redes de comunicación y sistemas informáticos

*Nivel:* *3*
*Código:* *MF0487_3*
*Asociado a la UC:* *UC0487_3 - Auditar redes de comunicación y sistemas informáticos*
*Duración (horas):* *180*
*Estado:* *Tramitación BOE*

### Capacidades y criterios de evaluación

**C1:** Aplicar técnicas de comprobación de seguridad en el aplicativo de sistemas informáticos, revisando su configuración, para verificar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la información gestionada.

**CE1.1** Describir procedimientos de verificación del inventariado del aplicativo en equipos para comprobar versiones y confirmar que dicho inventario está actualizado, explicando los pasos a seguir.

**CE1.2** Describir procedimientos de comprobación del aplicativo, ya sea "software" de base, aplicaciones genéricas o específicas de seguridad, indicando como determinar si un aplicativo es legítimo y está actualizado.

**CE1.3** Explicar técnicas de revisión de la instalación y configuración de sistemas operativos, detallando los parámetros y valores o configuraciones que afectan a su seguridad.

**CE1.4** Definir los conceptos de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know"), explicando cómo determinar si una aplicación o un usuario lo cumple.

**CE1.5** Clasificar el "software" de seguridad contra programas maliciosos tales como antivirus/"antimalware", EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection and Response"), entre otros, indicando su utilidad y ámbito de aplicación.

**CE1.6** Explicar procedimientos de instalación y configuración de "software" de seguridad contra programas maliciosos, indicando parámetros y valores a comprobar, verificando que tiene activas unas funciones.

**CE1.7** Indicar los pasos a seguir para comprobar las cuentas de usuario de sistemas y aplicaciones, determinando su robustez y la aplicación del principio de "mínimo privilegio".

**CE1.8** En un supuesto práctico de aplicación de técnicas de comprobación de seguridad en el aplicativo de sistemas informáticos, revisando su configuración, para verificar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la información gestionada:

- Revisar un inventariado de activos, verificando el aplicativo en unos equipos existentes y sus características, comprobando las versiones que se ejecutan, para confirmar que está actualizado y no hay programas que no aparezcan en el mismo.
- Revisar la instalación y configuración de los sistemas operativos, confirmando que el "software" instalado es legítimo, está actualizado y tanto los usuarios como las aplicaciones cuentan con los permisos de "mínimo privilegio" para desempeñar sus funciones en el sistema.
- Comprobar la instalación y configuración de un "software" de seguridad contra programas maliciosos tales como antivirus/"antimalware", EPP ("Endpoint Protection Platform") y EDR

("Endpoint Detection and Response"), entre otros, verificando que el "software" es legítimo, está actualizado y tiene activas unas funciones indicadas.
- Revisar un conjunto de aplicaciones, comprobando licencias y versiones para confirmar que son legítimas, están actualizadas y únicamente pueden ser accedidas por un determinado personal y que ese acceso tenga unas limitaciones basadas en el principio de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know").
- Comprobar unas cuentas de usuario, verificando que son individuales, cuentan con una política de contraseñas robusta y han sido elaboradas bajo el principio de "mínimo privilegio" y segregación de funciones.
- Documentar las pruebas realizadas, incluyendo referencias a los activos del sistema, los parches y actualizaciones instalados en los sistemas operativos y aplicaciones, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

**C2:** Aplicar técnicas de comprobación de seguridad en equipos e instalaciones de un sistema informático, revisando el bastionado, para verificar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la información gestionada.

**CE2.1** Describir procedimientos de inventariado de activos y de verificación de equipos y sus características, explicando los pasos a seguir.

**CE2.2** Enumerar los elementos de protección de instalaciones y equipos, tales como mecanismos de apertura por usuario y contraseña, llave física, detectores biométricos entre otros, de modo que se asegure que están protegidos contra accesos físicos no autorizados, explicando su configuración y aplicación de manera separada o combinada.

**CE2.3** Describir procedimientos para aplicar políticas de "mesas limpias", indicando los puntos a comprobar.

**CE2.4** Describir las condiciones ambientales de temperatura y humedad para un sistema o instalación, localizando en la documentación los márgenes especificados por el fabricante, comprobando su aplicación efectiva.

**CE2.5** Indicar las posibles adaptaciones para la protección frente a desastres en una instalación, definiendo las características de emplazamiento y la protección aplicables según el riesgo.

**CE2.6** Explicar las protecciones frente a alteraciones tales como caídas del suministro eléctrico, picos de electricidad y ruido, describiendo su ámbito de aplicación y las posibles configuraciones a definir.

**CE2.7** En un supuesto práctico de aplicación de técnicas de comprobación de seguridad en equipos e instalaciones de un sistema informático, revisando el bastionado, para verificar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la información gestionada:
- Revisar un inventariado de activos, verificando los equipos existentes y sus características, para confirmar que no hay equipos que no aparezcan en el mismo.
- Comprobar unas instalaciones de manera presencial para asegurarse de que los equipos y la información están protegidos contra accesos físicos no autorizados, usando elementos al efecto de manera separada o combinada tales como mecanismos de apertura por usuario y contraseña, llave física, detectores biométricos entre otros, aplicando un sistema de aviso previo y bloqueando sesiones por inactividad y usando políticas de "mesas limpias".
- Comprobar unas instalaciones, verificando que se cumplen las condiciones ambientales de temperatura y humedad requeridas por los fabricantes para su funcionamiento y comprobando la protección contra desastres naturales que pueden afectar físicamente un emplazamiento y

previniendo posibles alteraciones del entorno tales como picos de electricidad o ruido eléctrico, entre otros.
- Documentar las pruebas realizadas durante la auditoría, incluyendo referencias a los activos del sistema y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

**C3:** Aplicar procedimientos de comprobación de la seguridad de una red, verificando elementos relativos, para prevenir posibles intrusiones, ataques y fugas de información.

**CE3.1** Enumerar técnicas de diseño, herramientas y aplicaciones de protección de una red, tales como VLAN, cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), "routers" y otros dispositivos de red, y creación de una zona aislada o desmilitarizada (DMZ), describiendo sus características, procedimiento de configuración y ámbito de aplicación.

**CE3.2** Describir procedimientos de revisión del diseño de la arquitectura de una red, mediante auditoría de caja blanca, explicando cómo comprobar que la red está configurada de forma que se minimice el impacto de posibles ataques del exterior y que todos los recursos que deben ser accesibles desde Internet, tales como páginas web y correo electrónico, se han instalado en una zona aislada o desmilitarizada (DMZ).

**CE3.3** Explicar procedimientos de revisión de dispositivos que controlan y gestionan el tráfico de la red tales como "router", "switch", "hub", cortafuegos, IDS, IPS, SIEM ("Security Information and Event Management"), entre otros, usando técnicas de caja blanca y de manera presencial y comprobando su configuración para comprobar que únicamente aceptan un tráfico permitido y están actualizados.

**CE3.4** Interpretar mensajes de error generados por los dispositivos de red, "routers", "switch", "hub" cortafuegos, IDS, IPS, SIEM y cualquier otro, revisándolos en forma de auditoría de caja blanca para asegurar que, de forma interna, registran cualquier anomalía para facilitar la gestión de incidentes y, de forma externa en modo auditoría de caja negra, para confirmar que no aportan información que permita a un posible atacante remoto obtener información de los puertos abiertos en el sistema.

**CE3.5** Detallar procedimientos de comprobación de acceso, garantizando que una red únicamente se accede de forma remota por determinado personal y bajo las condiciones de tiempo y lugar de origen previamente autorizados y sólo a través de las VPN (Redes privadas Virtuales).

**CE3.6** Explicar las formas de uso de programas o herramientas en la nube que proporciona un proveedor, indicando cómo comprobar que se lleva a cabo de una forma acordada y permitida.

**CE3.7** Reconocer protocolos de cifrado seguros en el uso de redes Wifi, indicando cómo verificar su configuración de modo que únicamente accedan a ellas personas autorizadas.

**CE3.8** Explicar procedimientos de comprobación de una conexión a Internet por parte de los usuarios, de modo que se verifique que únicamente pueden acceder a los servicios y contenidos determinados usuarios.

**CE3.9** Interpretar reglas de cortafuegos y sistemas de monitorización y/o servicios externos de protección anti DDoS (denegación de servicio), explicando cómo verificar que el sistema se encuentra protegido contra este tipo de ataques.

**CE3.10** En un supuesto práctico de aplicación de procedimientos de comprobación de la seguridad de una red, verificando elementos relativos, para prevenir posibles intrusiones, ataques y fugas de información:
- Revisar un diseño de arquitectura de una red, mediante auditoría de caja blanca, comprobando que la red está configurada de forma que se minimice el impacto de posibles

ataques del exterior: utilizando VLAN, cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), "routers" y otros dispositivos de red e instalando todos los recursos de la empresa que deben ser accesibles desde Internet tales como páginas web y correo electrónico, en una zona aislada o desmilitarizada (DMZ).
- Revisar unos dispositivos que controlan y gestionan el tráfico de la red tales como "router", "switch", "hub", cortafuegos, IDS, IPS, SIEM ("Security Information and Event Management"), entre otros, usando técnicas de caja blanca: de manera física y comprobando su configuración para comprobar que únicamente aceptan el tráfico permitido y están actualizados.
- Revisar en forma de auditoría de caja blanca mensajes de error generados por los dispositivos de red, "routers", "switch", "hub" cortafuegos, IDS, IPS, SIEM y cualquier otro, asegurando que registran cualquier anomalía para facilitar la gestión de incidentes y, de forma externa en modo auditoría de caja negra, para confirmar que no aportan información que permita a un posible atacante remoto obtener información de los puertos abiertos en el sistema.
- Comprobar que los elementos de la red únicamente son accedidos de forma remota por determinado personal y bajo ciertas condiciones de tiempo y lugar de origen y sólo a través de las VPN (Redes privadas Virtuales).
- Revisar el uso de programas o herramientas en la nube, verificando que se lleva a cabo de cierta forma supuestamente acordada con un proveedor del servicio.
- Comprobar una red Wifi, verificando que utilizan protocolos de cifrado seguros y que únicamente acceden a ellas personas determinadas previamente.
- Comprobar una conexión a Internet, verificando que únicamente pueden acceder a los servicios y contenidos personas previamente autorizadas.
- Documentar las pruebas realizadas durante la auditoría, incluyendo referencias a los activos inspeccionados, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.
- Verificar que están habilitados y funcionales los sistemas anti DDoS (Denegación de servicio), comprobando si se han configurado sistemas al efecto tales como reglas de cortafuegos, sistemas de monitorización y/o servicios externos de protección, entre otros.

**C4:** Aplicar procedimientos de comprobación de la seguridad de un sitio web, realizando pruebas de simulación de ataques para detectar posibles fallos de seguridad.

**CE4.1** Describir procedimientos de verificación de la instalación y configuración de unos sistemas de gestión de contenidos (CMS) y servidores web, explicando los pasos a seguir para comprobar que están instaladas las últimas versiones estables y que únicamente tienen instalados los módulos imprescindibles para su funcionamiento.

**CE4.2** Detallar el proceso de comprobación de cuentas de usuario de un sitio web, indicando las verificaciones a realizar para garantizar que son generadas bajo el principio de "mínimo privilegio" y cuentan con una política de acceso segura, bien mediante contraseñas robustas respecto a su composición, longitud y caducidad, entre otros, bien por autenticación multifactor (MFA).

**CE4.3** Explicar los pasos a seguir para verificar la información generada de forma pública por un servidor web y/o un sistema de gestión de contenidos (CMS), indicando las comprobaciones a realizar para que no muestre ninguna información que permita obtener fácilmente información relacionada con la configuración del sistema tal como tipo de programa empleado, versión, entre otros.

**CE4.4** Describir procedimientos de comprobación de la gestión de sesiones en el sistema, explicando los pasos para verificar que tanto las "cookies" como los "tokens" de sesión se

generan de forma segura y no predecible, para evitar que un atacante externo pueda aprovecharse de ellas para acceder al sistema de forma no autorizada.

**CE4.5** Reconocer mecanismos que impidan la entrada de caracteres que provoquen un comportamiento no deseado del sistema, tales como la introducción de código (por inyección de SQL o XSS, entre otros) o la generación de errores en el sistema (tal como por desbordamiento de "buffer" por introducción de cadenas largas en los formularios y puntos de acceso de información por parte del usuario), explicando los pasos para verificarlos.

**CE4.6** Aplicar técnicas de verificación de la gestión de errores y excepciones del sistema, explicando los pasos para verificar que éstos son registrados y que la información mostrada en el lado del cliente no revela información que pueda permitir a los usuarios una posterior explotación del fallo.

**CE4.7** Describir procedimientos de comprobación de que la información entre el cliente y el servidor se envía de forma segura, explicando los pasos para verificar que se realiza a través de protocolos tales como HTTPS y TLS y que la información enviada se cifra siguiendo estándares actualizados.

**CE4.8** En un supuesto práctico de aplicación de procedimientos de comprobación de la seguridad de un sitio web, realizando pruebas de simulación de ataques para detectar posibles fallos de seguridad:

- Verificar una instalación y configuración de un sistema de gestión de contenidos (CMS) o servidor web, comprobando que están instaladas las últimas versiones estables y que únicamente tienen instalados los módulos imprescindibles para su funcionamiento, revisando la documentación asociada.
- Comprobar cuentas de usuario del sitio web, verificando que son generadas bajo el principio de "mínimo privilegio" y cuentan con una política de acceso segura.
- Verificar la información generada de forma pública por el servidor web y/o sistema de gestión de contenidos (CMS), comprobando que no muestre ninguna información que permita obtener fácilmente información relacionada con la configuración del sistema tal como tipo de programa empleado, versión, entre otros.
- Comprobar la gestión de sesiones en el sistema, verificando que tanto las "cookies" como los "tokens" de sesión se generan de forma segura y no predecible, tal como evitando la numeración secuencial para la identificación de usuarios, para impedir que un atacante externo pueda aprovecharse de ellas para acceder al sistema de forma no autorizada.
- Comprobar unos formularios y puntos de acceso de información por parte del usuario, verificando que cuentan con mecanismos que impidan la entrada de caracteres que provoquen un comportamiento no deseado del sistema como la introducción de código (por inyección de SQL o XSS, entre otros) o la generación de errores en el sistema tales como desbordamiento de "buffer" por introducción de cadenas largas.
- Comprobar la gestión de errores y excepciones del sistema, verificando que éstos son registrados y la información mostrada en el lado del cliente no revela información que pueda permitir a los usuarios una posterior explotación del fallo.
- Comprobar que la información entre el cliente y el servidor se envía de forma segura, verificando que se realiza a través de protocolos tales como HTTPS y TLS y que la información enviada se cifra siguiendo estándares actualizados.
- Documentar las pruebas realizadas durante la auditoría, incluyendo referencias a los activos inspeccionados, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

**C5:** Aplicar procedimientos de comprobación de la seguridad de la información, verificando y asegurando elementos relativos, para garantizar la integridad, disponibilidad, confidencialidad, autenticidad y el "no repudio" y el cumplimiento de la normativa aplicable de protección de datos.

**CE5.1** Describir técnicas de comprobación de la asignación de roles de usuarios responsables de la gestión, tratamiento y almacenamiento de los datos, explicando los pasos para verificar que se accede a la información requerida en cada caso y su alineación con el principio de "mínimo privilegio" y "necesidad de saber".

**CE5.2** Identificar las medidas de seguridad físicas y lógicas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos, detallando cómo verificar que se cumple con los principios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio según normativa aplicable de protección de datos.

**CE5.3** Enumerar posibilidades para el intercambio de información, describiendo canales y mecanismos de autorización de acceso.

**CE5.4** Describir el contenido y características de un registro de actividades de tratamiento de los datos, explicando las comprobaciones de completitud y grado de actualización, así como el proceso de verificación de que el tratamiento únicamente se efectúa por personas autorizadas.

**CE5.5** Detallar procedimientos para el borrado seguro de la información, estableciendo los pasos a seguir en cada caso para la destrucción de soportes, uso de herramientas de borrado permanente, utilización de contenedores específicos que no permitan la recuperación de la información, entre otros, para que no se pueda acceder a la información contenida previamente en caso de deshecho, reutilización o cesión de dispositivos digitales a terceros.

**CE5.6** Explicar el proceso de verificación de la realización de copias de seguridad, describiendo los pasos a seguir para comprobar que es posible recuperar la información en unos plazos de tiempo.

**CE5.7** Indicar elementos de seguridad a revisar en los usos y costumbres de los usuarios describiendo cómo verificar elementos que afectan a la seguridad.

**CE5.8** En un supuesto práctico de aplicación de procedimientos de comprobación de la seguridad de la información, verificando y asegurando elementos relativos, para garantizar la integridad, disponibilidad, confidencialidad, autenticidad y el "no repudio" y el cumplimiento de la normativa aplicable de protección de datos:

- Comprobar una asignación de los roles de un hipotético personal responsable de la gestión, tratamiento y almacenamiento de los datos, verificando que cada rol accede a la información requerida en cada caso y su alineación con el principio de "mínimo privilegio" y "necesidad de saber".
- Comprobar unas medidas de seguridad físicas y lógicas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos, verificando que se cumple con los principios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio según normativa aplicable de protección de datos.
- Comprobar unos intercambios de información, verificando que se realiza únicamente a través de los canales autorizados, de la forma convenida y por unas personas definidas.
- Revisar un registro de actividades de tratamiento de datos personales, verificando que está completo y actualizado, comprobando que el tratamiento únicamente se efectúa por personas autorizadas en una normativa de seguridad de una hipotética organización.
- Revisar unos protocolos de eliminación de información, confirmando que garantizan el borrado seguro de la información, para que, en caso de cesión de dispositivos digitales a terceros, no se pueda acceder a la información contenida previamente en él.

- Verificar un proceso de realización de copias de seguridad, comprobando que está alineado con una política de seguridad de una hipotética organización, de forma que sea posible recuperar la información en unos plazos de tiempo.
- Revisar usos y costumbres de unos hipotéticos usuarios, verificando puntos que afectan a la seguridad tales como que saben cómo y dónde reportar los incidentes informáticos, no hacen uso de dispositivos no autorizados o de origen desconocido, aplican la política de "mesas limpias", bloquean el equipo si van a estar ausentes y no divulgan información asociada con su trabajo.
- Elaborar un informe de auditoría, incluyendo el alcance, la documentación revisada, las pruebas e hipotéticas entrevistas realizadas, los posibles obstáculos encontrados y las evidencias obtenidas, presentando especial atención a los hallazgos clasificados y no conformidades de las que también se indicará su criticidad, detallando el grado de cumplimiento legal y las medidas de mejora convenientes.

## Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.8; C2 respecto a CE2.7; C3 respecto a CE3.10; C4 respecto a CE4.8 y C5 respecto a CE5.8.

### Otras Capacidades:

Demostrar un buen hacer profesional.
Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Mantener una actitud asertiva, empática y conciliadora con los demás demostrando cordialidad y amabilidad en el trato.
Respetar los procedimientos y normas internas de la organización.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

## Contenidos

### 1 Normativa y estándares relacionados con la auditoría de seguridad

Normativa aplicable de servicios de Internet. Normativa aplicable de protección de datos. Estándares aplicables a la auditoría.

### 2 Auditoría de seguridad en el aplicativo de sistemas informáticos

Procedimientos de verificación del inventariado del aplicativo en equipos. "Software" de base, aplicaciones genéricas o específicas de seguridad. Comprobación y actualización de versiones. Comprobación de legitimidad del "software". Técnicas de revisión de la instalación y configuración de sistemas operativos. Parámetros y valores de configuración que afectan a la seguridad. Conceptos de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know"). Determinación del grado de cumplimiento en el acceso a aplicaciones. Clasificaciones de "software" de seguridad contra programas maliciosos. Antivirus/"antimalware", EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection and Response"). Utilidad y ámbito de aplicación. Instalación y configuración de "software" de seguridad contra programas maliciosos. Parámetros y valores a comprobar. Verificación de Funciones activadas y desactivadas. Comprobación de cuentas de usuario de sistemas y aplicaciones. Robustez de contraseñas y aplicación del principio de "mínimo privilegio". Informes de auditoría de sistemas.

### 3 Auditoría de seguridad en equipos e instalaciones de un sistema informático

Procedimientos de inventariado de activos y de verificación de equipos y sus características. Elementos de protección de instalaciones y equipos. Mecanismos de apertura por usuario y contraseña, llave física, detectores biométricos entre otros, de modo que se asegure que están protegidos contra accesos físicos no autorizados. Configuración y aplicación de manera separada o combinada. Aplicación de políticas de "mesas limpias". Puntos a comprobar. Verificación de condiciones ambientales de temperatura y humedad para un sistema o instalación. Verificación de protección frente a desastres en una instalación. Características de emplazamiento. Valoración de riesgos. Verificación de protecciones frente a alteraciones. Protección frente a caídas del suministro eléctrico, picos de electricidad y ruido.

## 4 Auditoría de seguridad en redes

Intrusiones, ataques y fugas de información. Técnicas de diseño, herramientas y aplicaciones de protección de redes. VLAN, cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), "routers" y otros dispositivos de red, y creación de una zona aislada o desmilitarizada (DMZ). Configuración y ámbito de aplicación. Revisión del diseño de la arquitectura de una red. auditorías de caja blanca y caja negra. Determinación de recursos accesibles. Zonas aisladas o desmilitarizadas (DMZ). Revisión de dispositivos que controlan y gestionan el tráfico de la red. "Router", "switch", "hub", cortafuegos, IDS, IPS, SIEM ("Security Information and Event Management"). Auditoría de caja blanca para comprobación de configuración. Auditoría de caja negra para comprobación del acceso y visibilidad. Interpretación de mensajes de error generados por los dispositivos de red. Comprobación de acceso. Garantía de acceso únicamente a personal autorizado. Condiciones de tiempo y lugar de origen. VPN (Redes privadas Virtuales). Formas de uso de programas o herramientas en la nube según proveedores. Comprobaciones de cumplimiento de la seguridad. Protocolos de cifrado seguros en redes Wifi. Verificación de configuración de acceso. Comprobación de conexión hacia Internet. Verificación de acceso a servicios y contenidos para determinados usuarios. Verificación de la protección anti DDoS (Denegación del servicio). Informes de auditoría de la red.

## 5 Auditoría de seguridad web

Verificación de la instalación y configuración de sistemas de gestión de contenidos (CMS) y servidores web. Comprobación de cuentas de usuario de un sitio web. Garantía del principio de "mínimo privilegio". Robustez de la política de contraseñas. Autenticación multifactor (MFA). Verificación de la información pública de un servidor web y/o un sistema de gestión de contenidos (CMS). Comprobaciones de visibilidad de información: tipo de programa y versión, entre otros. Procedimientos de comprobación de la gestión de sesiones en el sistema. Verificación de "cookies" y "tokens" de sesión seguros y no predecibles. Verificación de mecanismos de protección ante entradas de caracteres que provoquen un comportamiento no deseado del sistema. Introducción de código (por inyección de SQL o XSS, entre otros). Comprobación de protección ante generación de errores en el sistema. Desbordamiento de "buffer". Verificación de la gestión de errores y excepciones del sistema. Registro. Visibilidad de la información mostrada en el lado del cliente. Comprobación de envío seguro de la información entre el cliente y el servidor. Uso de protocolos tales como HTTPS y TLS. Cifrado de información enviada. Estándares. Informes de auditoría web. Sistemas WAF ("Web Application Firewall").

## 6 Auditoría de protección de datos

Integridad, disponibilidad, confidencialidad, autenticidad, "no repudio" y trazabilidad de procesos. Comprobación de la asignación de roles de usuarios responsables de la gestión, tratamiento y almacenamiento de los datos. Alineación con el principio de "mínimo privilegio" y "necesidad de saber". Comprobación de medidas de seguridad físicas y lógicas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos. Comprobaciones sobre el

intercambio de información. Canales y control del acceso. Verificación del registro de actividades de tratamiento de datos. Comprobaciones de completitud y grado de actualización. Verificación del acceso por personas autorizadas. Verificación del borrado seguro de la información. Destrucción de soportes. Herramientas de borrado permanente. Contenedores específicos de soportes desechados. Revisión y verificación de usos y costumbres del usuario que afectan a la seguridad. Verificación de la realización de copias de seguridad. Informes de auditoría de protección de datos.

## Parámetros de contexto de la formación

### Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Instalación de 2 m² por alumno o alumna.

### Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la auditoría de redes de comunicación y sistemas informáticos, que se acreditará simultáneamente mediante las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 3 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

## MÓDULO FORMATIVO 3

Gestión de incidentes de ciberseguridad

*Nivel:* *3*
*Código:* *MF0488_3*
*Asociado a la UC:* *UC0488_3 - Gestionar incidentes de ciberseguridad*
*Duración (horas):* *120*
*Estado:* *Tramitación BOE*

### Capacidades y criterios de evaluación

**C1:** Aplicar procedimientos de respuesta ante incidentes y mecanismos para la detección de intrusos según directrices ante incidentes nacionales e internacionales para los equipos de respuesta.

**CE1.1** Reconocer la estructura y contenidos de la documentación relativa a procedimientos de detección y respuesta de incidentes, verificando que estén documentados, que indican los roles y responsabilidades de seguridad y que implementan los requerimientos de la política de seguridad de la organización.

**CE1.2** Aplicar técnicas de modelización de los sistemas, seleccionando los mecanismos de registro a activar, observando las alertas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones y signos de comportamiento sospechoso a partir de indicadores de compromiso (IOC: "Indicator of Compromise") facilitados por equipos de respuesta ante incidentes nacionales e internacionales.

**CE1.3** Describir los mecanismos de registro del sistema, verificándolos y contrastándolos con unas especificaciones de seguridad y/o mediante un sistema de indicadores y métricas.

**CE1.4** Explicar procedimientos de detección de los comportamientos no habituales, mediante un sistema de indicadores y métricas y los mecanismos de análisis de registros, explicando los pasos a seguir para su comprobación y verificación.

**CE1.5** Detallar procedimientos de instalación, configuración y actualización de los sistemas de detección de intrusos (IDS), indicando cómo verificarlos en función de unas especificaciones de seguridad y/o mediante un sistema de indicadores y métricas.

**CE1.6** Describir procesos de verificación de los procedimientos de restauración del sistema informático, establecidos en un Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan"), explicando cómo recuperar el sistema ante un incidente grave.

**CE1.7** En un supuesto práctico de aplicación de procedimientos de respuesta ante incidentes y mecanismos para la detección de intrusos según directrices ante incidentes nacionales e internacionales para los equipos de respuesta:

- Los procedimientos de detección y respuesta de incidentes se localizan, verificando que están documentados, que indican los roles y responsabilidades de seguridad y que implementan los requerimientos de la política de seguridad de la organización.
- La modelización de los sistemas se efectúa, seleccionando los mecanismos de registro a activar, observando las alertas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones y signos de comportamiento sospechoso a partir de indicadores de compromiso (IOC: "Indicator of Compromise") facilitados por equipos de respuesta ante incidentes nacionales e internacionales.

- La activación de los mecanismos de registro del sistema se verifica, contrastándolos con las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.
- La planificación de los mecanismos de análisis de registros se verifica, de forma que se garantice la detección de los comportamientos no habituales, mediante un sistema de indicadores y métricas.
- La instalación, configuración y actualización de los sistemas de detección de intrusos (IDS) se verifica en función de las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.
- Los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan") definido por la organización, se verifican, comprobando que pueden recuperarse en tiempo y forma ante un incidente grave.

**C2:** Aplicar técnicas activas y preventivas de detección de incidentes y minimización de riesgos, según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.

**CE2.1** Enumerar herramientas de detección de intrusiones, (IDS: "Intrusion Detection System") o "antimalware" entre otros, describiendo su ámbito de aplicación y características para la detección de programas maliciosos según tipología.

**CE2.2** Señalar repositorios de guías y directrices nacionales e internacionales para la detección y prevención de intrusiones, clasificándolos por ámbito de aplicación.

**CE2.3** Describir técnicas para comprobar que las herramientas utilizadas para detectar intrusiones no han sido comprometidas ni afectadas por programas maliciosos, analizándolas siguiendo las guías y directrices de los equipos de respuesta nacionales e internacionales.

**CE2.4** Enumerar herramientas específicas de análisis y detección de parámetros de funcionamiento sospechosos tales como sistemas de Gestión de información y eventos de seguridad (SIEM: "Security Information and Event Management") e IDS, describiendo sus funcionalidades y características.

**CE2.5** Clasificar programas específicos de verificación de integridad de componentes "software" del sistema, explicando su funcionalidad y características.

**CE2.6** Describir dispositivos de protección física, explicando los mecanismos para su verificación por medio de los registros de cada sistema, pruebas específicas, pruebas de estrés, entre otras.

**CE2.7** Explicar procedimientos de detección, análisis y registro de sucesos y signos extraños que pudieran considerarse una alerta, delimitando la gravedad de los mismos, especificando para cada suceso información tal como: día y hora de la detección, persona que lo comunicó, sistemas implicados y acciones realizadas, entre otros.

**CE2.8** Enumerar fuentes abiertas (OSINT: "Open Source Intelligence"), clasificándolas según las características de cada hipotética entidad, consultándolas a través usando medios de comunicación, Internet, datos gubernamentales, publicaciones profesionales entre otras para la verificación de la exposición de datos filtrados.

**CE2.9** Enumerar centros de respuesta ante incidentes nacionales y/o internacionales, localizando la ubicación de fuentes y recursos para la consulta periódica de alertas.

**CE2.10** En un supuesto práctico de aplicación de técnicas activas y preventivas de detección de incidentes y minimización de riesgos según directrices de los equipos de respuesta ante incidentes nacionales e internacionales:

- Comprobar que unas herramientas utilizadas para detectar intrusiones no han sido comprometidas ni afectadas por programas maliciosos analizándolas siguiendo las guías y directrices de los equipos de respuesta nacionales e internacionales.

- Detectar funcionamientos sospechosos analizando parámetros de funcionamiento tales como conexiones no autorizadas, mensajes de alerta de los sistemas de detección de intrusiones (IDS: "Intrusion Detection System") o "antimalware" entre otros, usando herramientas específicas tales como sistemas de Gestión de información y eventos de seguridad (SIEM: "Security Information and Event Management") e IDS, entre otras.
- Verificar la integridad de unos componentes "software" en un sistema, usando programas específicos.
- Verificar el funcionamiento de unos dispositivos de protección física por medio de los registros de cada sistema, pruebas específicas, pruebas de estrés, entre otras.
- Recoger sucesos y signos extraños que pudieran considerarse una alerta en un informe para su posterior análisis, en función de la gravedad de los mismos, especificando para cada uno ítems tales como día y hora de la detección, persona hipotética que lo comunicó, sistemas implicados y acciones realizadas, entre otros.
- Verificar la exposición o filtración de los datos en una hipotética entidad, consultando fuentes abiertas (OSINT: "Open Source Intelligence") según las características de dicha organización.
- Comprobar la información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales, verificándola de manera periódica para establecer en su caso los mecanismos de seguridad recomendados en caso de exposición a las amenazas publicadas.

**C3:** Aplicar procedimientos de coordinación de respuestas ante incidentes de seguridad, activando mecanismos para contenerlos y solucionarlos según unos requisitos de servicio.

**CE3.1** Describir la aplicación de protocolos de respuesta ante la detección de un incidente de seguridad, explicando su localización, estructura, contenidos y situaciones que activan su aplicación y roles de las personas responsables de cada actuación.

**CE3.2** Explicar procedimientos de recogida de información para el análisis forense de un sistema vulnerado, previo aislamiento del sistema, capturando una imagen precisa, anotando de manera detallada (incluyendo fechas y horas indicando si se utiliza horario local o UTC), recogiendo la información según el orden de volatilidad (de mayor a menor) entre otras.

**CE3.3** Enumerar mecanismos de contención de intrusiones, en función de la tipología de la misma y la estructura del sistema.

**CE3.4** Describir posibles acciones para continuar la prestación de servicios en un sistema vulnerado, explicando los pasos para determinar unos daños causados y planificar la recuperación del servicio.

**CE3.5** En un supuesto práctico de respuesta ante un incidente hipotético, activando mecanismos para contenerlo y solucionarlo según unos requisitos de servicio:
- Recoger información para el análisis forense del sistema vulnerado, una vez aislado el sistema, capturando una imagen tan precisa como sea posible, realizando notas detalladas (incluyendo fechas y horas indicando si se utiliza horario local o UTC), recogiendo la información según el orden de volatilidad (de mayor a menor) entre otras.
- Determinar las características de la intrusión, analizando el sistema atacado mediante herramientas de detección de intrusos (IDS), usando las facilidades específicas de cada herramienta.
- Contener la intrusión para limitar el alcance de los daños, realizando actuaciones tales como desconexión de equipos y/o segmentos de red y cierre de puertos, entre otros.
- Elaborar documentación de un incidente, recogiendo todas las acciones realizadas y las conclusiones obtenidas se realiza para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido, manteniendo de esta forma un registro de lecciones aprendidas ("Lessons Learned").

- Planificar posibles acciones para continuar la normal prestación de servicios del sistema vulnerado a partir de la determinación de los daños causados, cumpliendo los criterios de calidad de servicio y requisitos funcionales de explotación.

**C4:** Definir procedimientos de implantación de planes de prevención y concienciación en ciberseguridad, para facilitar la previsión de ciberincidentes y su respuesta en caso de producirse, según los requisitos de servicio.

**CE4.1** Determinar los medios utilizables para la difusión de medidas de ciberseguridad tales como correo electrónico, intranet corporativa, listas de distribución y sesiones específicas, entre otros.

**CE4.2** Especificar instrucciones para la protección de puestos de trabajo, incluyendo ítems tales como escenarios y ejemplos de riesgo y medidas de seguridad, entre otros.

**CE4.3** Enumerar documentos a incluir en un plan de concienciación de ciberseguridad dirigido a los empleados, especificando contenidos y estructura de los mismos para elaborar material de cursos o tutoriales para su difusión o impartición.

**CE4.4** En un supuesto práctico de definición de procedimientos de implantación de planes de prevención y concienciación en ciberseguridad, para facilitar la previsión de ciberincidentes y su respuesta, en caso de producirse, según los requisitos de servicio y dentro de las directivas de la organización:

- Establecer una normativa de protección de puestos de trabajo, incluyendo ítems tales como escenarios y ejemplos de riesgo y medidas de seguridad, entre otros.
- Definir un plan de concienciación de ciberseguridad dirigido a hipotéticos empleados, elaborando material y cursos o tutoriales para su difusión o impartición.
- Simular la difusión de medidas de ciberseguridad, usando medios tales como correo electrónico, intranet corporativa, listas de distribución y sesiones específicas, entre otros.
- Simular la difusión de material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a hipotéticos empleados, usando mecanismos tales como correo electrónico, plataformas web de difusión, aulas y canales de vídeo para cursos, entre otros.

## Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.7; C2 respeto a CE2.10; C3 respecto a CE3.5 y C4 respecto a CE4.4.

### Otras Capacidades:

Demostrar un buen hacer profesional.
Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Mantener una actitud asertiva, empática y conciliadora con los demás demostrando cordialidad y amabilidad en el trato.
Respetar los procedimientos y normas internas de la organización.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

## Contenidos

### 1 Prevención de incidentes de ciberseguridad y preparación de la respuesta

Documentación de procedimientos de detección y respuesta de incidentes. Roles y responsabilidades de seguridad. Mecanismos de registro de sistemas. Activación: indicadores y métricas. Alertas (parámetros de utilización de la red, inventariado de archivos a vigilar, indicadores

de compromiso -IOC: "Indicator of Compromise"-). Procedimientos de detección de los comportamientos no habituales. Análisis de registros, indicadores y métricas. Procedimientos de instalación, configuración y actualización de los sistemas de detección de intrusos (IDS). Verificación de los procedimientos de restauración del sistema informático. Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan"). Normativa aplicable de protección de datos. Estándares específicos de la tecnología afectada.

### 2 Detección de incidentes de ciberseguridad

Herramientas de detección de intrusiones, (IDS: "Intrusion Detection System"). "Antimalware". Ámbito de aplicación y características. Tipología de ataques y programas maliciosos. Repositorios de guías y directrices nacionales e internacionales para la detección y prevención de intrusiones. Procedimientos de comprobación de integridad en herramientas de detección de intrusiones. Herramientas específicas de análisis y detección de parámetros de funcionamiento sospechosos. Sistemas de Gestión de información y eventos de seguridad (SIEM: "Security Information and Event Management"). Herramientas específicas de verificación de integridad de componentes "software" del sistema. Dispositivos de protección física. Mecanismos de verificación: registros del sistema, pruebas específicas, pruebas de estrés, entre otras. Procedimientos de detección, análisis y registro de sucesos y signos anormales. Fuentes abiertas (OSINT: "Open Source Intelligence"). Centros de respuesta ante incidentes nacionales y/o internacionales.

### 3 Respuesta ante incidentes de ciberseguridad

Aislamiento del sistema. Mecanismos de contención de intrusiones. Orquestación, organización, automatización y respuesta de la seguridad (SOAR). Recogida de información. Análisis forense.

### 4 Prevención y concienciación en ciberseguridad

Medios de difusión. Correo electrónico, intranet corporativa, listas de distribución y sesiones específicas, entre otros. Protección de puestos de trabajo. Escenarios y ejemplos de riesgo y medidas de seguridad. Plan de concienciación de ciberseguridad. Cursos y tutoriales.

## Parámetros de contexto de la formación

### Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Instalación de 2 m² por alumno o alumna.

### Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la gestión de incidentes de ciberseguridad, que se acreditará simultáneamente mediante las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 3 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

## MÓDULO FORMATIVO 4

Implementación de sistemas seguros de acceso y transmisión de datos

| | |
|---|---|
| *Nivel:* | *3* |
| *Código:* | *MF0489_3* |
| *Asociado a la UC:* | *UC0489_3 - Implementar sistemas seguros de acceso y transmisión de datos* |
| *Duración (horas):* | *180* |
| *Estado:* | *Tramitación BOE* |

### Capacidades y criterios de evaluación

**C1:** Aplicar procedimientos de implantación de protocolos y herramientas en operaciones de intercambio de datos según las necesidades de uso, garantizando la integridad y confidencialidad de la información y el control de acceso, para obtener comunicaciones o canales de comunicación seguros.

**CE1.1** Describir el procedimiento de implantación de redes privadas virtuales para garantizar la comunicación a través de redes públicas, explicando los pasos a seguir.

**CE1.2** Enumerar técnicas de protección de conexiones inalámbricas disponibles en el mercado, detallando su aplicación y configuración, aportando información sobre el grado de confianza en función de las vulnerabilidades detectadas y publicadas.

**CE1.3** Explicar el "principio de proporcionalidad" aplicable al ámbito de la garantía de seguridad y concretando su uso para la selección de protocolos en redes inalámbricas describiendo sus características.

**CE1.4** Enumerar servicios que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones, indicando sus ventajas, desventajas y contexto de aplicación y explicando cómo diferenciar usuarios por perfiles y los pasos para configurar sus permisos.

**CE1.5** Identificar herramientas de cifrado extremo a extremo, para garantizar la seguridad de las comunicaciones, explicando sus características y aplicaciones.

**CE1.6** Describir el procedimiento de implantación y configuración de certificados digitales para garantizar la identidad de servidores, indicando aquellos servicios que lo soportan.

**CE1.7** Enumerar técnicas de seguridad para la autenticación de doble o triple factor, tales como las basadas en certificados de usuario, DNI electrónico, "token", biométricos u otros mecanismos, indicando su grado de fortaleza y posibles vulnerabilidades.

**CE1.8** Indicar el procedimiento a seguir para configurar servicios en los que se utiliza autenticación basada en contraseñas, estableciendo políticas de complejidad, renovación, bloqueo, almacenamiento y/o recuperaciones.

**CE1.9** En un supuesto práctico de aplicación de procedimientos de implantación de protocolos y herramientas en operaciones de intercambio de datos según las necesidades de uso, garantizando la integridad y confidencialidad de la información y el control de acceso para obtener comunicaciones o canales de comunicación seguros:

- Garantizar la confidencialidad e integridad en unas comunicaciones durante el tránsito a través de redes públicas, haciendo uso de redes privadas virtuales, comunicándolos al proveedor del servicio.

- Aplicar técnicas de protección de conexiones inalámbricas disponibles en el mercado, seleccionando aquellas basadas en estándares reconocidos como confiables en el sector, para cubrir vulnerabilidades, teniendo en cuenta el principio de proporcionalidad.
- Implantar unos servicios accesibles a través de la red telemática y que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones se implantan, diferenciando usuarios por perfiles y asignándoles permisos según ese perfil.
- Proteger unos servicios accesibles a través de la red telemática y que no incorporan técnicas criptográficas, usando herramientas disponibles para el cifrado extremo a extremo, para garantizar la seguridad de las comunicaciones.
- Garantizar la identidad de unos servidores en aquellos servicios que lo soportan, usando certificados digitales, configurando las aplicaciones cliente con el certificado raíz de confianza que garantice al usuario la autenticidad del servidor.
- Documentar las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas, incluyendo las características de las configuraciones aplicadas y en un formato establecido y ajustado a estándares.
- Asegurar unos servicios incorporando una autenticación de doble o triple factor basada en certificados de usuario, DNI electrónico, "token", biométricos u otros mecanismos.
- Configurar unos servicios en los que se utiliza autenticación basada en contraseñas, estableciendo reglas de complejidad, renovación, bloqueo, almacenamiento y/o recuperaciones.

**C2:** Aplicar procedimientos para la implantación del uso de sistemas de firma y certificados de persona, para asegurar la autenticidad, integridad, confidencialidad y "no repudio" de los datos que intervienen en una transferencia de información personal, según las necesidades de uso.

**CE2.1** Detallar el procedimiento a seguir para acceder a servicios a través de una red telemática mediante autenticación mutua de cliente y servidor, utilizando autenticación del cliente basada en certificados digitales de identidad personal.

**CE2.2** Describir el proceso de obtención y verificación de certificados digitales de identidad personal, indicando los pasos que establece una entidad certificadora.

**CE2.3** Explicar mecanismos para la transmisión cifrada del correo electrónico y otras comunicaciones, ya sea interpersonales o entre procesos y/o componentes, empleando certificados digitales para firmar y cifrar extremo a extremo el contenido de dichos mensajes y describiendo los pasos a seguir para su configuración y utilización.

**CE2.4** Enumerar mecanismos y opciones de firma digital de documentos, explicando cómo incluir dicha firma en el momento del envío o, en su caso, al almacenar cada documento.

**CE2.5** Identificar sistemas de sellado digital de tiempo, describiendo su aplicación a documentos u otros elementos, para garantizar la existencia de un documento electrónico en un instante concreto, garantizando que la información contenida no ha sido alterada por terceros.

**CE2.6** Describir el proceso de garantía de integridad de los componentes en sitios web y del "software" interno, explicando cómo usar la firma digital para conseguirlo.

**CE2.7** En un supuesto práctico de aplicación de procedimientos para la implantación del uso de sistemas de firma y certificados de persona para asegurar la autenticidad, integridad y confidencialidad de los datos que intervienen en una transferencia de información personal según las necesidades de uso:
- Implantar el acceso a unos servicios a través de la red telemática de forma que asegure la autenticación mutua de cliente y servidor, utilizando autenticación del cliente basada en certificados digitales de identidad personal.

- Aplicar el proceso de obtención y verificación de certificados digitales de identidad personal, siguiendo los pasos establecidos por la entidad certificadora.
- Implementar unos mecanismos para la transmisión cifrada del correo electrónico y otras comunicaciones, ya sea interpersonales o entre procesos y/o componentes, empleando certificados digitales para firmar y cifrar extremo a extremo el contenido de dichos mensajes, en los casos que indique la política de seguridad de la organización.
- Aplicar una firma digital a unos documentos de varios tipos, incluyendo dicha firma en el momento de un envío o, en su caso, al almacenarlos.
- Aplicar el sellado digital de tiempo a documentos electrónicos de varios tipos, garantizando su existencia en un instante concreto y que no ha sido alterado por terceros, siguiendo las instrucciones del fabricante.
- Firmar digitalmente componentes de un sitio web y "software", garantizando su integridad según el procedimiento del sistema o herramienta de firmado.
- Documentar unos sistemas de firma digital implantados, indicando su ámbito de aplicación, el procedimiento para su uso, la tipología de documentos y aplicaciones a firmar y el sistema de firma aplicado, entre otros, usando un formato y ajustándolo a estándares.

**C3:** Aplicar procesos de implementación de infraestructuras de clave pública, siguiendo instrucciones del fabricante y en función de las condiciones de uso, para garantizar la seguridad, según los estándares del sistema.

**CE3.1** Describir el proceso de instalación de una jerarquía de certificación, configurando la herramienta que la implementa siguiendo las instrucciones del proveedor y en función del uso que se vaya a dar a los certificados.

**CE3.2** Explicar el proceso de redacción de una declaración de prácticas de certificación y una política de certificación, describiendo la definición los procedimientos, derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.

**CE3.3** Definir el procedimiento de instalación de un sistema de autoridad de certificación, según indicaciones del fabricante y las prácticas recomendadas del sector.

**CE3.4** Describir el procedimiento de emisión de certificados digitales, según los usos que van a recibir los certificados y siguiendo los procedimientos indicados en una declaración de prácticas de certificación.

**CE3.5** Explicar los pasos a seguir para verificar que la validez de los certificados emitidos por la autoridad de certificación es mantenida por el servicio de revocación de certificados, según lo indicado en la declaración de prácticas de certificación.

**CE3.6** En un supuesto práctico de aplicación de procesos de implementación de infraestructuras de clave pública siguiendo instrucciones del fabricante y en función de las condiciones de uso, para garantizar la seguridad, según los estándares del sistema:
- Instalar una jerarquía de certificación, configurando la herramienta que la implementa siguiendo las instrucciones del proveedor y en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.
- Redactar una declaración de prácticas de certificación y una política de certificación definiendo los procedimientos, derechos y obligaciones de los responsables de la autoridad de certificación y de los hipotéticos usuarios.
- Instalar un sistema de autoridad de certificación, siguiendo las indicaciones del fabricante, las prácticas recomendadas del sector y de acuerdo con una política de seguridad.
- Publicar el certificado digital de la autoridad de certificación y su política asociada, en un lugar accesible por los hipotéticos usuarios para su consulta, siguiendo las directrices contenidas en la declaración de prácticas de certificación.

- Almacenar la clave privada de la autoridad de certificación, manteniéndola segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.
- Emitir los certificados digitales según los usos que van a recibir los certificados y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.
- Verificar la validez de los certificados emitidos por la autoridad de certificación, comprobando que es mantenida por el servicio de revocación de certificados, según lo indicado en la declaración de prácticas de certificación.
- Las infraestructuras de clave pública implantadas se documentan, recogiendo sus datos de configuración, según un formato o plantilla.

**C4:** Aplicar técnicas para revisar el "hardware" y el diseño de la red de área local, aplicando adaptaciones para garantizar la seguridad de las comunicaciones y la protección de los datos en las mismas.

**CE4.1** Describir modelos de referencia estándar que satisfagan requerimientos de seguridad, localizando los aspectos que son de interés para la revisión de la topología en lo concerniente a la seguridad.

**CE4.2** Explicar las modificaciones topológicas en una red que afectan a la seguridad, tales como adición o supresión de dispositivos de comunicaciones, establecimiento de subredes perimetrales de aislamiento o desmilitarizadas (DMZ), entre otros, describiendo cómo y en qué puntos se mejora la protección y los pasos para su configuración para minimizar riesgos.

**CE4.3** Detallar técnicas de segmentación de una red, ya sea de forma física mediante equipos tales como "routers" o lógica utilizando VLAN ("Virtual Local Área Networks"), explicando el proceso de implementación para cumplir con la compartimentación organizativa de una empresa, separando en función de la identidad de los equipos o de los usuarios y la política de seguridad.

**CE4.4** Explicar la tipología de las reglas o pautas de filtrado perimetral entre segmentos de la red y, en su caso, entre máquinas específicas, describiendo cómo se establecen, de acuerdo con una segmentación y una política de seguridad.

**CE4.5** Enumerar mecanismos de protección para las redes y de acceso que rompen con el perímetro tradicional de la red corporativa, tales como redes inalámbricas y dispositivos móviles y portátiles, particulares o corporativos, con conexión a las redes de la organización, detallando cómo se establecen, identificando los dispositivos empleados, para delimitar su alcance y proteger el acceso mediante cifrado seguro de acuerdo con una política de seguridad.

**CE4.6** Describir mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention"), explicando los pasos para su implementación, mediante instalación de "hardware" o "software" al efecto, para detectar potenciales brechas de datos/transmisiones de datos y prevenirlas a través de monitoreo, detección y bloqueo de información sensible.

**CE4.7** Aplicar procedimientos para proporcionar redundancia, alta disponibilidad y tolerancia a fallos a la red troncal, mediante configuración de unos equipos que la gestionan, para asegurar una transmisión de datos confiable y segura entre los nodos que la conforman.

**CE4.8** Explicar procedimientos de salvaguarda de configuraciones, para su revisión, indicando características y parámetros configurables para la programación de copias de seguridad de las mismas, y los pasos a seguir para almacenarlas en condiciones de seguridad y de modo que permitan una eficaz recuperación.

**CE4.9** En un supuesto práctico de aplicación de técnicas para revisar el "hardware" y el diseño de la red de área local, aplicando adaptaciones para garantizar la seguridad de las comunicaciones y la protección de los datos en las mismas:
- Adaptar la topología de una red, valorando mediante el análisis de modelos de referencia estándar que se satisfagan los requerimientos de seguridad, seleccionando la nueva topología y

añadiendo o suprimiendo dispositivos de comunicaciones, teniendo en cuenta la valoración realizada y minimizando riesgos.
- Segmentar la red, ya sea de forma física mediante equipos tales como "routers" o lógica utilizando VLAN ("Virtual Local Área Networks"), de acuerdo con una compartimentación organizativa y/o la identidad de los equipos o los usuarios.
- Establecer unas políticas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, de acuerdo con la segmentación establecida y una política de seguridad.
- Establecer unos mecanismos de protección para las redes de acceso que rompen con el perímetro tradicional de la red, tales como redes inalámbricas y dispositivos móviles y portátiles con conexión a las redes internas, delimitando su alcance y protegiendo el acceso mediante cifrado seguro.
- Implementar unos mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention"), instalando el "software" al efecto en virtud de unos requisitos de seguridad, para detectar potenciales brechas en el acceso y/o transmisión de datos y prevenirlos a través de monitoreo, detección y bloqueo de información sensible.
- Modificar el diseño de la red introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, bien duplicando la red física, equipos y "software", bien mediante la virtualización de sistemas.
- Configurar, en su caso, unos equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal, asegurando una transmisión de datos confiable y segura entre los distintos nodos que la conforman.
- Revisar unos procedimientos de salvaguarda de configuraciones, modificando en su caso la programación de copias de seguridad de las mismas mediante la funcionalidad habilitada en el sistema, almacenándolas en condiciones de seguridad y de modo que se permita una eficaz recuperación.
- Elaborar la documentación de configuración de seguridad, ajustándola a estándares e incluyendo todos los valores de configuración implantados.

**C5:** Aplicar procedimientos periódicos de revisión del "software" de comunicaciones en red y el control de acceso, actualizándolo, añadiendo o suprimiendo elementos o modificando las configuraciones para garantizar la seguridad de las comunicaciones y la protección de los datos en las mismas según las directrices de la organización.

**CE5.1** Describir el "software" de comunicaciones que se ejecuta en unos dispositivos de red, valorando su compatibilidad, teniendo en cuenta su funcionalidad y explicando cómo comprobar su integridad, legitimidad y verificar que estén actualizados para corregir problemas de seguridad.

**CE5.2** Enumerar productos "software" de comunicaciones relacionados con la seguridad, tales como cortafuegos ("firewalls"), o "proxies", explicando su utilidad, cómo configurarlos y localizando sus prestaciones y características en la documentación técnica asociada.

**CE5.3** Explicar procedimientos de salvaguarda del "software", para su revisión, indicando características y parámetros configurables para la programación de copias de seguridad de las mismas, y los pasos a seguir para almacenarlas en condiciones de seguridad y de modo que se permita una eficaz recuperación.

**CE5.4** Clasificar medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros, valorando la aportación a la seguridad en el control de acceso, sus ventajas e inconvenientes y explicando cómo ajustarlos de forma que garanticen la seguridad y la trazabilidad de los parámetros y las

definiciones de configuración, tal como establecer protocolos para el cambio cíclico de contraseñas fijas que no caducan o mecanismos de control de acceso del equipo de red de forma que sólo puedan ser modificados desde puntos permitidos y por administradores autorizados, entre otros.

**CE5.5** Describir mecanismos de configuración de seguridad en el ámbito de red, tales como la seguridad de puerto y los mecanismos de control de tormentas de difusión, tales como el protocolo de árbol de expansión ("spanning-tree"), los protocolos de redundancia ("Parallel Redundancy Protocol" -PRP-) y "Highly-available Seamless Redundancy" (HSR), explicando su utilidad y los pasos a seguir para su implementación.

**CE5.6** En un supuesto práctico de aplicación de procedimientos de revisión del "software" de comunicaciones en red y el control de acceso, actualizándolo, añadiendo o suprimiendo elementos o modificando las configuraciones para garantizar la seguridad de las comunicaciones y la protección de los datos en las mismas según las directrices de la organización:

- Evaluar un "software" de comunicaciones que se ejecuta en unos dispositivos de red, valorando su compatibilidad, teniendo en cuenta su funcionalidad y su idoneidad para el diseño a corto y medio plazo y comprobando su integridad, legitimidad y grado de actualización para corregir problemas de seguridad.
- Incluir en el diseño de una red productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies", comparando prestaciones y características e interpretando la documentación técnica asociada.
- Revisar unos procedimientos de salvaguarda del "software", modificando en su caso la programación de los "backup", almacenándolos en condiciones de seguridad y de modo que se permita una eficaz recuperación.
- Revisar unos medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros, ajustándolos de forma que garanticen la seguridad y trazabilidad de los parámetros y definiciones de configuración, estableciendo protocolos para el cambio cíclico de contraseñas fijas que no caducan, estableciendo mecanismos de control de acceso del equipo de red de forma que sólo puedan ser modificados desde unos puntos permitidos y por unos administradores autorizados.
- Aplicar una configuración de seguridad en el ámbito de red, garantizando el funcionamiento de punto críticos tales como la seguridad de puerto y los mecanismos de control de tormentas de difusión, tales como el protocolo de árbol de expansión ("spanning-tree"), protocolos de redundancia ("Parallel Redundancy Protocol" -PRP-) y "Highly-available Seamless Redundancy" (HSR), entre otros.
- Elaborar la documentación del "software" de seguridad se elabora, incluyendo productos, referencias y todos los valores de configuración implantados y ajustándolo a estándares.

## Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.9; C2 respecto a CE2.7; C3 respecto a CE3.6; C4 respecto a CE4.9 y C5 respecto a CE5.6.

### Otras Capacidades:

Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.

Adaptarse a la organización, a sus cambios organizativos y tecnológicos, así como a situaciones o contextos nuevos.

Mantener una actitud asertiva, empática y conciliadora con las personas demostrando cordialidad y amabilidad en el trato.
Mostrar iniciativa en la búsqueda de soluciones y en la resolución de problemas.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

## Contenidos

### 1 Normativa y estándares relacionados con el acceso y la transmisión de datos

Normativa aplicable de protección de datos. Estándares de seguridad relacionados con tecnologías específicas de acceso y transmisión de datos.

### 2 Implantación de protocolos y herramientas en operaciones de intercambio de datos

Seguridad de la información y criptografía. Cifrado de clave simétrica. Cifrado de clave pública y firma. Técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones. Herramientas de cifrado extremo a extremo. Redes privadas virtuales. IP Security Protocol. Túneles cifrados. Configuración. Protección de conexiones inalámbricas. Vulnerabilidades y protección. Protocolos. "Principio de proporcionalidad". Implantación y configuración de certificados digitales de servidores. Técnicas de seguridad para la autenticación de doble o triple factor. Certificados de usuario, DNI electrónico, "token", biométricos u otros mecanismos. Autenticación basada en contraseñas. Políticas de complejidad, renovación, bloqueo, almacenamiento y/o recuperaciones.

### 3 Implantación del uso de sistemas de firma y certificados de persona

Procedimientos de acceso a servicios a través de una red telemática. Autenticación mutua de cliente y servidor. Autenticación del cliente basada en certificados digitales de identidad personal. Proceso de obtención y verificación de certificados digitales de identidad personal. Entidades certificadoras. Transmisión cifrada del correo electrónico y comunicaciones interpersonales o entre procesos y/o componentes. Firma y cifrado extremo a extremo. Firma digital de documentos. Herramientas. Sistemas de sellado digital de tiempo. Garantía de integridad en componentes web y "software" mediante firma digital.

### 4 Implementación de infraestructuras de clave pública

Infraestructura de clave pública (PKI). Política de certificado y declaración de prácticas de certificación. Procedimientos, derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios. Jerarquías de autoridades de certificación. Emisión de certificados digitales. Usos. Comprobación de validez de los certificados. Servicio de revocación de certificados. Infraestructuras de gestión de privilegios (PMI).

### 5 Seguridad de la red de área local Topología y "Hardware"

Modelos de referencia estándar en lo concerniente a la seguridad. Dispositivos de comunicaciones y configuración segura. Topologías seguras. Subredes perimetrales de aislamiento o desmilitarizadas (DMZ). Técnicas de segmentación de una red. Técnicas físicas y lógicas (VLAN). Filtrado perimetral entre segmentos de red y entre máquinas específicas. Reglas de filtrado. Redes inalámbricas y dispositivos móviles y portátiles. Protección contra rotura del perímetro de la red. Prevención de fuga de datos (DLP: "Data Loss Prevention"). "Hardware" y "software" de detección y prevención de brechas. Monitoreo, detección y bloqueo de información sensible. Redundancia en red troncal. Alta disponibilidad. Procedimientos de salvaguarda de configuraciones. Periodicidad del proceso. Almacenamiento seguro. Restauración de copias.

### 6 "Software" de comunicaciones en red y el control de acceso

Taxonomía de "software" de comunicaciones. Comprobaciones de integridad, legitimidad y actualización. Cortafuegos ("firewalls") y "proxies". Procedimientos de salvaguarda del "software". Periodicidad. Almacenamiento seguro. Restauración de copias. Identificación de accesos a la red y a la administración de los equipos. Autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros. Configuración de políticas para contraseñas. Seguridad de puerto y los mecanismos de control de tormentas de difusión. Protocolo de árbol de expansión ("spanning-tree"). Protocolos de redundancia ("Parallel Redundancy Protocol" -PRP-) y "Highly-available Seamless Redundancy" (HSR).

## Parámetros de contexto de la formación

### Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Instalación de 2 m² por alumno o alumna.

### Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la implementación de sistemas seguros de acceso y transmisión de datos, que se acreditará simultáneamente mediante las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 3 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.