Estándar de competencias profesionales

Administrar la infraestructura de red telemática

Familia Profesional	**Informática y Comunicaciones**
Nivel	**3**
Código	**ECP0230_3**
Estado	**BOE**
Publicación	**Orden EFD/1394/2024**

Competencia profesional

Elementos de la competencia

EC1 Configurar los equipos y dispositivos de la infraestructura de red de datos, ajustando parámetros y configurando redes virtuales -VLAN-, a partir del diseño previo para su puesta en explotación.

IC1.1 Los equipos de la infraestructura de red de datos se configuran, ajustando los parámetros y definiciones de manera individual con los valores fijados en el diseño y en el orden y modo que determina el fabricante.

IC1.2 Las subredes VLAN se configuran, aplicando el diseño previo para el aislamiento de segmentos de red.

IC1.3 La documentación de configuración se elabora, incluyendo todos los valores de configuración implantados y las definiciones topológicas implícitas en modo de esquema gráfico.

IC1.4 Las configuraciones de "software" y "hardware" se salvaguardan, realizando copia de seguridad de las mismas mediante la funcionalidad habilitada en el sistema, almacenándolas en condiciones de seguridad y de modo que permitan una eficaz recuperación.

EC2 Configurar la seguridad de los equipos y dispositivos de la infraestructura de red de datos, estableciendo entre otros los mecanismos de acceso y redundancia, a partir del diseño previo y según el plan de seguridad para su puesta en explotación.

IC2.1 La estabilidad y disponibilidad eléctrica de los componentes y/o equipos de red se garantiza, configurando los parámetros asociados, prestando especial atención a los recursos disponibles.

IC2.2 Los medios de identificación de accesos a la red y a la administración de los equipos tales como usuarios, perfiles, roles u otros se eligen, ajustándolos de forma que garanticen la seguridad y trazabilidad de los parámetros y definiciones de configuración, siguiendo los criterios establecidos en la política de seguridad, almacenándolos y utilizando para ello aplicaciones y/o procedimientos que garanticen su confidencialidad, estableciendo protocolos para el cambio cíclico de contraseñas fijas que no caducan.

IC2.3 Los dispositivos de red se configuran para incluir autenticación 8021x, definiendo un servidor Radius u otro sistema de autenticación.

IC2.4 Los equipos de la infraestructura de red de datos se configuran para su acceso por medio de aplicaciones que aíslen y garanticen la seguridad del sistema frente a accesos indebidos.

IC2.5 Los mecanismos de control de acceso del equipo de red se configuran de forma que sólo puedan ser modificados desde los puntos permitidos y por los administradores autorizados.

IC2.6 La configuración de seguridad en el ámbito de red se aplica, garantizando el funcionamiento de puntos críticos tales como la seguridad de puerto y los mecanismos de control de tormentas de difusión, tales como el protocolo de árbol de expansión ("spanning-tree").

IC2.7 Los equipos que proporcionen redundancia a la red troncal se configuran, usando la consola para asignar una IP única y para comunicarlos entre sí de forma que el secundario tome el control en caso de caída.

IC2.8 Las configuraciones de "software" y "hardware" relativas a la seguridad se salvaguardan, realizando copia de seguridad de las mismas mediante la funcionalidad habilitada en el sistema, almacenándolas en condiciones de seguridad y de modo que permitan una eficaz recuperación.

IC2.9 La documentación de configuración de seguridad se elabora, incluyendo todos los valores de configuración implantados.

EC3 Comprobar la funcionalidad de los elementos de la infraestructura de red de datos, empleando herramientas de diagnóstico y técnicas de verificación para asegurar el servicio integrado de la misma.

IC3.1 La continuidad de red extremo a extremo, la carga y las aplicaciones clientes de la infraestructura de red se prueban, verificando que se ajustan a lo planificado en la etapa de diseño.

IC3.2 La cobertura y calidad de la señal se prueba desde diferentes puntos de la zona de cobertura, teniendo en cuenta la ubicación de los puntos de acceso y las características arquitectónicas del edificio.

IC3.3 La funcionalidad se verifica, según lo planificado en la etapa de diseño, de forma que se garantice la estabilidad de la red en casos extremos.

IC3.4 El "software" de red se verifica conjuntamente con los equipos, empleando las técnicas y herramientas que se adapten a cada situación a comprobar.

IC3.5 La sincronización de todos los dispositivos se comprueba, asegurando que se encuentran bajo un único servicio NTP, para garantizar la correlación de eventos.

IC3.6 La documentación final de verificación y prueba se elabora, incluyendo las actividades realizadas y los resultados obtenidos, adjuntando esquemas, información sobre cobertura inalámbrica y rendimientos esperados/conseguidos.

EC4 Comprobar la seguridad de los elementos de la infraestructura de red de datos, asegurando el control de acceso y la redundancia entre otros, empleando herramientas de diagnóstico y técnicas de verificación.

IC4.1 Los sistemas redundantes se comprueban de manera separada ("failover"), para establecer que se garantiza la continuidad del servicio en caso de contingencia de algún dispositivo.

IC4.2 La seguridad del acceso mediante usuarios/contraseñas se comprueba en todos los dispositivos "hardware"/"software", asegurando que las contraseñas por defecto del sistema se han cambiado por otras seguras.

IC4.3 La autenticación por Radius u otro sistema se comprueba, provocando fallos para verificar su funcionamiento.

IC4.4 La documentación final de verificación y prueba de la seguridad se elabora, incluyendo las actividades realizadas y los resultados obtenidos.

EC5 Monitorizar el funcionamiento de la infraestructura de red de datos, de forma que se permita evaluar las prestaciones del sistema, estimar su rendimiento y determinar los elementos que deben ampliarse o sustituirse para evitar la degradación del rendimiento del sistema.

IC5.1 Los procesos y componentes a monitorizar se seleccionan con criterios de disponibilidad, estado de carga y seguridad, comprobando que los "firmware" se han actualizado.

IC5.2 Los umbrales de los procesos y componentes que se van a monitorizar se seleccionan de acuerdo con el nivel de servicio requerido y las especificaciones de los fabricantes.

IC5.3 Las alarmas previstas se seleccionan de forma que estén relacionadas entre sí para facilitar el análisis a los operadores.

IC5.4 Los monitores de elementos de red que configuren un servicio determinado se agrupan por tipo de dispositivo para facilitar la comprensión por los operadores de red.

IC5.5 El sistema se configura definiendo los parámetros que habiliten la generación de los eventos para la gestión de alarmas o grupos de alarmas.

IC5.6 Las alarmas relativas a nuevas actualizaciones se establecen para alertar de manera temprana sobre la necesidad de instalar la versión más reciente de los fabricantes.

IC5.7 Las alarmas y eventos se registran de forma que puedan ser analizados con posterioridad, permitiendo prever qué elementos deben ampliarse o sustituirse con el fin de que el sistema mantenga su rendimiento.

EC6 Monitorizar la seguridad de la red de datos, de forma que se lancen los avisos en caso de riesgo de acceso no autorizado y/o amenazas a la integridad, disponibilidad y confidencialidad, para poder subsanar los puntos de fallo.

IC6.1 Los puntos de fallo de alta disponibilidad (redundancia) de sistemas críticos se definen para que las alarmas avisen automáticamente en caso de contingencia grave de forma automática o semiautomática.

IC6.2 Las alarmas relativas al estado de sistemas "antimalware" y de protección se configuran, asignando valores a los parámetros de cada herramienta.

IC6.3 Las intrusiones se monitorizan, vigilando la autenticación 8021x mediante un sistema de detección automatizado.

IC6.4 Las alarmas y eventos de seguridad se registran de forma que puedan ser analizados con posterioridad, informando del estado actual de la protección ante amenazas y permitiendo prever qué elementos deben ampliarse o sustituirse con el fin de mantener la red segura.

EC7 Mantener o en su caso supervisar el mantenimiento de la red de datos, adaptando los planes preventivos establecidos a las particularidades de la instalación, partiendo de los resultados de las comprobaciones previas, diagnosticando la causa y solucionando el problema aplicando el procedimiento que especifique la entidad responsable de la red y con la periodicidad establecida en la etapa de diseño para asegurar el funcionamiento de la red.

IC7.1 Las acciones de mantenimiento se planifican, ejecutándolas de acuerdo a los procedimientos y horarios y de forma que minimicen el impacto en la producción.

IC7.2 Los problemas se diagnostican, analizando los resultados de las comprobaciones previas y localizando el punto de fallo.

IC7.3 Las copias de seguridad de los dispositivos a configurar se efectúan con anterioridad a cualquier actuación, usando los mecanismos que proporcione el fabricante o herramientas al efecto, facilitando su posterior recuperación en caso de fallo de la nueva configuración.

IC7.4 Las actualizaciones lanzadas por los fabricantes antes de su despliegue se comprueban ejecutándolas en un entorno o segmento de red aislado.

IC7.5 La acción de mantenimiento se aplica, corrigiendo los problemas diagnosticados en el punto de fallo.

IC7.6 La infraestructura de red de datos se prueba con posterioridad a cada acción de mantenimiento de forma que se verifique el funcionamiento.

IC7.7 Las acciones de mantenimiento se registran, elaborando la documentación o incluyéndola en la herramienta al efecto, siguiendo criterios que faciliten la consulta y la trazabilidad de incidencias.

EC8 Atender las incidencias, diagnosticando las causas de disfuncionalidad del sistema y adoptando medidas para el rápido restablecimiento de la operatividad del mismo.

IC8.1 La incidencia se verifica, reproduciendo el comportamiento indicado en el parte de avería, precisando el efecto de la misma y recogiendo la secuencia de eventos producidos.

IC8.2 El segmento o red afectado por incidencias de ciberseguridad se aísla, interrumpiendo su conexión al resto de la red.

IC8.3 La avería del sistema se diagnostica, previa localización, utilizando la documentación técnica de la red y los equipos, las herramientas o "software" de diagnóstico especializado y aplicando el procedimiento de forma inmediata, diferenciando las averías que pertenecen a la red local de las de la red de área extensa.

IC8.4 Los dispositivos y/o equipos sustituidos se ajustan conforme al diseño siguiendo los procedimientos recogidos en la documentación de mantenimiento, restaurando en su caso la configuración desde la copia de seguridad.

IC8.5 El sistema se prueba, asegurando la funcionalidad, los ajustes finales, la reconfiguración de los parámetros, la carga del "software" y la fiabilidad, siguiendo el procedimiento especificado en la documentación del sistema.

IC8.6 Las actualizaciones de seguridad de "hardware" y "software" se aplican como respuesta a las alarmas activas, usando las herramientas y procedimientos que facilite el fabricante, verificando la actualización en un entorno de pruebas antes de pasarlo a explotación.

IC8.7 El informe de reparación de averías o incidencias se elabora en el formato que especifique la entidad responsable de la red, recopilando ítems tales como fecha de la incidencia,

diagnóstico, medidas aplicadas entre otros, para la actualización del repositorio de incidencias.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

Equipamiento de infraestructura de comunicaciones. Cableados de cobre y fibra óptica. Herramientas de configuración "software". "Software" de diagnóstico de averías. Aplicaciones ofimáticas. Herramientas de presentación gráfica de informes. Analizadores de red. Herramientas de monitorización. Aplicaciones de gestión de incidencias/"help-desk". Aplicaciones para almacenamiento y/ o transmisión segura de información. Gestores y generadores de contraseñas. Programas para configuración remota de equipos de comunicaciones. Herramientas de monitorización de cobertura inalámbrica. Gestores de actualizaciones de los sistemas operativos y "hardware". Consolas de gestión de antivirus/"antimalware". Monitor amenazas en "firewall". Monitor de copias de seguridad de las versiones de producción de la instalación. Sistemas IDS. Servidor de autenticación Radius u otro.

Información utilizada o generada

Documentación externa de trabajo (normativa aplicable de telecomunicaciones; normativa aplicable de protección de datos, propiedad intelectual e industrial; normativa aplicable de ciberseguridad; normativa aplicable sobre prevención de riesgos laborales). Documentación interna de trabajo (plan de prevención de riesgos laborales -ergonomía, seguridad en el trabajo, agentes físicos -; plan de direccionamiento de redes; plan de implantación del sistema de comunicaciones; procedimiento interno de atención al cliente; guía de calidad; plan de mantenimiento; informes de monitorización; informes de prestaciones y propuestas de mejora; informes de seguimiento y propuestas/modificaciones de las instalaciones; procedimiento de actualización de sistemas operativos; procedimientos de actualización de las "firmware" de los dispositivos físicos; protocolos de seguimiento de alertas tempranas de ciberseguridad; histórico de modificaciones de las configuraciones; informes de alertas de intrusión detectadas; documentos de planificación y control de la ejecución de instalaciones de comunicaciones; informes de amenazas de ciberseguridad; plan de contingencia). Documentación técnica (manuales de instalación, referencia y uso de equipos de comunicaciones; información sobre redes locales y de área extensa y sistemas de comunicación públicos y privados; información sobre equipos y "software" de

comunicaciones; documentación técnica de proyectos e instalaciones de comunicaciones; publicaciones de alertas tempranas de ciberseguridad; boletines de seguridad del fabricante).