Estándar de competencias profesionales

Asegurar equipos informáticos

Familia Profesional	**Informática y Comunicaciones**
Nivel	**3**
Código	**ECP0486_3**
Estado	**BOE**
Publicación	**RD 917/2024**

Competencia profesional

Elementos de la competencia

EC1 Configurar equipos informáticos siguiendo los procedimientos establecidos en el plan de seguridad de la organización para protegerlos de la pérdida, manipulación y sustracción de información no autorizada.

IC1.1 Los tipos de usuarios se definen, estableciendo los privilegios de acceso a los recursos (aplicaciones "software", carpetas, entre otros), según las funciones desempeñadas dentro de la organización.

IC1.2 Las cuentas de usuario se crean, utilizando las herramientas específicas del sistema operativo, dándoles un nombre de usuario, una contraseña y asignándolas a los tipos de usuarios definidos en el sistema informático.

IC1.3 La política de contraseñas se configura, estableciendo parámetros tales como complejidad, caducidad, revocación, bloqueo, reutilización, entre otros.

IC1.4 El control de acceso al equipo informático se establece, configurando parámetros tales como el número de intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros.

IC1.5 La seguridad del equipo informático ante ataques externos se refuerza, configurando un cortafuegos según las necesidades de uso del equipo, estableciendo reglas de filtrado de las conexiones entrantes y salientes.

IC1.6 La seguridad de la información del equipo informático (integridad, accesos, entre otros) frente a riesgos de ataque malicioso se revisa, comprobando la instalación y configuración del "software" de protección adecuado (EDP -"EndPoint Detection and Response"-, "anti-ransomware", "anti-malware", entre otros).

IC1.7 La recopilación, tratamiento y eliminación de la información por parte de los usuarios se revisa, documentando detalladamente los protocolos a seguir según el grado de confidencialidad de la información.

IC1.8 La política de seguridad de la organización se transmite a los usuarios, publicando informaciones tales como restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos, ámbitos de responsabilidades relativos a la utilización de los equipos informáticos.

EC2 Configurar equipos servidores, aplicando los mecanismos de protección establecidos en el plan de seguridad de la organización para protegerlos de accesos indebidos.

IC2.1 Los servicios que ofrece el servidor (correo, web, servicio de impresión, entre otros) se configuran, haciendo uso de los entornos específicos de cada servicio, estableciendo valores a sus parámetros de configuración, conforme a las medidas de bastionado establecidas por la organización, si procede.

IC2.2 Los servicios del sistema operativo preinstalados no necesarios (NFS, DNS, entre otros) en el servidor se desactivan, borrándolos del sistema, garantizando así que no pueden ser activados.

IC2.3 La comunicación con el servidor (autentificación de usuarios, intercambio de información) se asegura, activando y configurando protocolos de seguridad tales como TLS (TLS, SSH, entre otros).

IC2.4 Los mecanismos de registro de actividad e incidencias del servidor se activan, configurando el registro de eventos del sistema y parametrizando valores tales como periodicidad, nivel de detalle (fecha, usuario, entre otros).

IC2.5 Los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor se activan, configurando y parametrizando, según el servicio, valores tales como tamaño de los ficheros logs, rotación, nivel de detalle (dirección IP, fecha, usuario, entre otros).

IC2.6 Las configuraciones realizadas e incidencias producidas se documentan, detallando el procedimiento llevado a cabo, las incidencias ocurridas (descripción, tipo, entre otros) y el correctivo aplicado para solventarlas, según procedimiento interno de la organización (plantillas, herramientas "software", entre otros).

EC3 Eliminar información en soportes y sistemas de almacenamiento de equipos informáticos, de forma segura, aplicando procedimientos de borrado seguro y destrucción física de información, siguiendo los procedimientos establecidos en la política de seguridad de la organización para prevenir la fuga de información confidencial.

IC3.1 Los métodos de destrucción física (trituración, desintegración, incineración, entre otros) se revisan, comprobando que el método utilizado se corresponde con el tipo de soporte de información.

IC3.2 El protocolo de retención de datos se interpreta, teniendo en cuenta la organización, búsqueda, acceso y eliminación de la información.

IC3.3 La información almacenada en los equipos informáticos y en los soportes de información se borran, utilizando herramientas "software" de borrado seguro de datos.

IC3.4 El procedimiento realizado se registra, generando un documento de certificación que detalle informaciones tales como, evidencias lógicas o gráficas del proceso, cuándo y cómo se ha realizado el proceso de destrucción o reutilización, especificaciones técnicas del "hardware", entre otras.

EC4 Aplicar medidas de seguridad física a equipos servidores, comprobando que su ubicación dispone de protección de acceso y condiciones ambientales específicas, entre otras, siguiendo el plan de seguridad de la organización para evitar interrupciones en la prestación de servicios del sistema.

IC4.1 La ubicación física de los servidores se revisa, comprobando que se encuentran situados en un espacio con acceso físico controlado y protegido.

IC4.2 Las condiciones ambientales (temperatura, humedad) de la ubicación física de equipos servidores se comprueban, verificando que se encuentran dentro del rango de trabajo óptimo considerado entre 17 y 21 grados.

IC4.3 El Sistema de Alimentación Ininterrumpida (SAI) se revisa, comprobando que está operativo a través de su sistema de alertas y reportando su estado en caso de anomalías de funcionamiento.

EC5 Verificar la realización de copias de seguridad, comprobando la información a respaldar, la frecuencia de respaldo, entre otros, para mantener la seguridad y disponibilidad de la información.

IC5.1 La información del equipo informático se comprueba, verificando que su clasificación en función de su criticidad y de su tipo (datos de sistema o datos de la organización) es acorde al plan de copias de seguridad.

IC5.2 El plan de copias de seguridad se verifica, comprobando que contempla los datos a guardar, su criticidad, tipo de salvaguarda, frecuencia de respaldo, entre otros.

IC5.3 Los dispositivos de almacenamiento de copias de seguridad (cintas, discos externos, entre otros) se comprueban, verificando que la información (fecha de la copia, información respaldada, entre otros) contenida en ellos se encuentra registrada en el plan de copias de seguridad.

IC5.4 Los procedimientos de obtención y verificación de copias de seguridad se verifican, realizando pruebas de funcionamiento de los mismos.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

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

Información utilizada o generada

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