Estándar de competencias profesionales

Implementar sistemas seguros de acceso y transmisión de datos

Familia Profesional	**Informática y Comunicaciones**
Nivel	**3**
Código	**ECP0489_3**
Estado	**BOE**
Publicación	**RD 917/2024**

Competencia profesional

Elementos de la competencia

EC1 Implantar protocolos y herramientas en operaciones de intercambio de datos según las necesidades de uso, garantizando la integridad y confidencialidad de la información, así como el control de acceso, para obtener comunicaciones o canales de comunicación seguros, cumpliendo las directivas del departamento responsable de la seguridad del sistema informático.

IC1.1 La confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas se garantiza, haciendo uso de redes privadas virtuales, comunicándolos al proveedor del servicio para lograr soluciones ajustadas al plan de seguridad.

IC1.2 Las técnicas de protección de conexiones inalámbricas disponibles en el mercado se aplican, seleccionando aquellas basadas en estándares reconocidos como confiables en el sector, para cubrir vulnerabilidades, teniendo en cuenta el principio de proporcionalidad.

IC1.3 Los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones se implantan, diferenciando usuarios por perfiles y asignándoles permisos según ese perfil.

IC1.4 Los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas se protegen, usando herramientas disponibles para el cifrado extremo a extremo, para garantizar la seguridad de las comunicaciones.

IC1.5 La identidad de los servidores se garantiza en aquellos servicios que lo soportan, usando certificados digitales, configurando las aplicaciones cliente con el certificado raíz de confianza que garantice al usuario la autenticidad del servidor.

IC1.6 Las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas se documentan, incluyendo las características de las configuraciones aplicadas, ajustándolo a estándares y/o en el formato establecido en la organización.

IC1.7 Los servicios, cuyo nivel riesgo estime el departamento entidad responsable de la gestión de la seguridad del sistema informático que lo requieran, se aseguran incorporando una autenticación de doble o triple factor basada en certificados de usuario, DNI electrónico, "token", biométricos u otros mecanismos.

IC1.8 Los servicios en los que se utiliza autenticación basada en contraseñas, se configuran, estableciendo políticas de complejidad, renovación, bloqueo, almacenamiento y/o recuperaciones.

EC2 Implantar el uso de sistemas de firma y certificados de persona para asegurar la autenticidad, integridad, confidencialidad y "no repudio" de los datos que intervienen en una transferencia de información personal según las necesidades de uso y dentro de las directivas del departamento responsable de la seguridad del sistema informático.

IC2.1 El acceso a servicios a través de la red telemática se implanta de forma que asegure la autenticación mutua de cliente y servidor, utilizando autenticación de la clientela basada en certificados digitales de identidad personal cuando la política de seguridad de la organización así lo requiera.

IC2.2 El proceso de obtención y verificación de certificados digitales de identidad personal se aplica, siguiendo los pasos establecidos por la entidad certificadora y con la periodicidad indicada por el departamento responsable de la seguridad del sistema.

IC2.3 Los mecanismos para la transmisión cifrada del correo electrónico y otras comunicaciones, ya sea interpersonales o entre procesos y/o componentes, se implementan empleando certificados digitales para firmar y cifrar extremo a extremo el contenido de dichos mensajes, en los casos que indique la política de seguridad de la organización.

IC2.4 Los mecanismos de firma digital de documentos seleccionados de acuerdo con la política de seguridad del departamento responsable se aplican, incluyendo dicha firma en el momento del envío o, en su caso, al almacenar cada documento.

IC2.5 Los sistemas de sellado digital de tiempo se implantan, aplicándolos a los documentos que requiera la seguridad de la organización, para garantizar la existencia de un documento electrónico en un instante concreto, garantizando que la información contenida no ha sido alterada por terceros.

IC2.6 La integridad de los componentes en sitios web y del "software" interno se garantiza, firmándolos mediante firma digital, según el procedimiento del sistema o herramientas de firmado.

IC2.7 Los sistemas de firma digital implantados se documentan indicando su ámbito de aplicación, el procedimiento para su uso, la tipología de documentos, aplicaciones a firmar y el sistema de firma aplicado, entre otros, siguiendo estándares y de acuerdo con el formato establecido en la organización.

EC3 Implementar infraestructuras de clave pública, siguiendo instrucciones del fabricante y en función de las condiciones de uso, para garantizar la seguridad, según los estándares del sistema y dentro de las directivas de la organización.

IC3.1 La jerarquía de certificación se instala configurando la herramienta que la implementa, siguiendo las instrucciones del proveedor, en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.

IC3.2 La declaración de prácticas de certificación y la política de certificación se redacta, definiendo los procedimientos, derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.

IC3.3 El sistema de autoridad de certificación se instala, siguiendo las indicaciones del fabricante, las prácticas recomendadas del sector y la política de seguridad de la organización.

IC3.4 El certificado digital de la autoridad de certificación y su política asociada se ponen a disposición de los usuarios, siguiendo las directrices contenidas en la declaración de prácticas de certificación.

IC3.5 La clave privada de la autoridad de certificación se almacena, manteniéndola segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.

IC3.6 Los certificados digitales se emiten según los usos que van a recibir los certificados y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.

IC3.7 La validez de los certificados emitidos por la autoridad de certificación se comprueba, verificando que es mantenido por el servicio de revocación de certificados, según lo indicado en la declaración de prácticas de certificación.

IC3.8 Las infraestructuras de clave pública implantadas se documentan recogiendo sus datos de configuración, ajustándose a estándares y según el formato establecido en la organización.

EC4 Revisar el "hardware" y el diseño de la red de área local, aplicando adaptaciones para garantizar la seguridad de las comunicaciones y la protección de los datos según las directrices de la entidad responsable de la gestión de la red.

IC4.1 La topología de la red se adapta según las necesidades de seguridad, valorando su idoneidad mediante el análisis de modelos de referencia estándar, seleccionando una nueva topología y añadiendo o suprimiendo dispositivos de comunicaciones para minimizar posibles riesgos.

IC4.2 La red de la organización se segmenta de acuerdo con la compartimentación organizativa, la identidad de los equipos o usuarios y la política de seguridad de la entidad responsable, ya sea de forma física, mediante equipos tales como "routers", o de forma lógica utilizando VLAN ("Virtual Local Área Networks").

IC4.3 Las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, se establecen de acuerdo con la segmentación establecida y la política de seguridad de la organización.

IC4.4 Los mecanismos de protección para las redes de acceso, ante elementos que rompen con el perímetro tradicional de la red corporativa, tales como redes inalámbricas, dispositivos móviles y portátiles, particulares o corporativos, con conexión a las redes de la organización se establecen identificando los dispositivos empleados, delimitando su alcance y protegiendo el acceso mediante cifrado seguro, de acuerdo con la política de seguridad de la organización.

IC4.5 Los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention") se implementan mediante "hardware" o "software" al efecto, en virtud de los requisitos de seguridad de la organización, para detectar potenciales brechas en el acceso y/o transmisión de datos y prevenirlas a través del monitoreo, detección y bloqueo de información sensible.

IC4.6 El diseño de la red se modifica en su caso, introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, bien duplicando la red física, equipos y "software", bien mediante la virtualización de sistemas.

IC4.7 Los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal se configuran, asegurando una transmisión de datos confiable y segura entre los distintos nodos que la conforman.

IC4.8 Los procedimientos de salvaguarda de configuraciones se revisan modificando, en su caso, la programación de sus copias de seguridad mediante la funcionalidad habilitada en el sistema, almacenándolas en condiciones de seguridad y permitiendo una eficaz recuperación.

IC4.9 La documentación de configuración de seguridad se elabora incluyendo todos los valores de configuración implantados, ajustándolo a estándares y según el formato establecido en la organización.

EC5 Revisar el "software" de comunicaciones en red y el control de acceso de manera periódica, actualizándolo, añadiendo o suprimiendo elementos y/o modificando configuraciones, para garantizar la seguridad de las comunicaciones y la protección de los datos, según las directrices de la organización.

IC5.1 El "software" de comunicaciones que se ejecuta en los dispositivos de red se evalúa, valorando su compatibilidad, teniendo en cuenta su funcionalidad y su idoneidad para el diseño a corto y medio plazo, comprobando su integridad, legitimidad y grado de actualización para corregir problemas de seguridad.

IC5.2 Los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies" se incluyen en el diseño de la red, comparando prestaciones y características e interpretando la documentación técnica asociada.

IC5.3 Los procedimientos de salvaguarda del "software" se revisan, modificando en su caso la programación de los "backup", almacenándolos en condiciones de seguridad y permitiendo una eficaz recuperación.

IC5.4 Los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros se revisan, ajustándolos de forma que garanticen la seguridad, la trazabilidad de los parámetros y las definiciones de configuración, estableciendo protocolos para el cambio cíclico de contraseñas fijas que no caducan, estableciendo mecanismos de control de acceso del equipo de red de forma que sólo puedan ser modificados desde puntos permitidos y por administradores autorizados.

IC5.5 La configuración de seguridad en el ámbito de red se aplica garantizando el funcionamiento de puntos críticos, tales como la seguridad de puerto y configurando los mecanismos de control de tormentas de difusión, tales como el protocolo de árbol de expansión ("spanning-tree"), protocolos de redundancia ("Parallel Redundancy Protocol" -PRP-) y "Highly-available Seamless Redundancy" (HSR), entre otros.

IC5.6 La documentación del "software" de seguridad se elabora incluyendo productos, referencias y todos los valores de configuración implantados, ajustándolo a estándares y según el formato establecido en la organización.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

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

Información utilizada o generada

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