CUALIFICACIÓN PROFESIONAL:
Operaciones de seguridad en sistemas informáticos

Familia Profesional:	***Informática y Comunicaciones***
Nivel:	***2***
Código:	***IFC300_2***
Estado:	***BOE***
Publicación:	***RD 917/2024***
Referencia Normativa:	***RD 545/2023, RD 1201/2007, Orden PRE/1636/2015***

Competencia general

Aplicar procedimientos de administración y configuración del "software" y "hardware" en sistemas informáticos, garantizando la seguridad de equipos, correo y comunicaciones, solucionando incidencias mediante acciones inmediatas para su tratamiento o escalando los problemas en su caso, cumpliendo la normativa aplicable medioambiental, sobre protección de datos, propiedad intelectual e industrial, seguridad informática y servicios de las comunicaciones.

Unidades de competencia

UC0957_2: Mantener el subsistema físico en sistemas informáticos
UC0958_2: Mantener el "software" de base y las aplicaciones en sistemas informáticos
UC0959_2: Configurar la ciberseguridad en equipos finales
UC2797_2: Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico
UC2798_2: Responder ante eventos de ciberseguridad

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 de soporte informático
- Operadores de centros de operaciones de seguridad integrada

- Operadores de equipos de respuesta ante emergencias informáticas
- Técnicos en operaciones de ciberseguridad
- Técnicos en operaciones de seguridad informática

Formación Asociada (570 horas)

Módulos Formativos

MF0957_2: Mantenimiento del subsistema físico en sistemas informáticos (90 horas)

MF0958_2: Mantenimiento del "software" de base y aplicaciones en sistemas informáticos (90 horas)

MF0959_2: Configuración de la ciberseguridad en equipos finales (120 horas)

MF2797_2: Configuración de la seguridad en redes de comunicaciones y sistemas de correo electrónico (180 horas)

MF2798_2: Respuesta ante eventos de ciberseguridad (90 horas)

UNIDAD DE COMPETENCIA 1

Mantener el subsistema físico en sistemas informáticos

Nivel: *2*
Código: *UC0957_2*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Mantener la conectividad a la red de datos de los sistemas informáticos, comprobando su estado, siguiendo especificaciones y criterios de calidad y seguridad de la entidad responsable de sistemas para permitir su interconexión.

CR1.1 La conexión del sistema informático a la red se verifica, comprobando el ajuste del cableado, el estado de los LED del interfaz y la configuración de la conexión, probando las comunicaciones y constatando que son efectivas mediante aplicaciones al efecto.

CR1.2 Los dispositivos físicos averiados, con mal funcionamiento o bajo rendimiento se sustituyen, reemplazándolos por componentes equivalentes que cumplan su misma función y aseguren su compatibilidad en el sistema, para mantenerlo operativo.

CR1.3 Los controladores de red se mantienen actualizados, comprobando la existencia de nuevas versiones del fabricante, instalándolas en su caso.

CR1.4 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP2: Solucionar incidencias relacionadas con el subsistema físico en equipos microinformáticos, detectando, diagnosticando y reparando, actualizando o sustituyendo los componentes "hardware" y dispositivos asociados averiados, siguiendo las especificaciones de la documentación técnica, los procedimientos establecidos por la entidad responsable del mantenimiento y de acuerdo con la planificación de la acción preventiva.

CR2.1 La causa del comportamiento anómalo se establece, consultando la documentación técnica del fabricante y el histórico de incidencias y averías y mediante la realización de pruebas funcionales para determinar las características de naturaleza física o lógica de la misma, valorando la posibilidad de reparación o sustitución en función de los costes económicos, la factibilidad de la misma y/o los cambios que se requiere ejecutar.

CR2.2 Las copias de seguridad ("backup") de los equipos microinformáticos, se llevan a cabo antes de la reparación o sustitución de los componentes, usando herramientas "software" para esta función y almacenando la copia en condiciones de seguridad, para asegurar la recuperación del sistema en caso necesario.

CR2.3 Los componentes "hardware" averiados se reparan, sustituyéndolos, actualizándolos o reajustándolos, utilizando herramientas e instrumentación de medida, asegurando las conexiones y la sujeción mecánica, conforme las recomendaciones del fabricante, y criterios de calidad en la realización de los trabajos.

CR2.4 Las incidencias que no se consiguen diagnosticar se reportan al nivel de responsabilidad superior, usando los canales de comunicación establecidos en la entidad responsable del mantenimiento.

CR2.5 La detección, diagnóstico y solución de la incidencia se documenta, utilizando el modelo o aplicación informática establecidos por la entidad responsable del mantenimiento, registrando las tareas efectuadas y garantizando la trazabilidad de los procesos en el histórico de incidencias y averías.

CR2.6 Los embalajes, residuos, componentes desechables y consumibles se tratan, almacenándolos en los lugares destinados a ello, según tipología y según criterios de reducción en origen, reutilización, reciclado, valorización y eliminación y garantizando el cumplimiento de la normativa medioambiental aplicable.

RP3: Verificar el funcionamiento del "hardware" en equipos microinformáticos y dispositivos asociados, mediante pruebas y mediciones, siguiendo las especificaciones de la documentación técnica y los procedimientos establecidos por la entidad responsable del mantenimiento.

CR3.1 Las pruebas y mediciones a realizar se preparan, definiendo su alcance, pasos a seguir y periodicidad de aplicación, para ser aplicadas con posterioridad.

CR3.2 El sistema o dispositivo se comprueba, mediante pruebas y mediciones, usando herramientas "software", verificando los registros ("log") del sistema, entre otros, para asegurar el funcionamiento de los equipos y componentes reparados o sustituidos.

CR3.3 Las pruebas de verificación, incidencias surgidas y soluciones adoptadas se documentan, utilizando el modelo o aplicación informática establecidos por la entidad responsable del mantenimiento, registrando las tareas efectuadas y garantizando la trazabilidad de los procesos en el histórico de incidencias y averías.

Contexto profesional

Medios de producción

Equipos informáticos. Elementos de protección (calzado aislante, guantes, descargador de electricidad estática -pulsera-, entre otros). Herramientas, y equipos de instrumentación eléctrico/electrónico. Dispositivos asociados por cable, "bluetooth" o en red, tales como impresoras, escáner, entre otros. Sistemas operativos y controladores. Herramientas "software" de diagnóstico. "Software" de mantenimiento informático. Herramientas de "backup" y de clonación.

Productos y resultados

Conectividad de los sistemas microinformáticos comprobada y verificada Incidencias relacionadas con el subsistema físico solucionadas Funcionamiento del "hardware" en equipos microinformáticos y dispositivos asociados verificado.

Información utilizada o generada

Normativa aplicable de planificación de la acción preventiva. Normativa aplicable de protección de datos, propiedad intelectual y medioambiental. Normativa electrotécnica aplicable. Estándares internacionales de electricidad y electrónica. Partes de trabajo. Especificaciones para el montaje de dispositivos informáticos. Documentación técnica de los dispositivos informáticos. Documentación técnica de instalación y mantenimiento de los dispositivos informáticos. Manuales del "software" de diagnóstico y copia de seguridad. Catálogos de productos, proveedores, precios.

UNIDAD DE COMPETENCIA 2

Mantener el "software" de base y las aplicaciones en sistemas informáticos

Nivel: *2*
Código: *UC0958_2*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Actualizar paquetes informáticos de propósito general, utilidades y aplicaciones específicas para su explotación posterior por parte de los usuarios y según las directrices recibidas de la entidad responsable.

CR1.1 El "software" se actualiza, validándolo previamente en entornos similares al entorno productivo si fuera necesario, para asegurar su funcionalidad y operatividad, confirmando que no se producen disfunciones y/o pérdidas de información y/o datos, asegurando la integridad del equipo y la disponibilidad de la información, confirmando que no se produce pérdida de los datos previamente almacenados.

CR1.2 Las incidencias que aparezcan durante el proceso de actualización se resuelven, diagnosticando el problema y consultando la documentación técnica del producto, volviendo a la versión anterior si fuera necesario, recurriendo a la persona responsable de sistemas y/o solicitado del fabricante asistencia en caso de persistir el problema.

CR1.3 El rendimiento del equipo se comprueba, evaluando y comparando indicadores tales como uso de CPU, ocupación de memoria, acceso a disco u otros, antes y después de la actualización.

CR1.4 La configuración "hardware" del equipo se revisa de acuerdo a los requisitos de la nueva versión para valorar posibles mejoras tales como aumento de memoria, CPU, cambio de disco o sustitución completa del equipo si fuera necesario.

CR1.5 La actualización de los paquetes informáticos se documenta, incluyendo detalles tales como el nombre de la aplicación actualizada, versión, las incidencias generadas e incompatibilidades detectadas, referenciando soportes y registros, utilizando el modelo y/o aplicación informática establecidos por la entidad responsable de la instalación, garantizando la trazabilidad de los procesos.

RP2: Resolver las incidencias que se presenten en la explotación de las aplicaciones, identificando su naturaleza, en los márgenes de tiempo y el nivel de calidad requerido en las normas internas de la entidad responsable, para dar soporte a los usuarios de las mismas.

CR2.1 La asistencia al usuario se lleva a cabo, teniendo en cuenta las técnicas de comunicación interpersonal establecidas por la entidad responsable del soporte, identificando la actuación requerida, satisfaciendo las exigencias y demandas del usuario y garantizando el resultado de la actuación, utilizando en su caso herramientas de acceso remoto al equipo defectuoso para agilizar su resolución.

CR2.2 El motivo que causó la incidencia se diagnostica:

- Revisando la documentación que contiene el histórico de actuaciones realizadas, a fin de determinar si alguna de ellas pudiera afectar al funcionamiento de la aplicación.

- Inspeccionando el equipo y comprobando que no hay instalado "software" que no cumpla los requisitos establecidos por el sistema de gestión de calidad de la organización.
- Validando el estado del sistema: comprobando que hay espacio en disco libre, la memoria/CPU no está saturada y el equipo mantiene unos tiempos de respuesta aceptables.

CR2.3 Los componentes "software" afectados se reinstalan con los parámetros indicados en las especificaciones establecidas en la documentación técnica y las necesidades de uso, implementando nuevas acciones correctoras en el caso de tratarse de incidencias repetitivas.

CR2.4 Las medidas de seguridad preventivas tales como revisión de certificados, ir realizando copias de seguridad periódicas de la información en un servidor de "backup", la comprobación que el proceso de restauración desde esos servidores es funcional, el mantenimiento de sistemas de disponibilidad u otros se activan para mantener la integridad de la información y la continuidad en la explotación durante la resolución del problema, siguiendo los procedimientos establecidos por la entidad responsable del mantenimiento.

CR2.5 La información original perdida o alterada se restaura, en su caso actualizándola, aplicando las medidas correctivas de que disponga la entidad responsable, siguiendo el protocolo y pasos establecidos por la entidad responsable de sistemas para la recuperación de información, de forma que el sistema vuelva a estar en explotación.

CR2.6 El funcionamiento del sistema una vez restaurado y la integridad de los datos, se verifican mediante pruebas al efecto, siguiendo las especificaciones recibidas de la persona o entidad responsable de sistemas para comprobar su funcionalidad.

CR2.7 Las actuaciones realizadas se documentan en los formatos establecidos a tal efecto por la entidad responsable, para facilitar su seguimiento, actualizando el repositorio de incidencias, la documentación técnica de la instalación y la configuración del sistema.

RP3: Mantener el sistema operativo, el "software" de base y aplicaciones estándar del sistema microinformático, mediante revisión, verificación y monitorización teniendo en cuenta las necesidades de uso, para detectar problemas y solucionarlos en su caso, siguiendo especificaciones y criterios de calidad y seguridad de la entidad responsable de sistemas.

CR3.1 El sistema de archivos se verifica, reconfigurando particiones en caso necesario y limpiando errores físicos, lógicos u otros, usando las utilidades, herramientas e interfaces que proporciona el sistema operativo, siguiendo especificaciones técnicas y según necesidades de operación.

CR3.2 El rendimiento y el uso de recursos "hardware" dentro del equipo, tales como uso de CPU, uso de RAM, memoria de intercambio y datos SMART, entre otros, se monitorizan según necesidades de operación, generando alarmas y notificaciones mediante la utilización de herramientas para dicha función y siguiendo los criterios y parámetros de la entidad responsable.

CR3.3 Las políticas de seguridad de usuarios y grupos se revisan, cotejándolas con las políticas actuales de la entidad responsable, para garantizar su vigencia y, en su caso, para realizar las modificaciones correspondientes, aplicando los parámetros especificados por dicha entidad responsable.

CR3.4 Las medidas de seguridad preventivas tales como actualizaciones, copias de seguridad periódicas de la información en un servidor de "backup", la comprobación que el proceso de restauración desde esos servidores es funcional, el mantenimiento de sistemas de disponibilidad u otros se activan para mantener la integridad de la información y la continuidad en la explotación.

CR3.5 El uso y gestión, por parte de los usuarios, de los dispositivos conectados directamente o por red al sistema microinformático, se comprueba, verificando que se realiza según la documentación técnica y procedimientos estipulados para explotar sus funcionalidades y en condiciones de seguridad.

CR3.6 Los problemas se detectan, interpretando los mensajes resultantes de la ejecución del "software" de base tales como los registros "log" del sistema u otros, mediante la consulta de los manuales, la documentación proporcionada por el fabricante y las especificaciones dadas por la organización.

CR3.7 Los problemas detectados se corrigen, aplicando soluciones según las necesidades en cada caso, teniendo en cuenta las señales de problema detectadas y su diagnóstico, siguiendo procedimientos del fabricante y de la entidad responsable de sistemas.

CR3.8 El trabajo realizado se documenta, indicando las incidencias surgidas y las soluciones aplicadas, utilizando un modelo de documento o una aplicación informática indicados por la entidad responsable de sistemas, para su archivo y posterior consulta.

Contexto profesional

Medios de producción

Equipos informáticos y periféricos. "Software" de seguridad y antivirus, de aplicaciones específicas. Herramientas de detección, diagnóstico y reparación de errores (en local o en remoto). Herramientas "software" de instalación y actualización. Actualizaciones y parches. Dispositivos móviles. "Software" de gestión colaborativo. Elementos de instalación (programas de ayuda, manuales, licencias). "Software" de copias de seguridad y recuperación. Soportes para copias de seguridad. Acceso a Internet.

Productos y resultados

Paquetes informáticos de propósito general, utilidades y aplicaciones específicas instaladas y actualizadas. Incidencias en la explotación de aplicaciones resueltas. Sistema operativo, "software" de base y aplicaciones estándar del sistema microinformático mantenidos.

Información utilizada o generada

Normativa relativa a la planificación de la actividad preventiva. Normativa aplicable en materia de seguridad e higiene, protección de datos y propiedad intelectual e industrial. Normas internas de la empresa sobre atención a la clientela y confidencialidad de la información. Partes de incidencias e histórico de incidencias. Documentación de la instalación. Petición de asistencia de usuarios. Registro histórico de actualizaciones de sistema operativo y aplicaciones. Plan de seguridad y calidad de la organización. Manuales y documentación técnica de sistemas operativos. Manuales de instalación del "software" de aplicación o de la aplicación específica. Guía de explotación de la aplicación. Manuales de actualización de sistemas operativos. Manuales de las aplicaciones incluidas en el sistema operativo. Manuales de las aplicaciones externas al sistema operativo.

UNIDAD DE COMPETENCIA 3

Configurar la ciberseguridad en equipos finales

Nivel: *2*
Código: *UC0959_2*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Instalar sistemas de protección frente a "malware" en equipos finales ("end point"), configurando los parámetros de protección, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

CR1.1 La configuración del sistema operativo se verifica para el funcionamiento de la protección frente a "malware", validando los parámetros especificados según indique la documentación técnica.

CR1.2 Los programas de utilidad incluidos en el sistema operativo se configuran para el uso de la protección frente a "malware", previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.

CR1.3 La seguridad relativa al "software" no deseado se define en el sistema de protección frente a "malware", asignando parámetros tales como extensiones de programas y ficheros no permitidas, carpetas de especial protección, listas blancas de ficheros, actuación frente a ficheros no firmados digitalmente o con firma desconocida o caducada, junto con el veredicto de bloquear, enviar a cuarentena, permitir o aplicación de cualquier otro filtro para proteger al sistema frente a "malware" y "software" no deseado.

CR1.4 Los eventos de notificación y alarmas se configuran en el sistema de protección frente a "malware", estableciendo parámetros tales como correos de notificación frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog" u otros.

CR1.5 Los paquetes de instalación del "software" cliente para equipos y servidores se configuran en el sistema, definiendo parámetros tales como versión de sistema operativo, carpetas de exclusión y/o exclusión de aplicación o programas particulares, entre otros.

CR1.6 Las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas se configuran en el sistema de protección frente a "malware", estableciendo las condiciones de actualización de todos los equipos.

CR1.7 Las opciones anti "tampering" para la protección contra la desactivación y desinstalación del "software" cliente de protección frente a "malware" se configuran, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.

CR1.8 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad, para comprobar la funcionalidad del sistema de seguridad.

CR1.9 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP2: Instalar sistemas avanzados de detección y respuesta (EDR: "Endpoint Detection and Response"), configurando los parámetros de protección, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

CR2.1 Los paquetes de instalación del "software" cliente de protección frente a amenazas avanzadas para equipos y servidores se configuran en el sistema, definiendo parámetros tales como versión de sistema operativo, datos específicos de suscripción a la plataforma de nube, y datos de conexión.

CR2.2 Las alertas avanzadas de detección de intrusión se definen en el sistema, estableciendo parámetros tales como tácticas, técnicas y procedimientos empleados por atacantes, programas y utilidades frecuentemente utilizadas, direcciones IP de comunicación, empleo de credenciales de administradores, entre otras, asignando la severidad de las alertas para la detección y notificando los eventos detectados por la plataforma.

CR2.3 Los eventos de notificación y alarmas se configuran en el sistema de protección frente a amenazas avanzadas, estableciendo parámetros tales como correos frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog", entre otros.

CR2.4 Las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas se configuran en el sistema, estableciéndolas en todos los equipos.

CR2.5 Las opciones anti "tampering" para la protección de desactivación y desinstalación del "software" cliente de protección se configuran, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.

CR2.6 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.

CR2.7 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP3: Instalar sistemas de cifrado de información en disco, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

CR3.1 La configuración del sistema operativo se verifica para el funcionamiento del cifrado, validando los parámetros especificados según indique la documentación técnica.

CR3.2 Los programas de utilidad incluidos en el sistema operativo, se configuran para el uso del cifrado, previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.

CR3.3 El almacenamiento seguro de información se define, configurándolo mediante la asignación de parámetros tales como tamaño, permisos de accesos, claves de protección para el almacenamiento de claves y certificados de descifrado de los clientes.

CR3.4 La relación de políticas de cifrado de información se aplican en el sistema, estableciendo parámetros tales como unidades de disco a cifrar, algoritmos de cifrado (AES, DES, entre otros), longitud de clave, secuencia de encendido de equipos, elemento de paso del cifrado (clave,

certificado, pin, entre otros) o número máximo de intentos de descifrado, según cada tipo de equipo y servidor.

CR3.5 Las opciones anti "tampering" de protección de desactivación y desinstalación del "software" cliente de cifrado se configuran en el sistema, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o desactivación del producto del cliente.

CR3.6 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.

CR3.7 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

Contexto profesional

Medios de producción

Equipos informáticos tales como ordenadores de sobremesa, portátiles y servidores. Conexión a red. Navegadores. Buscadores. Aplicaciones ofimáticas. Analizadores de vulnerabilidades. Programas de análisis de contraseñas. Antivirus/"antimalware". EPP ("Endpoint Protection Platform"). EDR ("Endpoint Detection and Response"). "Software" de flujo de trabajo para envío de alarmas e incidencias a responsables. Servicios y aplicaciones de cifrado de información.

Productos y resultados

Sistemas de protección frente a "malware" en equipos finales ("end point") instalados y configurados. Sistemas avanzados de detección y respuesta (EDR: "Endpoint Detection and Response") instalados y configurados. Sistemas de cifrado de información en disco instalados y configurados.

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, procedimientos y políticas de seguridad, histórico de ataques e incidencias, informes de análisis de vulnerabilidades, relación de contraseñas débiles, 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

Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico

Nivel: *2*
Código: *UC2797_2*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Instalar sistemas de cortafuegos, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

CR1.1 Las zonas de seguridad se asocian a los interfaces de red del cortafuegos, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad y el resto de zonas.

CR1.2 Las políticas de seguridad relativas a flujos de conexiones permitidas entre redes y subredes se aplican sobre las zonas de seguridad, configurando acciones tales como:

- Permitir los flujos de conexiones iniciados desde redes de mayor seguridad hacia redes de menor seguridad.
- Establecer los flujos de conexiones hacia redes con vulnerabilidades intencionadas "honeynets".
- Bloquear los flujos de conexiones iniciados desde redes de menor seguridad a redes de mayor seguridad que no estén explícitamente permitidas.
- Aplicar el filtrado en el cortafuegos entre las zonas de seguridad, estableciendo las direcciones IP y puertos permitidos y no permitidos.

CR1.3 La relación de políticas de filtrado de tráfico se aplican sobre los cortafuegos, estableciendo las reglas y firmas de protección específicas frente a ataques conocidos entre las zonas, tales como "Port enumeration", "TCP Split handshake", "TCP SYN flood", entre otros, para protegerlas frente a ellos.

CR1.4 Los eventos de notificación y alarmas se configuran en el cortafuegos, estableciendo parámetros tales como correos de notificación frente a alertas críticas y altas y/o envío de paquetes de notificación mediante "syslog", entre otros.

CR1.5 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.

CR1.6 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP2: Instalar sistemas de detección y prevención de intrusiones (IDS/IPS), configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

CR2.1 Los cables de red de entrada y salida de datos se conectan a cada uno de los interfaces del IDS/IPS de acuerdo con especificaciones técnicas y organizativas, para posibilitar la inspección del tráfico de red.

CR2.2 Las zonas de seguridad se asocian a los interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas.

CR2.3 Los sistemas señuelo ("honeypot") se configuran, estableciendo aplicaciones y servicios trampa atractivos ante ataques, recopilando información sobre métodos y comportamientos, para la protección de la red de producción real.

CR2.4 Las firmas de detección de ataques se configuran, habilitándolas en el sistema IDS/IPS de acuerdo con las especificaciones técnicas y organizativas, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones, para la protección de las redes de comunicaciones.

CR2.5 Las firmas de detección de ataques del sistema IDS/IPS se actualizan periódicamente, instalando la versión más reciente.

CR2.6 Las reglas de detección de ataques por comportamiento se configuran, habilitándolas en el sistema IDS/IPS de acuerdo con las especificaciones técnicas y organizativas, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones, para la protección de las redes de comunicaciones.

CR2.7 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.

CR2.8 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP3: Instalar sistemas de filtrado de navegación, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

CR3.1 Las políticas de acceso a la navegación se configuran, estableciendo las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas, para la protección de las redes.

CR3.2 Las políticas de acceso de categorías de contenidos web se configuran, estableciendo aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web.

CR3.3 Los perfiles de acceso de navegación se configuran para cada usuario y nodo de comunicación, definiendo para cada uno de ellos las políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar.

CR3.4 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.

CR3.5 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP4: Instalar sistemas de gestión de eventos de seguridad ("Security Information and Event Management", SIEM), configurando los parámetros relacionados,

siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

CR4.1 La configuración del sistema operativo se verifica para el funcionamiento de los SIEM, validando los parámetros especificados según indique la documentación técnica.

CR4.2 Los programas de utilidad incluidos en el sistema operativo, se configuran para el uso de los SIEM, previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.

CR4.3 Los sistemas de recolección de información se configuran en el SIEM, especificando el tipo de fuente de información, tal como sistema de protección contra el "malware", cortafuegos, sistemas de detección de intrusión, "honeypot", entre otros, para su registro en la herramienta.

CR4.4 Las reglas de "parseado" y normalización de eventos para cada tipo de fuente se configuran, de acuerdo con las especificaciones técnicas específicas del fabricante para cada fuente, configurando campos tales como tipo de evento, dirección IP, usuario, entre otros.

CR4.5 Las reglas de agregado y correlación para cada caso de uso se configuran, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros, para el sistema de detección de alertas del SIEM.

CR4.6 Las reglas de generación de alertas para cada caso de uso se configuran, asignando parámetros tales como severidad, tipo de alerta, sistemas afectados, fecha y hora, entre otros, para la posterior notificación y tratamiento de la alerta.

CR4.7 Los eventos de notificación de alertas se configuran en el SIEM, estableciendo parámetros para cada tipo de alerta y severidad, tales como correos de notificación frente a apertura de tiques en sistemas de gestión de la demanda u otros medios o sistemas válidos, para la notificación automatizada de eventos.

CR4.8 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.

CR4.9 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP5: Configurar "software" de base y aplicaciones de sistemas informáticos para la protección del correo electrónico, verificando su funcionalidad y comprobando la seguridad siguiendo especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del sistema.

CR5.1 La configuración del sistema operativo se verifica para el funcionamiento de la protección del correo electrónico, comprobando los parámetros específicos que se indique en la documentación técnica del producto.

CR5.2 Los programas de utilidad disponibles en el sistema operativo se instalan, verificando que son los mínimos que se necesitan para las funciones requeridas, configurándolos para su uso con los parámetros que se indiquen en la documentación o instrucciones de configuración.

CR5.3 Los usuarios imprescindibles para el funcionamiento del sistema se crean, configurando el mínimo conjunto de privilegios para cada uno, de acuerdo a las especificaciones técnicas.

CR5.4 Los sistemas de encriptado de comunicaciones y correo electrónico se instalan o, en su caso, se activan, configurando claves o certificados para garantizar la privacidad de las transmisiones.

CR5.5 La instalación se verifica, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.

CR5.6 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP6: Instalar sistemas perimetrales de filtrado de correo electrónico, configurando los parámetros y acciones relacionados con su seguridad, según especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del correo electrónico.

CR6.1 Los sistemas de consulta de reputación de dominios y las acciones de filtrado de correo se configuran, estableciendo las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo electrónico recibido.

CR6.2 La información detallada que se requiere para la confección de los registros DNS tal como:

- Relación de dominios desde los que se enviara el correo electrónico.
- Direcciones IP públicas de los sistemas de correo electrónico con flujo saliente.
- Configuración de la política SPF ("Sender Policy Framework").
- Relación de dominios de correo electrónico, y clave pública DKIM ("Domainkey Identified Mail") asociada.
- Publicación de política del dominio en entradas DNS de DMARC ("Domain-based Message Authentication, Reporting and Conformance").

Se proporciona al área responsable de la organización, para su implementación en los sistemas DNS, usando los canales de comunicación que se establezca en la entidad responsable.

CR6.3 Los umbrales de valoración de correos electrónicos para la determinación de correo sospechoso y no deseado se comprueban, verificando que son aplicados sobre los sistemas de protección de correo electrónico, de acuerdo con las especificaciones técnicas recibidas.

CR6.4 La relación de dominios, "emails" y ficheros adjuntos que deben de tener un tratamiento especial en relación a la seguridad se definen, configurando los sistemas de protección de correo electrónico y asignando acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.

CR6.5 Los filtros de análisis semántico para la detección de contenido no deseado se definen sobre los sistemas de protección de correo electrónico asignando acciones para cada uno de éstos tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.

CR6.6 El sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos se define, configurando, entre otros, el servidor y el "email" de notificación, para asegurar la comunicación de alertas del sistema al equipo responsable de la gestión del incidente.

CR6.7 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP7: Instalar sistemas perimetrales de prevención de fuga de información en el correo electrónico, configurándolos según especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del correo electrónico.

CR7.1 La relación de políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico se aplican, proporcionando para cada tipo de fichero o conjunto de información, el veredicto de bloquear, poner en cuarentena o notificar una violación de la política al usuario.

CR7.2 Los usuarios encargados de los análisis de investigación de los casos se configuran, definiendo para cada uno de ellos el nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos.

CR7.3 Los medios y sistemas de notificación de violación de las políticas de fuga de información se configuran en el sistema, verificando su funcionamiento, de acuerdo con las especificaciones técnicas recibidas.

CR7.4 La instalación se verifica, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.

CR7.5 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

Contexto profesional

Medios de producción

Equipos informáticos tales como ordenadores de sobremesa, portátiles y servidores. Conexión a red. Navegadores. Servidores y clientes de redes privadas virtuales (VPN). Programas de conexión segura a servicios telemáticos. Analizadores de vulnerabilidades. Programas de análisis de contraseñas. Antivirus/"antimalware". EPP ("Endpoint Protection Platform"). Cortafuegos. Sistemas de detección de intrusiones (IDS). Sistemas de prevención de intrusiones (IPS). Sistemas de filtrado de navegación. "Software" para garantizar la confidencialidad e integridad de las comunicaciones. "Software" de flujo de trabajo para envío de alarmas e incidencias a responsables. Interfaces de correo electrónico con soporte para correo seguro. Soluciones de prevención de fuga de datos (DLP).

Productos y resultados

Sistemas de cortafuegos instalados y configurados. Sistemas de detección y prevención de intrusiones (IDS/IPS) instalados y configurados. Sistemas de filtrado de navegación instalados y configurados. "Software" de base y aplicaciones de sistemas informáticos configuradas. Sistemas perimetrales de filtrado de correo electrónico instalados y configurados. Sistemas perimetrales de prevención de fuga de información en el correo electrónico instalados y configurados.

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, procedimientos y políticas de seguridad, histórico de ataques e incidencias, informes de análisis de vulnerabilidades, informe de servicios y puntos de acceso al sistema informático, relación de contraseñas débiles, normas internas de prevención de amenazas de seguridad, 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 5

Responder ante eventos de ciberseguridad

Nivel: *2*
Código: *UC2798_2*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Implementar eventos y alertas de seguridad, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

CR1.1 Los eventos de sistemas recolectados en el sistema de monitorización se parametrizan configurándolos de modo que se asegure que la información que proporciona es completa y precisa para facilitar su posterior tratamiento.

CR1.2 Las reglas de tratamiento de los eventos normalizados se implementan, configurándolas en función de su severidad para la generación de alertas.

CR1.3 Las reglas de correlación entre eventos normalizados y alertas se implementan, configurándolas en función de su severidad para la generación de alertas.

CR1.4 Las reglas de agregación de eventos normalizados y alertas se implementan, configurando métricas y elementos para su agrupación.

CR1.5 Los mecanismos de remediación automática o semiautomática de las alertas son implementados, de acuerdo con las condiciones de remediación.

CR1.6 La documentación de las alertas y reglas de normalización, agregación y correlación realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP2: Ejecutar procedimientos frente alertas de seguridad, identificando parámetros, origen y condiciones y comunicando a las personas responsables de su gestión, para subsanar incidencias de seguridad, según normas y procedimientos de la entidad responsable.

CR2.1 El procedimiento operativo de seguridad a aplicar ante las alertas generadas por el sistema de monitorización se selecciona, interpretando cada alerta y consultando el maestro de alertas y procedimientos establecido por la organización.

CR2.2 Los procedimientos de seguridad se aplican, de acuerdo con las condiciones de entorno de la alerta específica, identificando parámetros relacionados tales como direcciones IP origen y destino, puerto accedido, tipo de evento, entre otros.

CR2.3 El escalado de alertas se ejecuta, comunicándolas a la persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos.

CR2.4 Las alertas gestionadas se cierran, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación.

CR2.5 La documentación relativa a las alertas gestionadas se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

RP3: Colaborar en la definición de procedimientos de respuesta a alertas de seguridad, recabando requisitos, condiciones de entorno y objetivos, definiéndolos y registrándolos, para preparar la respuesta ante incidencias, según normas y procedimientos de la entidad responsable.

CR3.1 Las alertas sin procedimiento asociado se marcan en la documentación para su uso posterior, utilizando el maestro de alertas y procedimientos operativos e identificando aquellas alertas no recogidas en él.

CR3.2 Los requisitos, condiciones de entorno y objetivos de remediación para cada alerta se recaban, previa identificación, documentándolos según modelos internos establecidos por la organización, para su control, uso y trazabilidad.

CR3.3 Los procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación decididos por la persona responsable, se redactan, indicando las acciones a realizar y prestando especial atención a los requisitos de continuidad de negocio definidas por la organización.

CR3.4 Los procedimientos de seguridad se prueban, verificando su aplicación y aprobándolos y registrándolos de acuerdo con el modelo definido por la organización.

CR3.5 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

Contexto profesional

Medios de producción

Equipos informáticos tales como ordenadores de sobremesa, portátiles y servidores. Conexión a red. Navegadores. Buscadores. Servidores y clientes de redes privadas virtuales (VPN). Programas de conexión segura a servicios telemáticos. Analizadores de vulnerabilidades. Antivirus/"antimalware". EPP ("Endpoint Protection Platform"). EDR ("Endpoint Detection" and "Response"). 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") y de recolección de información (tipo "Syslog"). "Software" para garantizar la confidencialidad e integridad de las comunicaciones. Consola de SNMP. "Software" de flujo de trabajo para envío de alarmas e incidencias a responsables.

Productos y resultados

Eventos y alertas de seguridad implementados procedimientos frente alertas de seguridad ejecutados. Colaboración en procedimientos de respuesta a alertas de seguridad realizada.

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, procedimientos y políticas de seguridad, histórico de ataques e incidencias, informes de análisis de vulnerabilidades, relación de contraseñas débiles, informe 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).

MÓDULO FORMATIVO 1

Mantenimiento del subsistema físico en sistemas informáticos

Nivel: *2*
Código: *MF0957_2*
Asociado a la UC: *UC0957_2 - Mantener el subsistema físico en sistemas informáticos*
Duración (horas): *90*
Estado: *Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de mantenimiento de la conectividad a la red de datos de un sistema informático, comprobando su estado, siguiendo especificaciones y criterios de calidad y seguridad de la entidad responsable de sistemas para permitir su interconexión.

CE1.1 Identificar las interfaces físicas de red, clasificándolas según su tipología, capacidad y conexionado físico.

CE1.2 Reconocer las conexiones, puertos, ranuras ("slot") o bahías físicas de conexión de las interfaces físicas de red, clasificándolas según su tipología, compatibilidad y capacidades.

CE1.3 Describir el proceso de configuración de las interfaces lógicas de red, explicando los pasos para configurar los elementos que la componen, tales como direccionado, máscara, servicios DNS, entre otros.

CE1.4 Enumerar aplicaciones de prueba y evaluación de la calidad de una conexión, explicando sus características y funcionalidades.

CE1.5 En un supuesto práctico de aplicación de procedimientos de mantenimiento de la conectividad a la red de datos de los sistemas informáticos, comprobando su estado siguiendo especificaciones y criterios de calidad y seguridad de la entidad responsable de sistemas para permitir su interconexión:

- Verificar la conexión de un sistema informático a la red, comprobando el ajuste del cableado, el estado de los LED del interfaz y la configuración de la conexión, probando las comunicaciones y constatando que son efectivas mediante aplicaciones al efecto.
- Sustituir dispositivos físicos averiados, con mal funcionamiento o bajo rendimiento, reemplazándolos por componentes equivalentes que cumplan su misma función y aseguren su compatibilidad en el sistema, para mantenerlo operativo.
- Actualizar los controladores de red, comprobando la existencia de nuevas versiones del fabricante, instalándolas en su caso.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C2: Aplicar técnicas de diagnóstico de una incidencia en equipos y componentes del sistema microinformático y de dispositivos asociados, usando herramientas, en su caso, para identificar su naturaleza.

CE2.1 Identificar componentes de electrónica analógica y digital, explicando sus aplicaciones más características, para asociar las métricas y equipamiento de medida necesario para estimar la funcionalidad de un dispositivo, de acuerdo a sus especificaciones técnicas.

CE2.2 Identificar los elementos eléctricos, electrónicos y electromecánicos contenidos dentro de los dispositivos de un equipo informático susceptibles de ajuste, calibración y/o reparación, para efectuar las acciones de reparación o sustitución, en función de las informaciones obtenidas por medio de procesos de diagnóstico y especificaciones recibidas.

CE2.3 Describir las características de las herramientas e instrumentos aplicables a las tareas de detección y solución de averías en condiciones de calidad, eficiencia y seguridad.

CE2.4 Describir las señales de alimentación, control y datos de los conectores, buses e interfaces de los componentes de un equipo informático, indicando el procedimiento para la evaluación y estimación de sus parámetros funcionales, de acuerdo a especificaciones técnicas del dispositivo a monitorizar.

CE2.5 Describir el procedimiento de ensamblaje y desensamblaje de componentes, equipos microinformáticos y dispositivos asociados, explicando los pasos a seguir para poder realizar las actuaciones en los mismos.

CE2.6 Explicar la tipología y características de las incidencias y averías en equipos microinformáticos y dispositivos asociados, describiendo las técnicas generales y los medios específicos para su localización con el fin de optimizar los procedimientos de reparación.

CE2.7 Describir las características de las herramientas "hardware" y "software" que se utilizan para el diagnóstico de incidencias y averías en el sistema microinformático, teniendo en cuenta sus especificaciones técnicas.

CE2.8 En un supuesto práctico de aplicación de técnicas de diagnóstico de una incidencia en equipos microinformáticos y dispositivos asociados, usando herramientas:

- Establecer una primera hipótesis en función de la información y documentación aportada y detectar los puntos críticos del equipo y/o componente mediante la consulta de los históricos de incidencias y averías.
- Identificar los síntomas y la naturaleza de la incidencia, caracterizándola por los efectos que produce y efectuar medidas en los puntos de testeo establecidos por los fabricantes o definidos por el procedimiento especificado.
- Localizar el bloque funcional o componente responsable de la incidencia, identificando los elementos de seguridad que deben ser tenidos en cuenta.
- Elaborar la documentación de las actividades realizadas y los resultados obtenidos utilizando los formatos y plantillas que se proporcionen.

C3: Aplicar procedimientos de ajuste, reparación y verificación de elementos averiados, usando herramientas manuales, equipos o "software" específico según el caso, para garantizar el funcionamiento del equipo o componente.

CE3.1 Describir herramientas y equipos para la reparación de averías de un equipo microinformático, clasificándolas en función de los tipos de dispositivo a reparar, de acuerdo a las especificaciones técnicas de los propios equipos.

CE3.2 Describir los componentes de los dispositivos de un sistema microinformático susceptibles de ajuste, reparación y sustitución para la resolución de averías, en función de los tipos de dispositivo a reparar, explicando sus características y procedimientos de sustitución o reparación.

CE3.3 Describir el procedimiento para la confección de cableado informático según el tipo de cable y conector, mediante presión, "crimpado" o soldadura, de adaptadores, conectores y latiguillos para cubrir necesidades específicas de conexión, explicando el uso de las herramientas al efecto.

CE3.4 Identificar tipos de impresoras y otros dispositivos asociados, distinguiendo las características entre ellas.

CE3.5 Reconocer fallos de funcionamiento propios de cada tipo de impresora o dispositivo asociado, para reemplazar las partes causantes del fallo, teniendo en cuenta las características técnicas.

CE3.6 Distinguir los procedimientos que se utilizan para la resolución de averías en impresoras y otros dispositivos asociados al equipo microinformático, en función de sus especificaciones técnicas.

CE3.7 En un supuesto práctico de reparación de una avería producida en un elemento del sistema microinformático, usando herramientas manuales, equipos o "software" específico según al caso:

- Identificar el componente causante de la avería, consultando el histórico de incidencias y averías y mediante la realización de pruebas funcionales para determinar las características de naturaleza física o lógica de la misma.
- Llevar a cabo las copias de seguridad ("backup") de los equipos microinformáticos, antes de la reparación o sustitución de los componentes, usando herramientas "software" para esta función y almacenando la copia en condiciones de seguridad, para asegurar la recuperación del sistema en caso necesario.
- Evaluar la sustitución del componente averiado o la posibilidad de su reparación, valorando los costes de reparación, tanto de piezas como de mano de obra.
- Sustituir o reparar el elemento responsable de la avería, confeccionando el cableado informático según el tipo de cable y conector, mediante presión, "crimpado" o soldadura, de adaptadores, conectores y latiguillos si fuese necesario para cubrir necesidades específicas de conexión, utilizando las herramientas al efecto.
- Comprobar los ajustes especificados en el "software" y en la configuración, verificando la funcionalidad del elemento reparado.
- Separar los embalajes, componentes desechables, consumibles y otros residuos, almacenándolos en los lugares destinados a ello, según tipología y según criterios de reducción en origen, reutilización, reciclado, valorización y eliminación y garantizando el cumplimiento de la normativa medioambiental aplicable.
- Documentar la solución de la avería, utilizando un modelo o aplicación, registrando las tareas efectuadas, incidencias y soluciones.

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

C1 respecto a CE1.5; C2 respecto a CE2.8 y C3 respecto a CE3.7.

Otras Capacidades:

Responsabilizarse del trabajo que desarrolla y del cumplimiento de los objetivos.
Finalizar el trabajo atendiendo a criterios de idoneidad, economía y eficacia.
Adaptarse a situaciones o contextos nuevos.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Componentes de un sistema informático

La unidad central de proceso: funciones y tipos, propósito y esquema de funcionamiento y estructura interna. El sistema de memoria: funciones y tipos, espacios de direccionamiento y mapas de memoria, y jerarquías de memoria. El sistema de E/S: funciones y tipos, controladores de E/S, dispositivos periféricos, dispositivos de almacenamiento y dispositivos de impresión, entre otros. Conexión entre componentes. Puertos, conectores y ranuras ("slot"). Buses internos y externos. Esquemas funcionales de los dispositivos y periféricos conectables por cable, medios inalámbricos o red a equipos informáticos. Componentes eléctricos, electrónicos y electromecánicos que componen los equipos y dispositivos. Medida de señales de las interfaces, buses y conectores de los diversos componentes de un sistema microinformático: de alimentación, de control y de datos. Soportes de almacenamiento: características, componentes y esquemas funcionales.

2 Conectividad de un equipo informático

Interfaces físicos de red. Clasificación y características. Direccionamiento en redes. Máscara de red Direcciones física y lógica. Cliente DNS. Configuración. Aplicaciones de prueba y evaluación de la conectividad. Comandos del sistema.

3 Incidencias relacionadas con el "hardware" en equipos informáticos

Tipos de incidencias en equipos informáticos: clasificación y características; averías típicas de los equipos informáticos tanto lógicas como físicas. Diagnóstico y localización de incidencias en equipos informáticos: técnicas de diagnóstico y detección. Herramientas "software" de diagnóstico: tipos y características. Herramientas "hardware" de diagnóstico: tipos y características. Conexionado externo e interno de los equipos informáticos: tipos de cables, tipos de conectores, significado de las patillas de las diversas interfaces y conectores de un equipo informático, técnicas de realización de cableado según tipología. Conexionado inalámbrico. Reparación de equipos informáticos. Elaboración de presupuestos de reparación: costes de componentes, tiempos, tipos de reparaciones y tipos componentes. Procedimientos de la reparación.

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 mantenimiento del subsistema físico en sistemas 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

Mantenimiento del "software" de base y aplicaciones en sistemas informáticos

Nivel:	*2*
Código:	*MF0958_2*
Asociado a la UC:	*UC0958_2 - Mantener el "software" de base y las aplicaciones en sistemas informáticos*
Duración (horas):	*90*
Estado:	*Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar técnicas de actualización de aplicaciones ofimáticas y corporativas en un equipo informático, descargando la última versión del fabricante, comprobando la compatibilidad con el sistema para aplicar las correcciones y mejoras de las nuevas versiones.

CE1.1 Localizar fuentes de descarga de aplicaciones, diferenciándolas según el modo de descarga tal como FTP, página web, actualización automática o descarga directa y el tipo de archivo o modo de instalación que proporciona.

CE1.2 Explicar mecanismos de detección de incidencias en las aplicaciones, describiendo cómo diagnosticar y resolver el problema.

CE1.3 Enumerar técnicas de comprobación del rendimiento de un sistema informático, describiendo el procedimiento de uso.

CE1.4 En un supuesto práctico de actualización de una aplicación "software" descargando la última versión del fabricante, comprobando la compatibilidad con el sistema:

- El "software" se actualiza, validándolo previamente en entornos similares al entorno productivo si fuera necesario, para asegurar su funcionalidad y operatividad, confirmando que no se producen disfunciones y/o pérdidas de información y/o datos, asegurando la integridad del equipo y la disponibilidad de la información, confirmando que no se produce pérdida de los datos previamente almacenados.
- Revisar la configuración inicial, verificando que sigue vigente o realizando las actualizaciones de parámetros afectados en su caso.
- Resolver las incidencias que aparezcan durante el proceso de actualización, diagnosticando el problema y consultando la documentación técnica del producto, volviendo a la versión anterior si fuera necesario, recurriendo a la persona responsable de sistemas y/o solicitado del fabricante asistencia en caso de persistir el problema.
- Comprobar el rendimiento del equipo, evaluando y comparando indicadores tales como uso de CPU, ocupación de memoria, acceso a disco u otros, antes y después de la actualización.
- Revisar la configuración "hardware" del equipo, verificando que se ajusta a los requisitos de la nueva versión, valorando posibles mejoras tales como aumento de memoria, CPU, cambio de disco o sustitución completa del equipo si fuera necesario.
- Documentar la actualización de los paquetes informáticos, incluyendo detalles tales como el nombre de la aplicación actualizada, versión, las incidencias generadas e incompatibilidades detectadas, referenciando soportes y registros, utilizando el modelo y/o aplicación informática establecidos por la entidad responsable de la instalación, garantizando la trazabilidad de los procesos.

C2: Aplicar técnicas de mantenimiento y de resolución de incidencias en la explotación de aplicaciones "software", identificando su naturaleza, para dar soporte a los usuarios de las mismas.

CE2.1 Describir el proceso de gestión de una incidencia, indicando los pasos desde que se recibe un aviso hasta que se resuelve totalmente.

CE2.2 Enumerar el tipo de incidencias más comunes en un sistema microinformático y los síntomas relacionados, asociando a cada una posibles soluciones y niveles de urgencia en la reparación.

CE2.3 Identificar técnicas de comunicación interpersonal tales como herramientas de gestión de incidencias, correo electrónico, videoconferencia u otras y herramientas de asistencia remota, describiendo su procedimiento de uso.

CE2.4 Aplicar técnicas de elaboración de informes de incidencia, a partir de supuestos errores descritos por un usuario.

CE2.5 Explicar procedimientos de salvaguarda de información y de recuperación de la misma después de una reparación, describiéndolos paso a paso.

CE2.6 En un supuesto práctico de aplicación de técnicas de mantenimiento en la explotación de aplicaciones "software", identificando su naturaleza:

- Asegurar que las aplicaciones se encuentran actualizadas, comprobando de manera periódica sus versiones.
- Revisar la vigencia de los certificados digitales, procediendo a su renovación en su caso.
- Programar las copias de seguridad, estableciendo una periodicidad adaptada a los riesgos.
- Definir el almacenamiento del "backup", garantizando la seguridad ante una posible pérdida del mismo, parametrizando los servidores o sistemas que lo alojarán.
- Establecer el tipo de copia a realizar, tal como total, diferencial o incremental, teniendo en cuenta la prioridad que se establezca de espacio y tiempos de copia o recuperación.
- Comprobar que el proceso de restauración desde esos servidores es funcional, mediante pruebas al efecto.
- Activar el mantenimiento de sistemas de disponibilidad u otros, para mantener la integridad de la información y la continuidad en la explotación durante la resolución de hipotéticos problemas.

CE2.7 En un supuesto práctico, de aplicación de técnicas de resolución de incidencias en la explotación de aplicaciones "software", identificando su naturaleza:

- Llevar a cabo la asistencia a un hipotético usuario, teniendo en cuenta técnicas de comunicación interpersonal, identificando la actuación requerida, satisfaciendo las exigencias y demandas del usuario y garantizando el resultado de la actuación, utilizando en su caso herramientas de acceso remoto al equipo defectuoso para agilizar su resolución.
- Diagnosticar el motivo que causó la incidencia: revisando la documentación que contiene el histórico de actuaciones realizadas a fin de determinar si alguna de ellas pudiera afectar al funcionamiento de la aplicación; inspeccionando el equipo y comprobando que no hay instalado "software" que no cumpla los requisitos técnicos del fabricante para el sistema; validando el estado del sistema: comprobando que hay espacio en disco libre, la memoria/CPU no está saturada y el equipo mantiene unos tiempos de respuesta aceptables.
- Documentar las actuaciones en un formato establecido a tal efecto, para facilitar su seguimiento, actualizando el repositorio de incidencias, la documentación técnica de la instalación y la configuración del sistema.

CE2.8 En un supuesto práctico de mantenimiento correctivo ante un fallo de "software" o tras la limpieza del equipo por virus, verificando el funcionamiento tras la aplicación de la solución:

- Reinstalar los componentes "software" afectados, estableciendo los parámetros indicados en las especificaciones establecidas en la documentación técnica y las necesidades de uso, implementando nuevas acciones correctoras en el caso de tratarse de incidencias repetitivas.
- Restaurar la información original perdida o alterada, en su caso actualizándola, aplicando medidas correctivas de forma que el sistema vuelva a estar en explotación.
- Verificar el funcionamiento del sistema una vez restaurado y la integridad de los datos, mediante pruebas al efecto para comprobar su funcionalidad.
- Documentar las actuaciones en un formato establecido a tal efecto, para facilitar su seguimiento, actualizando el repositorio de incidencias, la documentación técnica de la instalación y la configuración del sistema.

C3: Aplicar procesos de mantenimiento del sistema operativo, "software" de base y aplicaciones estándar, mediante revisión, verificación y monitorización, teniendo en cuenta las necesidades de uso, para detectar problemas y solucionarlos en su caso, en condiciones de calidad y seguridad.

CE3.1 Describir el sistema de archivos, explicando sus características y objetivos y las herramientas de gestión del almacenamiento, tales como herramientas de particionado y de tratamiento de errores físicos y lógicos.

CE3.2 Explicar el sistema de gestión de usuarios y grupos, describiendo las políticas de seguridad aplicables.

CE3.3 Describir procedimientos de actualización de versiones y copia de seguridad, clasificando los tipos de copia, explicando los pasos a seguir en cada caso, para salvaguardar la integridad y disponibilidad de un sistema.

CE3.4 Describir herramientas de monitorización de los recursos "hardware" del sistema microinformático, tales como memoria RAM, procesos activos, espacio en disco, CPU y Entrada/Salida, entre otros, explicando los procedimientos de uso.

CE3.5 Explicar el proceso de configuración de las opciones de accesibilidad de un sistema operativo, para facilitar el uso del equipo microinformático a personas con discapacidades, indicando los parámetros configurables y su funcionalidad.

CE3.6 Describir la configuración de un entorno de trabajo, tal como selección de fuentes, ajuste de la resolución del monitor, inclusión de accesos directos, aplicaciones de inicio y aspecto en general, indicando las opciones disponibles y su objetivo.

CE3.7 Enumerar las aplicaciones proporcionadas por un sistema operativo para la explotación de las funcionalidades de los dispositivos asociados al sistema, señalando sus características.

CE3.8 Clasificar mensajes y avisos proporcionados por el sistema microinformático para discriminar su importancia y criticidad, y explicar el proceso de respuesta según el tipo de alarma.

CE3.9 En un supuesto práctico de mantenimiento de un sistema operativo, "software" de base y aplicaciones estándar en un equipo microinformático mediante revisión, verificación y monitorización, teniendo en cuenta las necesidades de uso:
- Verificar el sistema de archivos, reconfigurando particiones en caso necesario y limpiando errores físicos, lógicos u otros, utilizando las utilidades, herramientas e interfaces que proporciona el sistema operativo, siguiendo unas especificaciones técnicas y según necesidades de operación.
- Monitorizar el rendimiento y el uso de recursos "hardware" dentro del equipo, tales como uso de CPU, uso de RAM, memoria de intercambio y datos SMART, entre otros, según necesidades de operación, generando alarmas y notificaciones mediante la utilización de herramientas para dicha función.

- Revisar las políticas de seguridad de usuarios y grupos, cotejándolas con unas políticas dadas, para garantizar su vigencia y, en su caso, para realizar las modificaciones correspondientes.
- Activar medidas de seguridad preventivas tales como actualizaciones, copias de seguridad periódicas de la información en un servidor de "backup", comprobando que el proceso de restauración desde esos servidores es funcional, para mantener la integridad de la información y la continuidad en la explotación.
- Comprobar el uso y gestión, por parte de los usuarios, de los dispositivos conectados directamente o por red al sistema microinformático, verificando que se realiza según la documentación técnica y procedimientos estipulados para explotar sus funcionalidades y en condiciones de seguridad.
- Detectar problemas, interpretando los mensajes resultantes de la ejecución del "software" de base tales como los registros "log" del sistema u otros, mediante la consulta de los manuales o la documentación proporcionada por el fabricante, entre otros.
- Corregir los problemas detectados, aplicando soluciones según las necesidades en cada caso, teniendo en cuenta las señales de problema detectadas y su diagnóstico, siguiendo procedimientos del fabricante.
- Documentar el trabajo realizado, indicando las incidencias surgidas y las soluciones aplicadas, utilizando un modelo de documento, para su archivo y posterior consulta.

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

C1 respecto a CE1.4; C2 respecto a CE2.6, CE2.7 y CE2.8; C3 respecto a CE3.9.

Otras Capacidades:

Responsabilizarse del trabajo que desarrolla y del cumplimiento de los objetivos.
Finalizar el trabajo atendiendo a criterios de idoneidad, economía y eficacia.
Adaptarse a situaciones o contextos nuevos.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Sistemas operativos en sistemas informáticos

Clasificación de los sistemas operativos. Tipos de licencia. Funciones de un sistema operativo. Sistemas operativos para equipos microinformáticos: características y utilización. Modo comando. Modo gráfico.

2 Mantenimiento de sistemas operativos en sistemas informáticos

Actualización de sistemas operativos. Procedimientos. Actualización de drivers y configuraciones de dispositivos. Usuarios y grupos. Permisos. Actualización de sistemas operativos. Servidores y herramientas de actualización, servicios y herramientas de alerta temprana. Utilidades del sistema operativo. Características y funciones. Utilidades del "software" de base: configuración del entorno de trabajo; administración y gestión de los sistemas de archivos; gestión de procesos y recursos; gestión y edición de archivos; monitorización de recursos; gestión de la seguridad de sistemas operativos y aplicaciones preinstaladas. Monitorización del sistema. Herramientas del sistema operativo para la obtención de información de estado. Visores del sistema y registros "log".

3 Configuración de aplicaciones, programas y utilidades

Tipos de licencias de aplicaciones y sistemas operativos: uso libre, uso temporal, en desarrollo (beta), acuerdos corporativos de uso de aplicaciones, licencias mediante código, licencias mediante mochilas. "Software" libre y "copyright". Componentes de una aplicación: manual de instalación, manual de usuario. Instalación y registro de aplicaciones. Configuración de aplicaciones.

4 Procedimientos de mantenimiento preventivo y correctivo del sistema informático

Verificación del sistema: procedimientos de obtención de información y características del "hardware", utilidades y herramientas de gestión, test, diagnóstico y reparación (CPU, memoria, discos, controlador gráfico), controladores de dispositivos. Procedimientos de limpieza y ahorro de espacio en disco. Procedimientos de copia de seguridad y recuperación. Tipos de copia de seguridad. Discos de recuperación del sistema. Monitorización remota del uso de recursos. Metodologías de resolución de problemas en las aplicaciones "software". Eliminación de virus y recuperación de los datos. Actualización de los patrones del antivirus.

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 el mantenimiento del "software" de base y aplicaciones en sistemas 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 3

Configuración de la ciberseguridad en equipos finales

Nivel: *2*
Código: *MF0959_2*
Asociado a la UC: *UC0959_2 - Configurar la ciberseguridad en equipos finales*
Duración (horas): *120*
Estado: *Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de instalación de sistemas de protección frente a "malware" en equipos finales ("endpoint"), configurando los parámetros de protección, siguiendo unas especificaciones y procedimientos para garantizar su seguridad.

CE1.1 Determinar los parámetros de configuración del sistema operativo a modificar para el funcionamiento de una protección frente a "malware", explicando cómo se verifica su funcionamiento los pasos para validar los parámetros especificados según indique la documentación técnica.

CE1.2 Relacionar programas de utilidad incluidos en el sistema operativo que se deben configurar para el uso de una protección frente a "malware", verificando cuáles son imprescindibles para la funcionalidad que se pretende, instalándolos y configurándolos de acuerdo con especificaciones técnicas o desinstalándolos en su caso.

CE1.3 Enumerar de parámetros de seguridad relativa al "software" no deseado a configurar en un sistema de protección frente a "malware", tales como extensiones de programas y ficheros no permitidas, carpetas de especial protección, listas blancas de ficheros, actuación frente a ficheros no firmados digitalmente o con firma desconocida o caducada, describiendo su utilidad y los pasos para asociar una acción según el caso, tal como bloquear, enviar a cuarentena, permitir o aplicación de cualquier otro filtro de protección frente a "malware" y "software" no deseado.

CE1.4 Describir el proceso de configuración de eventos de notificación y alarmas en un sistema de protección frente a "malware", indicando los pasos para establecer parámetros tales como correos de notificación frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog" u otros.

CE1.5 Explicar el proceso de instalación del "software" cliente para equipos y servidores, definiendo los pasos de configuración en un sistema, y los valores a asignar en parámetros tales como versión de sistema operativo, carpetas de exclusión y/o exclusión de aplicación o programas particulares, entre otros.

CE1.6 Detallar el proceso para configurar frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en un sistema de protección frente a "malware", estableciendo las condiciones de actualización de todos los equipos.

CE1.7 Enumerar opciones anti "tampering" para la protección contra la desactivación y desinstalación del "software" cliente de protección frente a "malware" en un sistema, detallando cómo establecer parámetros de seguridad tales como contraseña o pin de

desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.

CE1.8 En un supuesto práctico de instalación de sistemas de protección frente a "malware", configurando los parámetros de protección, siguiendo unas especificaciones para garantizar su seguridad:

- Verificar la configuración de un sistema operativo para el funcionamiento de una protección frente a "malware", validando los parámetros que indique la documentación técnica.
- Configurar programas de utilidad incluidos en el sistema operativo, para el uso de la protección frente a "malware", previa instalación en su caso y verificando que se mantienen únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.
- Definir la seguridad relativa al "software" no deseado en un sistema de protección frente a "malware", asignando parámetros tales como extensiones de programas y ficheros no permitidas, carpetas de especial protección, listas blancas de ficheros, actuación frente a ficheros no firmados digitalmente o con firma desconocida o caducada, junto con el veredicto de bloquear, enviar a cuarentena, permitir o aplicación de cualquier otro filtro de protección, entre otros, para proteger al sistema frente a "malware".
- Configurar eventos de notificación y alarmas en un sistema de protección frente a "malware", estableciendo parámetros tales como correos de notificación frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog" u otros.
- Configurar paquetes de instalación del "software" cliente para equipos y servidores se configuran en el sistema, definiendo parámetros tales como versión de sistema operativo, carpetas de exclusión y/o exclusión de aplicación o programas particulares, entre otros.
- Configurar frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en un sistema de protección frente a "malware", estableciendo las condiciones de actualización de todos los equipos.
- Configurar opciones anti "tampering" para la protección contra la desactivación y desinstalación de un "software" cliente de protección frente a "malware", estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.
- Verificar la instalación mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad, para comprobar la funcionalidad del sistema de seguridad.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos o plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C2: Instalar sistemas avanzados de detección y respuesta (EDR: "Endpoint Detection and Response"), configurando los parámetros de protección, siguiendo unas especificaciones y procedimientos para garantizar su seguridad.

CE2.1 Describir el procedimiento de instalación de unos paquetes de "software" cliente de protección frente a amenazas avanzadas para equipos y servidores, indicando los pasos y valores de parámetros de configuración tales como versión de sistema operativo, datos específicos de suscripción a la plataforma de nube, y datos de conexión.

CE2.2 Enumerar tácticas, técnicas y procedimientos empleados por atacantes, programas y utilidades frecuentemente utilizadas, direcciones IP de comunicación, empleo de credenciales de administradores, detallando su uso en la configuración de alertas avanzadas de detección de intrusión se definen en el sistema y describiendo los pasos para asignar un grado de severidad y configurar la notificación de los eventos detectados por una plataforma.

CE2.3 Clasificar parámetros activos de detección de amenazas avanzadas tal como frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas, explicando cómo se configuran en un sistema y para múltiples equipos.

CE2.4 Enumerar opciones anti "tampering" para la protección de desactivación y desinstalación del "software" cliente de protección frente a amenazas avanzadas, describiendo su configuración y el establecimiento de parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.

CE2.5 En un supuesto práctico de instalación de sistemas avanzados de detección y respuesta (EDR: "Endpoint Detection and Response"), configurando los parámetros de protección, siguiendo unas especificaciones, para garantizar su seguridad:

- Configurar en un sistema paquetes de instalación del "software" cliente de protección frente a amenazas avanzadas para equipos y servidores, definiendo parámetros tales como versión de sistema operativo, datos específicos de suscripción a la plataforma de nube, y datos de conexión.
- Definir alertas avanzadas de detección de intrusión en el sistema, estableciendo parámetros tales como tácticas, técnicas y procedimientos empleados por atacantes, programas y utilidades frecuentemente utilizadas, direcciones IP de comunicación, empleo de credenciales de administradores, entre otras, así como asignando la severidad de las alertas para la detección y notificación de los eventos detectados por la plataforma.
- Configurar unos eventos de notificación y alarmas en el sistema de protección frente a "malware", estableciendo parámetros tales como correos frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog", entre otros.
- Configurar frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en el sistema, estableciéndolas en todos los equipos.
- Configurar opciones anti "tampering" para la protección de desactivación y desinstalación del "software" cliente de protección frente a amenazas avanzadas, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.
- Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos o plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C3: Aplicar procedimientos de instalación de sistemas de cifrado de información en disco, configurando los parámetros relacionados, siguiendo unas especificaciones y procedimientos para garantizar su seguridad.

CE3.1 Identificar puntos de configuración del sistema operativo relativos al funcionamiento del cifrado, describiendo como comprobar y validar los parámetros relacionados según indique la documentación técnica.

CE3.2 Identificar programas de utilidad incluidos en el sistema operativo que es necesario instalar y/o configurar para el uso del cifrado, explicando cómo verificar cuáles son los imprescindibles para la funcionalidad que se pretende, de acuerdo con unas especificaciones técnicas.

CE3.3 Enumerar posibilidades para almacenamiento seguro de información, describiendo el proceso de configuración mediante la asignación de parámetros tales como tamaño, permisos

de accesos, claves de protección para el almacenamiento de claves y certificados de descifrado de los clientes.

CE3.4 Describir el procedimiento para definir en el sistema unas políticas de cifrado, explicando cómo establecer parámetros tales como unidades de disco a cifrar, algoritmos de cifrado (AES, DES, entre otros), longitud de clave, secuencia de encendido de equipos, elemento de paso del cifrado (clave, certificado, pin, entre otros) o número máximo de intentos de descifrado, según cada tipo de equipo y servidor.

CE3.5 Clasificar opciones anti "tampering" de protección de desactivación y desinstalación del "software" cliente de cifrado, diferenciando sus ventajas e inconvenientes, explicando cómo se configuran en el sistema, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o desactivación del producto del cliente.

CE3.6 En un supuesto práctico de aplicación de procedimientos de instalación de sistemas de cifrado de información en disco, configurando los parámetros relacionados, siguiendo unas especificaciones y procedimientos para garantizar su seguridad:

- Verificar la configuración de un sistema operativo para el funcionamiento del cifrado, validando los parámetros especificados según indique la documentación técnica.
- Configurar los programas de utilidad incluidos en un sistema operativo para el uso del cifrado, previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.
- Definir un almacenamiento seguro de información, configurándolo mediante la asignación de parámetros tales como tamaño, permisos de accesos, claves de protección para el almacenamiento de claves y certificados de descifrado de los clientes.
- Definir una relación de políticas de cifrado de información en el sistema, estableciendo parámetros tales como unidades de disco a cifrar, algoritmos de cifrado (AES, DES, entre otros), longitud de clave, secuencia de encendido de equipos, elemento de paso del cifrado (clave, certificado, pin, entre otros) o número máximo de intentos de descifrado, según cada tipo de equipo y servidor.
- Configurar en el sistema opciones anti "tampering" de protección de desactivación y desinstalación del "software" cliente de cifrado, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o desactivación del producto del cliente.
- Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

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

C1 respecto a CE1.8; C2 respecto a CE2.5 y C3 respecto a CE3.6.

Otras Capacidades:

Aplicar las instrucciones de trabajo de manera organizada, precisa y meticulosa.
Comprender y valorar las motivaciones y consecuencias del trabajo bien realizado.
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.

Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Configuración de la seguridad en sistemas operativos

Configuración del sistema operativo para el funcionamiento de protección frente a "malware", sistemas avanzados de detección y respuesta y sistemas de cifrado de información en disco. Parámetros. Configuración de programas de utilidad incluidos en el sistema operativo para el uso de una protección frente a "malware", sistemas avanzados de detección y respuesta y sistemas de cifrado de información en disco.

2 Sistemas de protección frente a "malware"

Sistema de protección frente a "malware". Parámetros de configuración: extensiones de programas y ficheros no permitidas, carpetas de especial protección, listas blancas de ficheros, actuación frente a ficheros no firmados digitalmente o con firma desconocida o caducada, entre otros. Acciones asociadas: bloquear, enviar a cuarentena, permitir o aplicación de cualquier otro filtro de protección, entre otros. Eventos de notificación y alarmas: correos de notificación frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog" u otros. Instalación del "software" cliente para equipos y servidores. Parámetros: versión de sistema operativo, carpetas de exclusión y/o exclusión de aplicación o programas particulares, entre otros. Parámetros activos de detección de "malware": frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas. Condiciones de actualización de todos los equipos. Opciones anti "tampering" para la protección contra la desactivación y desinstalación del "software" cliente de protección frente a "malware" en un sistema. Parámetros: contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.

3 Sistemas avanzados de detección y respuesta (EDR: "Endpoint Detection and Response")

Instalación de paquetes de "software" cliente de protección frente a amenazas avanzadas para equipos y servidores. Parámetros: versión de sistema operativo, datos específicos de suscripción a la plataforma de nube, y datos de conexión entre otros. Tácticas, técnicas y procedimientos empleados por atacantes, programas y utilidades frecuentemente utilizadas, direcciones IP de comunicación, empleo de credenciales de administradores. Configuración de alertas avanzadas de detección de intrusión. Parámetros activos de detección de amenazas avanzadas: frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas. Opciones anti "tampering" para la protección de desactivación y desinstalación del "software" cliente de protección frente a amenazas avanzadas. Parámetros: contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección. Sistemas XDR ("Extended Detection and Response").

4 Sistemas de cifrado de información en disco

Almacenamiento seguro de información. Configuración de sistemas de cifrado. Parámetros: tamaño, permisos de accesos, claves de protección para el almacenamiento de claves y certificados de descifrado de los clientes, entre otros. Definición de políticas de cifrado. Establecimiento de unidades de disco a cifrar, algoritmos de cifrado (AES, DES, entre otros), longitud de clave, secuencia de encendido de equipos, elemento de paso del cifrado (clave, certificado, pin, entre otros) o número máximo de intentos de descifrado, según cada tipo de equipo y servidor. Opciones

anti "tampering" de protección de desactivación y desinstalación del "software" cliente de cifrado. Parámetros: contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o desactivación del producto de los clientes.

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 configuración de la ciberseguridad en equipos finales, 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 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 4

Configuración de la seguridad en redes de comunicaciones y sistemas de correo electrónico

Nivel:	*2*
Código:	*MF2797_2*
Asociado a la UC:	*UC2797_2 - Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico*
Duración (horas):	*180*
Estado:	*Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de instalación de un sistema de cortafuegos, configurando los parámetros relacionados, siguiendo unas especificaciones y procedimientos, para garantizar la seguridad de una red.

CE1.1 Diferenciar zonas de seguridad en redes, describiendo cómo asociarlas a los interfaces de red y los pasos para establecer una zona de menor seguridad, generalmente conectada a Internet, una zona de mayor seguridad, una zona desmilitarizada y el resto de zonas.

CE1.2 Describir el procedimiento de aplicación de una política de seguridad relativa a flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad, explicando los pasos para configurar elementos tales como:

- Establecer unos flujos de conexiones iniciados desde redes de mayor seguridad hacia redes de menor seguridad.
- Establecer los flujos de conexiones hacia redes con vulnerabilidades intencionadas "honeynets".
- Bloquear flujos de conexiones iniciados desde redes de menor seguridad a redes de mayor seguridad que no estén explícitamente permitidas.
- Aplicar el filtrado en un cortafuegos entre las zonas de seguridad, estableciendo las direcciones IP y puertos permitidos y no permitidos.

CE1.3 Explicar el proceso de configuración sobre los cortafuegos de una relación de políticas de filtrado entre zonas de seguridad, describiendo el establecimiento de direcciones IP y puertos permitidos y no permitidos entre las zonas de diferente tipo.

CE1.4 Explicar el proceso de configuración sobre los cortafuegos de una relación de políticas de filtrado de tráfico entre las zonas de seguridad, detallando las posibilidades de parametrización de reglas y firmas de protección específicas frente a ataques conocidos entre las diferentes zonas, tales como "Port enumeration", "TCP Split handshake", "TCP SYN flood", entre otros.

CE1.5 Detallar el proceso de configuración de eventos de notificación y alarmas en un cortafuegos, describiendo el establecimiento de parámetros tales como correos de notificación frente a alertas críticas y altas y/o envío de paquetes de notificación mediante "syslog", entre otros.

CE1.6 En un supuesto práctico de aplicación de procedimientos de instalación de un sistema de cortafuegos, configurando los parámetros relacionados, siguiendo unas especificaciones y procedimientos, para garantizar la seguridad de una red:

- Asociar unas zonas de seguridad a interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas.
- Aplicar una política de seguridad relativa a flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad, configurando acciones tales como permitir los flujos de conexiones iniciados desde redes de mayor seguridad hacia redes de menor seguridad, Establecer los flujos de conexiones hacia redes con vulnerabilidades intencionadas "honeynets". bloquear los flujos de conexiones iniciados desde redes de menor seguridad a redes de mayor seguridad que no estén explícitamente permitidas y aplicar el filtrado en el cortafuegos entre las zonas de seguridad, estableciendo las direcciones IP y puertos permitidos y no permitidos.
- Aplicar una relación de políticas de filtrado entre las zonas de seguridad sobre los cortafuegos, estableciendo las direcciones IP y puertos permitidos y no permitidos entre las zonas de diferente tipo.
- Aplicar sobre los cortafuegos una relación de políticas de filtrado de tráfico entre las zonas de seguridad, estableciendo las reglas y firmas de protección específicas frente a ataques conocidos entre las zonas, tales como "Port enumeration", "TCP Split handshake", "TCP SYN flood", entre otros.
- Configurar en el cortafuegos eventos de notificación y alarmas, estableciendo parámetros tales como correos de notificación frente a alertas críticas y altas y/o envío de paquetes de notificación mediante "syslog", entre otros.
- Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C2: Aplicar procedimientos de instalación de sistemas de detección y prevención de intrusiones (IDS/IPS), configurando parámetros relacionados, siguiendo unas especificaciones y procedimientos, para garantizar la seguridad de un sistema de comunicaciones.

CE2.1 Detallar el proceso de conexión de cables de entrada y salida a los interfaces de un IDS/IPS de acuerdo a unas especificaciones técnicas, explicando los pasos a seguir para posibilitar la inspección del tráfico de red, asociando unas zonas de seguridad, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas.

CE2.2 Explicar el procedimiento para configurar firmas de detección de ataques en el sistema IDS/IPS, habilitándolas de acuerdo con las especificaciones técnicas, indicando cómo establecer las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones y la configuración de la periodicidad de actualización de dichas firmas.

CE2.3 Describir el funcionamiento de un sistema señuelo ("honeypot"), explicando cómo se configuran para establecer aplicaciones y servicios trampa atractivos ante ataques, recopilando información sobre métodos y comportamientos.

CE2.4 Definir reglas de detección de ataques por comportamiento, describiendo los procesos de configuración para habilitarlas en el sistema IDS/IPS, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones.

CE2.5 En un supuesto práctico de aplicación de procedimientos de instalación de sistemas de detección y prevención de intrusiones (IDS/IPS), configurando los parámetros relacionados, siguiendo unas especificaciones y procedimientos, para garantizar su seguridad de un sistema:

- Los cables de red de entrada y salida de datos se conectan a cada uno de los interfaces del IDS/IPS de acuerdo a especificaciones técnicas y organizativas, para posibilitar la inspección del tráfico de red.
- Asociar zonas de seguridad a los interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas.
- Configurar firmas de detección de ataques, habilitándolas en el sistema IDS/IPS de acuerdo con las especificaciones técnicas y organizativas, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones.
- Actualizar las firmas de detección de ataques del sistema IDS/IPS periódicamente, instalando la versión más reciente.
- Configurar unas reglas de detección de ataques por comportamiento, habilitándolas en el sistema IDS/IPS de acuerdo a las especificaciones técnicas, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones, para la protección de las redes de comunicaciones.
- Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C3: Aplicar procedimientos de instalación de sistemas de filtrado de navegación, configurando parámetros relacionados, siguiendo unas especificaciones y procedimientos para garantizar la seguridad de las comunicaciones.

CE3.1 Describir el procedimiento de configuración de unas políticas de acceso a la navegación en un sistema de filtrado, explicando cómo se establecen las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas.

CE3.2 Explicar el proceso de configuración de unas políticas de acceso de categorías de contenidos web en un sistema de filtrado, describiendo los pasos para establecer aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web.

CE3.3 Clasificar perfiles de acceso de navegación, detallando cómo se configuran para cada usuario y nodo de comunicación en un sistema, definiendo para cada uno de ellos las políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar.

CE3.4 En un supuesto práctico de aplicación de procedimientos de instalación de sistemas de filtrado de navegación, configurando parámetros relacionados, siguiendo unas especificaciones y procedimientos para garantizar la seguridad de las comunicaciones:
- Configurar una política de acceso a la navegación, estableciendo las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas, para la protección de las redes.
- Configurar una política de acceso de categorías de contenidos web, estableciendo aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web.
- Configurar unos perfiles de acceso de navegación para cada usuario y nodo de comunicación, definiendo para cada uno de ellos las políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar.
- Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad.

- Confeccionar la documentación de los procesos realizados se confecciona, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C4: Aplicar procedimientos de instalación de sistemas de gestión de eventos de seguridad (SIEM), configurando parámetros relacionados, siguiendo unas especificaciones y procedimientos, para garantizar la seguridad de un sistema.

CE4.1 Identificar los puntos de configuración de un sistema operativo para el funcionamiento de un SIEM, detallando el proceso de validación de los parámetros especificados según la documentación técnica.

CE4.2 Reconocer los programas de utilidad incluidos en el sistema operativo que se requieren para el uso de los SIEM, desinstalándolos en caso contrario, detallando cómo configurarlos de acuerdo con especificaciones técnicas.

CE4.3 Enumerar fuentes de información, tal como sistema de protección contra el "malware", cortafuegos, sistemas de detección de intrusión, entre otros, para su registro en la herramienta, indicando el proceso de configuración en el SIEM, describiendo las reglas de "parseado" y normalización de eventos para cada tipo de fuente de acuerdo a las especificaciones técnicas específicas del fabricante para cada fuente y configurando campos tales como tipo de evento, dirección IP, usuario, entre otros.

CE4.4 Describir la estructura de las reglas de agregado y correlación en el sistema de detección de alertas de un SIEM, explicando el proceso de configuración para cada caso de uso, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros.

CE4.5 Explicar el procedimiento de configuración de reglas de generación de alertas para cada caso de uso en el sistema de detección de alertas de un SIEM, asignando parámetros tales como severidad, tipo de alerta, sistemas afectados, fecha y hora, entre otros, para la posterior notificación y tratamiento de la alerta.

CE4.6 Detallar el procedimiento para configurar eventos de notificación de alertas en el SIEM, indicando los pasos para establecer parámetros para cada tipo de alerta y severidad, tales como correos de notificación frente a apertura de tiques en sistemas de gestión de la demanda u otros medios o sistemas válidos, para la notificación automatizada de eventos.

CE4.7 En un supuesto práctico de aplicación de procedimientos de instalación de sistemas de gestión de eventos de seguridad (SIEM), configurando parámetros relacionados, siguiendo unas especificaciones y procedimientos, para garantizar la seguridad de un sistema:

- Verificar la configuración de un sistema operativo para el funcionamiento de los SIEM, validando los parámetros especificados según indique la documentación técnica.
- Configurar programas de utilidad incluidos en el sistema operativo para el uso de los SIEM, previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.
- Configurar sistemas de recolección de información en el SIEM, especificando el tipo de fuente de información, tal como sistema de protección contra el "malware", cortafuegos, sistemas de detección de intrusión, entre otros, para su registro en la herramienta.
- Configurar unas reglas de "parseado" y normalización de eventos para cada tipo de fuente, de acuerdo a las especificaciones técnicas específicas del fabricante para cada fuente, configurando campos tales como tipo de evento, dirección IP, usuario, entre otros.
- Configurar unas reglas de agregado y correlación para cada caso de uso, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros, para el sistema de detección de alertas del SIEM.

- Configurar unas reglas de generación de alertas para cada caso de uso, asignando parámetros tales como severidad, tipo de alerta, sistemas afectados, fecha y hora, entre otros, para la posterior notificación y tratamiento de la alerta.
- Configurar en el SIEM unos eventos de notificación de alertas, estableciendo parámetros para cada tipo de alerta y severidad, tales como correos de notificación frente a apertura de tiques en sistemas de gestión de la demanda u otros medios o sistemas válidos, para la notificación automatizada de eventos.
- Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C5: Aplicar procedimientos de configuración del "software" de base y aplicaciones de un sistema informático para la protección del correo electrónico, verificando su funcionalidad y comprobando la seguridad, siguiendo unas especificaciones y procedimientos para la protección del sistema.

CE5.1 Explicar el procedimiento de verificación de la configuración del sistema operativo, indicando cómo comprobar su funcionamiento y los parámetros específicos que se recojan en la documentación técnica del producto para la instalación y configuración de la protección del correo electrónico.

CE5.2 Enumerar programas de utilidad disponibles en un sistema operativo, determinando cuáles serían los mínimos a instalar para determinadas funciones requeridas, describiendo los pasos para su configuración con los parámetros que se indique en la documentación o instrucciones al efecto.

CE5.3 Describir perfiles, privilegios y el proceso de asignación a usuarios para el funcionamiento del sistema, según los principios de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know") y de acuerdo a especificaciones técnicas.

CE5.4 Comprender el funcionamiento de los sistemas de encriptado de comunicaciones y correo electrónico, describiendo el proceso de instalación y configuración de claves y certificados.

CE5.5 Diferenciar pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad, detallando el procedimiento de aplicación en cada caso.

CE5.6 En un supuesto práctico de aplicación de procedimientos de configuración del "software" de base y aplicaciones de un sistema informático, verificando su funcionalidad y comprobando la seguridad, siguiendo unas especificaciones y procedimientos:
- Verificar la configuración de un sistema operativo para el funcionamiento de la protección del correo electrónico, comprobando los parámetros específicos que se indiquen en la documentación técnica del producto.
- Instalar unos programas de utilidad disponibles en el sistema operativo, verificando que son los mínimos que se necesitan para las funciones requeridas, configurándolos para su uso con los parámetros que se indique en la documentación o instrucciones de configuración.
- Crear unos usuarios imprescindibles para el funcionamiento del sistema, configurando el mínimo conjunto de privilegios para cada uno, de acuerdo a las especificaciones técnicas.
- Verificar la instalación, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.

- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos o plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C6: Aplicar procesos de instalación de sistemas perimetrales de filtrado de correo electrónico, configurando los parámetros y acciones relacionados con su seguridad, según unas especificaciones y procedimientos para la protección del sistema de correo.

CE6.1 Enumerar sistemas de consulta de reputación de dominios y acciones de filtrado de correo, describiendo cómo establecer las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo electrónico recibido.

CE6.2 Describir información detallada que se requiere para la confección de los registros DNS, explicando cómo localizarla, tal como:

- Relación de dominios desde los que se enviara el correo electrónico.
- Direcciones IP públicas de los sistemas de correo electrónico con flujo saliente.
- Configuración de la política SPF ("Sender Policy Framework").
- Relación de dominios de correo electrónico, y clave pública DKIM ("Domainkey Identified Mail") asociada.
- Publicación de política del dominio en entradas DNS de DMARC ("Domain-based Message Authentication, Reporting and Conformance").

CE6.3 Explicar los mecanismos de configuración de umbrales de valoración de correos electrónicos para la determinación de correo sospechoso y no deseado, indicando cómo se comprueban, y cómo se verifica que son aplicados sobre los sistemas de protección de correo electrónico.

CE6.4 Detallar el proceso de configuración de unos sistemas de protección de correo electrónico a relación de dominios, "emails" y ficheros adjuntos que deben de tener un tratamiento especial en relación a la seguridad, describiendo cómo se asignan acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.

CE6.5 Interpretar filtros de análisis semántico para la detección de contenido no deseado en el correo electrónico, describiendo el proceso de definición de acciones para cada uno, tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.

CE6.6 Describir un sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos, indicando cómo configurar, entre otros, el servidor y el "email" de notificación, para asegurar la comunicación de alertas del sistema a un hipotético equipo responsable de la gestión del incidente.

CE6.7 En un supuesto práctico de aplicación de procesos de instalación de sistemas perimetrales de filtrado de correo electrónico, configurando los parámetros y acciones relacionados con su seguridad, según unas especificaciones y procedimientos:

- Configurar unos sistemas de consulta de reputación de dominios y las acciones de filtrado de correo, estableciendo las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo electrónico recibido.
- Relacionar la información que se requiere para la confección de unos registros DNS, detallando los valores de los parámetros para su implementación.
- Comprobar umbrales de valoración de unos correos electrónicos para la determinación de correo sospechoso y no deseado, verificando que son aplicados sobre los sistemas de protección de correo electrónico.

- Configurar un sistema de protección para una relación de dominios, "emails" y ficheros adjuntos que deben de tener un tratamiento especial, asignando acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.
- Definir filtros de análisis semántico para la detección de contenido no deseado sobre los sistemas de protección de correo electrónico, asignando acciones para cada uno de éstos tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.
- Definir un sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos, configurando, entre otros, el servidor y el "email" de notificación, para asegurar la comunicación de alertas del sistema a un hipotético equipo responsable de la gestión del incidente.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos o plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C7: Aplicar procedimientos de instalación de sistemas perimetrales de prevención de fuga de información en el correo electrónico, configurándolos según unas especificaciones y procedimientos para garantizar su seguridad.

CE7.1 Clasificar políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico, tales como bloquear, poner en cuarentena o generar una notificación de violación de la política, describiendo los pasos para asignarlas a cada tipo de fichero o conjunto de información.

CE7.2 Describir el procedimiento de configuración de nivel de acceso de usuarios encargados de los análisis de investigación de los casos, indicando los pasos para establecer ese nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos.

CE7.3 Reconocer los medios y sistemas de notificación de violación de las políticas de fuga de información en un sistema, explicando cómo se configuran y cómo se verifica su funcionamiento, de acuerdo a las especificaciones técnicas.

CE7.4 Enumerar tipos de pruebas tales como pruebas de análisis del rendimiento, funcionales y de seguridad, describiendo los pasos para verificar y comprobar la funcionalidad del sistema de seguridad.

CE7.5 En un supuesto práctico de aplicación de procedimientos de instalación de sistemas perimetrales de prevención de fuga de información en el correo electrónico, configurándolos según unas especificaciones y procedimientos para garantizar su seguridad:
- Aplicar una relación de políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico, proporcionando para cada tipo de fichero o conjunto de información, el veredicto de bloquear, poner en cuarentena o notificar una violación de la política al usuario.
- Configurar unos usuarios encargados de los análisis de investigación de los casos, definiendo para cada uno de ellos el nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos.
- Configurar en el sistema unos medios y sistemas de notificación de violación de las políticas de fuga de información, verificando su funcionamiento, de acuerdo a las especificaciones técnicas.
- Verificar la instalación, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos o plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

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

C1 respecto a CE1.6; C2 respecto a CE2.5; C3 respecto a CE3.4; C4 respecto a CE4.7; C5 respecto a CE5.6; C6 respecto a CE6.7 y C7 respecto a CE7.5.

Otras Capacidades:

Aplicar las instrucciones de trabajo de manera organizada, precisa y meticulosa.
Comprender y valorar las motivaciones y consecuencias del trabajo bien realizado.
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.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Instalación de un sistema de cortafuegos

Zonas de seguridad en redes: zona de menor seguridad, zona de mayor seguridad, zona desmilitarizada y el resto de zonas. Asociación a interfaces de red. Flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad. Políticas de seguridad. Acciones de bloqueo. Redes con vulnerabilidades intencionadas "honeynets". Establecimiento de flujos de conexión. Configuración del filtrado entre zonas en cortafuegos. Configuración de filtrado de tráfico entre las zonas de seguridad. Parametrización de reglas y firmas de protección específicas frente a ataques conocidos entre las zonas, tales como "Port enumeration", "TCP Split handshake", "TCP SYN flood", entre otros. Configuración de eventos de notificación y alarmas en un cortafuegos.

2 Instalación de sistemas de detección y prevención de intrusiones (IDS/IPS)

Conexión de cables de entrada y salida a los interfaces de un IDS/IPS según zonas de seguridad. Sistemas señuelo ("Honeypot"). Configuración de firmas de detección de ataques en el sistema IDS/IPS. Reglas y acciones. Periodicidad de actualización de firmas. Detección de ataques por comportamiento. Reglas y acciones a realizar.

3 Instalación de sistemas de filtrado de navegación

Configuración del sistema de filtrado. Redes internas y permisos de navegación. Condiciones. Políticas de acceso de categorías de contenidos web en un sistema de filtrado. Cuota de acceso. Clasificación de perfiles de acceso de navegación. Configuración en el sistema de usuarios y nodos de comunicación según políticas de acceso de navegación. "Proxies" transparentes.

4 Instalación de sistemas de gestión de eventos de seguridad (SIEM)

Configuración de sistemas operativos para el funcionamiento de un SIEM. Configuración de programas de utilidad incluidos en el sistema operativo para el uso de los SIEM. Fuentes de información a registrar en el SIEM: sistema de protección contra el "malware", cortafuegos, sistemas de detección de intrusión, entre otros. Reglas de "parseado" y normalización de eventos para cada tipo de fuente. Configuración de campos tales como tipo de evento, dirección IP, usuario, entre otros. Reglas de agregado y correlación en el sistema de detección de alertas de un SIEM. Parámetros: ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros. Reglas de generación de alertas para cada caso de uso en el sistema de detección de alertas de un SIEM. Parámetros: severidad, tipo de alerta, sistemas afectados, fecha y hora, entre otros. Eventos de notificación de alertas en el SIEM. Notificación automatizada de eventos.

5 Configuración del "software" de base y aplicaciones para la protección del correo electrónico

Verificación de la configuración de sistemas operativos. Utilidades disponibles en un sistema operativo. Instalación/desinstalación y configuración según criterios de seguridad. Usuarios. Perfiles y privilegios. Principios de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know"). Encriptado de comunicaciones y correo electrónico. Certificados. Encriptado simétrico y asimétrico. Pruebas del sistema. Análisis del rendimiento, pruebas funcionales y pruebas de seguridad.

6 Sistemas perimetrales de filtrado de correo electrónico

Sistemas de consulta de reputación de dominios. Sistema de filtrado de correo "antispam". Acciones a tomar por el sistema de filtrado. Confección de registros DNS. Información y parámetros relacionados: relación de dominios desde los que se enviara el correo electrónico, direcciones IP públicas de los sistemas de correo electrónico con flujo saliente, configuración del veredicto SPF ("Sender Policy Framework"), relación de dominios de correo electrónico, y clave pública DKIM ("Domainkey Identified Mail"), publicación de política del dominio en entradas DNS de DMARC ("Domain-based Message Authentication, Reporting and Conformance"). Determinación de correo sospechoso y no deseado. Configuración de umbrales de valoración. Sistemas de protección de correo electrónico a relación de dominios, "emails" y ficheros adjuntos. Configuración del tratamiento en relación a la seguridad. Asignación de acciones. Filtros de análisis semántico para la detección de contenido no deseado. Definición de acciones. Sistemas de notificación de eventos y alertas frente a correos potencialmente peligrosos. Configuración de servidor y correo de notificación.

7 Sistemas perimetrales de prevención de fuga de información en el correo electrónico

Políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico. Clasificación de contenido y acciones: bloqueo, puesta en cuarentena y/o generación de notificaciones de violación de la política. Usuarios encargados de los análisis de investigación de los casos. Configuración de nivel de acceso y potestad de liberar, eliminar o retener los correos electrónicos. Medios y sistemas de notificación de violación de las políticas de fuga de información. Tipos de prueba de la funcionalidad del sistema: pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad.

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 configuración de la seguridad en redes de comunicaciones y sistemas de correo electrónico, 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 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 5

Respuesta ante eventos de ciberseguridad

Nivel: *2*
Código: *MF2798_2*
Asociado a la UC: *UC2798_2 - Responder ante eventos de ciberseguridad*
Duración (horas): *90*
Estado: *Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos para implementar eventos y alertas de seguridad, configurando los parámetros relacionados, siguiendo unas especificaciones y procedimientos para garantizar la seguridad de un sistema.

CE1.1 Describir procedimientos de parametrización de eventos de sistemas recolectados en el sistema de monitorización explicando su configuración de modo que se asegure que la información que proporciona es completa y precisa y se facilite su posterior tratamiento.

CE1.2 Interpretar reglas de tratamiento de eventos normalizados, explicando su estructura y describiendo el proceso de implementación y configuración en función de su severidad para la generación de alertas.

CE1.3 Interpretar reglas de correlación de eventos normalizados y alertas, describiendo el proceso de implementación y configuración en función de su severidad para la generación de alertas.

CE1.4 Interpretar reglas de agregación de eventos normalizados y alertas, describiendo el proceso de configuración de métricas y elementos para su agrupación.

CE1.5 Explicar los mecanismos de remediación automática o semiautomática de alertas, describiendo el proceso de implementación, de acuerdo con las condiciones de remediación.

CE1.6 En un supuesto práctico de aplicación de procedimientos para implementar eventos y alertas de seguridad, configurando los parámetros relacionados, siguiendo unas especificaciones y procedimientos para garantizar la seguridad de un sistema:

- Parametrizar eventos de sistemas recolectados en el sistema de monitorización, configurándolos de modo que se asegure que la información que proporciona es completa y precisa para facilitar su posterior tratamiento.
- Implementar unas reglas de tratamiento de los eventos normalizados, configurándolas en función de su severidad para la generación de alertas.
- Implementar unas reglas de correlación entre eventos normalizados y alertas, configurándolas en función de su severidad para la generación de alertas.
- Implementar unas reglas de agregación de eventos normalizados y alertas, configurando métricas y elementos para su agrupación.
- Implementar unos mecanismos de remediación automática o semiautomática de las alertas son implementados, de acuerdo con las condiciones de remediación.
- Confeccionar la documentación de las alertas y reglas de normalización, agregación y correlación realizados, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C2: Aplicar procedimientos frente alertas de seguridad, identificando parámetros, origen y condiciones para comunicarlo y gestionarlo y subsanar incidencias de seguridad.

CE2.1 Interpretar alertas, consultando un maestro de alertas y procedimientos para seleccionar el procedimiento operativo de seguridad.

CE2.2 Reconocer las condiciones de entorno de una alerta específica, identificando parámetros relacionados tales como direcciones IP origen y destino, puerto accedido, tipo de evento, entre otros, para aplicar procedimientos de seguridad.

CE2.3 Identificar la información resultante de una alerta que se debería escalar a una hipotética persona responsable para su gestión, tal como resultado del evento, IP origen y destino y puertos, entre otros datos, describiendo los pasos para recoger esa información.

CE2.4 Describir el proceso para cerrar una alerta, recogiendo la información relacionada, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación.

CE2.5 En un supuesto práctico de aplicación de procedimientos frente alertas de seguridad, identificando parámetros, origen y condiciones para comunicarlo y gestionarlo y subsanar incidencias de seguridad:

- Seleccionar el procedimiento operativo de seguridad a aplicar ante las alertas generadas por un sistema de monitorización se selecciona, interpretando cada alerta y consultando un maestro de alertas y procedimientos.
- Aplicar unos procedimientos de seguridad, de acuerdo con las condiciones de entorno de la alerta específica, identificando parámetros relacionados tales como direcciones IP origen y destino, puerto accedido, tipo de evento, entre otros.
- Seleccionar las alertas que deben ser comunicadas a la hipotética persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos.
- Cerrar las alertas gestionadas, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación.
- Confeccionar documentación relativa a las alertas gestionadas, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

C3: Aplicar técnicas de apoyo a la definición de procedimientos de respuesta a alertas de seguridad, recabando requisitos, condiciones de entorno y objetivos, definiéndolos y registrándolos, para preparar la respuesta ante incidencias.

CE3.1 Identificar alertas sin procedimiento asociado, explicando cómo localizarlas utilizando un maestro de alertas y procedimientos operativos, para marcarlas y documentarlas.

CE3.2 Reconocer requisitos, condiciones de entorno y objetivos de remediación para alertas, describiendo los pasos para recabarlas y documentarlas según unos modelos y plantillas.

CE3.3 Describir la configuración de procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación, indicando las acciones a realizar y prestando especial atención a la continuidad de negocio.

CE3.4 En un supuesto práctico de aplicación de técnicas de apoyo a la definición de procedimientos de respuesta a alertas de seguridad, recabando requisitos, condiciones de entorno y objetivos, definiéndolos y registrándolos, para preparar la respuesta ante incidencias:

- Marcar en una documentación las alertas sin procedimiento asociado, utilizando un maestro de alertas y procedimientos operativos e identificando aquellas alertas no recogidas en él para su uso posterior.

- Recabar requisitos, condiciones de entorno y objetivos de remediación para unas alertas, previa identificación, documentándolos según unos modelos y plantillas.
- Redactar procedimientos de seguridad ya definidos, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación, indicando las acciones a realizar y prestando especial atención a los requisitos de continuidad de negocio.
- Probar los procedimientos de seguridad se prueban, verificando su aplicación y aprobándolos y registrándolos de acuerdo con un modelo o plantilla.
- Confeccionar la documentación de los procesos realizados, siguiendo unos modelos y plantillas, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

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

C1 respecto a CE1.6; C2 respecto a CE2.5 y C3 respecto a CE3.4.

Otras Capacidades:

Aplicar las instrucciones de trabajo de manera organizada, precisa y meticulosa.
Comprender y valorar las motivaciones y consecuencias del trabajo bien realizado.
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.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Eventos y alertas de seguridad

Sistemas de monitorización. Parametrización de eventos. Reglas de tratamiento de eventos normalizados. Severidad de las alertas. Reglas de correlación de eventos normalizados y alertas. Reglas de agregación de eventos normalizados y alertas. Métricas y elementos para su agrupación. Remediación automática o semiautomática de alertas.

2 Procedimientos ante alertas de seguridad

Interpretación de las alertas. Maestro de alertas y procedimientos. Procedimientos operativos de seguridad. Condiciones de entorno de alertas específicas. Parámetros relacionados: direcciones IP origen y destino, puerto accedido, tipo de evento, entre otros. Condiciones de escalado. Cierre de alertas.

3 Apoyo a la definición de procedimientos de respuesta a alertas de seguridad

Identificación y documentación de alertas sin procedimiento asociado. Requisitos, condiciones de entorno y objetivos de remediación para alertas. Procedimientos de seguridad, elementos: alerta, condiciones de entorno, objetivos y requisitos de remediación, acciones a realizar. Garantía de la continuidad de negocio.

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 respuesta ante eventos 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 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.