Estándar de competencias profesionales

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

Familia Profesional	**Informática y Comunicaciones**
Nivel	**2**
Código	**ECP2797_2**
Estado	**BOE**
Publicación	**RD 917/2024**

Competencia profesional

Elementos de la competencia

EC1 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.

IC1.1 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.

IC1.2 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.

IC1.3 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.

IC1.4 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.

IC1.5 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.

IC1.6 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.

EC2 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.

IC2.1 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.

IC2.2 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.

IC2.3 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.

IC2.4 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.

IC2.5 Las firmas de detección de ataques del sistema IDS/IPS se actualizan periódicamente, instalando la versión más reciente.

IC2.6 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.

IC2.7 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.

IC2.8 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.

EC3 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.

IC3.1 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.

IC3.2 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.

IC3.3 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.

IC3.4 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.

IC3.5 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.

EC4 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.

IC4.1 La configuración del sistema operativo se verifica para el funcionamiento de los SIEM, validando los parámetros especificados según indique la documentación técnica.

IC4.2 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.

IC4.3 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.

IC4.4 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.

IC4.5 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.

IC4.6 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.

IC4.7 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.

IC4.8 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.

IC4.9 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.

EC5 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.

IC5.1 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.

IC5.2 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.

IC5.3 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.

IC5.4 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.

IC5.5 La instalación se verifica, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.

IC5.6 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.

EC6 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.

IC6.1 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.

IC6.2 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").

IC6.2 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.

IC6.3 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.

IC6.4 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.

IC6.5 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.

IC6.6 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.

IC6.7 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.

EC7 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.

IC7.1 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.

IC7.2 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.

IC7.3 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.

IC7.4 La instalación se verifica, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.

IC7.5 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

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. 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).

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).