Estándar de competencias profesionales

Configurar la ciberseguridad en equipos finales

Familia Profesional	**Informática y Comunicaciones**
Nivel	**2**
Código	**ECP0959_2**
Estado	**BOE**
Publicación	**RD 917/2024**

Competencia profesional

Elementos de la competencia

EC1 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.

IC1.1 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.

IC1.2 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.

IC1.3 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.

IC1.4 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.

IC1.5 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.

IC1.6 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.

IC1.7 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.

IC1.8 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad, para comprobar la funcionalidad del sistema de seguridad.

IC1.9 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.

EC2 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.

IC2.1 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.

IC2.2 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.

IC2.3 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.

IC2.4 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.

IC2.5 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.

IC2.6 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.

IC2.7 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.

EC3 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.

IC3.1 La configuración del sistema operativo se verifica para el funcionamiento del cifrado, validando los parámetros especificados según indique la documentación técnica.

IC3.2 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.

IC3.3 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.

IC3.4 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.

IC3.5 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.

IC3.6 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.

IC3.7 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

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

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.

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).