Estándar de competencias profesionales

Mantener los procesos de comunicaciones en redes locales

Familia Profesional	**Informática y Comunicaciones**
Nivel	**2**
Código	**ECP0955_2**
Estado	**BOE**
Publicación	**RD 545/2023**

Competencia profesional

Elementos de la competencia

EC1 Monitorizar la red local, para detectar y, en su caso, solucionar o reportar los fallos, asegurando su rendimiento en ausencia de congestión de tráfico de datos y el acceso a los servidores, según la tipología de red y siguiendo los procedimientos indicados por la entidad responsable de la misma, garantizando la calidad de servicio y la seguridad física y lógica.

IC1.1 La herramienta de monitorización seleccionada por el administrador de red se instala, configurando el servidor y la sonda local asociada a su misma máquina con los sensores, para garantizar la correcta supervisión de todos los dispositivos asociados a la red local, generando una plataforma de gestión unificada.

IC1.2 Las sondas de monitorización remota se instalan, configurándolas en los puntos de la red a supervisar, para que, mediante chequeos del tráfico de red, proporcionen información a la plataforma de gestión.

IC1.3 Los agentes del 'software' de red se instalan, comprobando su ejecución de forma continua en los nodos a gestionar, para que proporcionen a la plataforma de gestión la información recogida por sus respectivos sistemas operativos.

IC1.4 Los ficheros de registro de actividad ('log') de los diferentes servicios se recopilan, con objeto de analizar los procesos asociados a los mismos, manteniendo los recursos de almacenamiento y gestión en condiciones adecuadas de visibilidad, accesibilidad, integración

y escalabilidad del proceso, para explotar los datos e identificar errores y conflictos a resolver.

IC1.5 La interfaz de la herramienta de gestión de red y los filtros de selección de alarmas y alertas se configuran, optimizando los procesos de notificación y gestión de incidencias.

EC2 Mantener los dispositivos de la red local, revisándolos de manera periódica, comprobando alarmas y solucionando incidencias con el fin de garantizar los servicios de comunicaciones dentro de los parámetros recogidos en los requisitos, siguiendo procedimientos indicados por el administrador de la red y normas de calidad del servicio establecidos en el plan de mantenimiento preventivo.

IC2.1 El mapa de la red se actualiza, lanzando tareas de descubrimiento de red desde la plataforma de gestión, para disponer de una imagen real de todos los dispositivos conectados en ella, según las especificaciones recibidas por el administrador de la red.

IC2.2 La conectividad de los dispositivos de la red, tanto activos como pasivos, se comprueba con las señales acústico-luminosas observables y la aplicación de comandos de red específicos para valorar posibles deterioros o alteraciones físicas o lógicas.

IC2.3 Las causas del comportamiento anómalo de los dispositivos de la red se identifican, para proceder a su solución, aplicando la metodología de diagnóstico establecida en el plan de mantenimiento por el administrador de la red, utilizando herramientas 'hardware' y 'software' de diagnóstico para localizar la fuente de posibles errores y consultando la documentación técnica.

IC2.4 Las incidencias detectadas, localizadas mediante procesos de inspección o recibidas desde las herramientas de monitorización, se subsanan previo diagnóstico, mediante conexión remota o de manera presencial, poniendo en marcha las medidas para su solución, tales como el reseteo, actualización o reemplazo de dispositivos, de cableado u otras.

IC2.5 La seguridad y configuración de la red a las políticas y normas establecidas en la organización se verifican, realizando pruebas y utilizando las herramientas específicas de seguridad para la generación de alarmas.

IC2.6 Los resultados de las pruebas se documentan en el plan de mantenimiento del administrador de red y en el histórico de incidencias y averías, incluyendo los datos de las incidencias y las soluciones adoptadas, utilizando el modelo o aplicación informática establecidos en la entidad responsable del servicio para registrar las actividades realizadas, garantizando la trazabilidad de los procesos.

EC3 Actualizar los componentes 'hardware' y 'firmware' de los dispositivos de comunicaciones de la red local, usando los medios proporcionados por el fabricante, para adecuar su

funcionalidad a los cambios en las tecnologías según las especificaciones y procedimientos recibidos del administrador de la red, así como la documentación técnica del fabricante.

IC3.1 El 'hardware' de los equipos de comunicaciones se actualiza parcial o totalmente, usando el medio proporcionado por el fabricante, con el fin de adaptarlo a nuevas funcionalidades.

IC3.2 El 'firmware' actualmente instalado en los equipos de comunicaciones se salvaguarda, realizando una copia de seguridad de la versión instalada, a fin de poder restaurarla en caso de fallo de la actualización.

IC3.3 El 'firmware' de los equipos de comunicaciones se actualiza, accediendo al sitio 'web' del fabricante o con la opción de búsqueda de actualizaciones, si dicha opción está disponible con el sistema operativo que gestiona cada dispositivo, para adaptarlo a nuevas funcionalidades.

IC3.4 Las configuraciones de los equipos de comunicaciones se modifican, incluyendo la parametrización que especifique el administrador de la red, para cambiarles la funcionalidad o adaptarlos a los nuevos equipos introducidos.

IC3.5 Los componentes 'hardware' y 'firmware' actualizados se verifican mediante pruebas, para asegurar su funcionalidad.

IC3.6 Las actuaciones realizadas sobre los dispositivos se documentan, utilizando el modelo o aplicación informática establecido por el administrador de la red para registrar las actividades realizadas, incluyendo las referencias de los dispositivos y la versión del 'firmware' actualizado, garantizando la trazabilidad de los procesos.

EC4 Comprobar la seguridad lógica y física concerniente a los dispositivos de comunicaciones de la red local, para garantizar tanto las condiciones de integridad, disponibilidad, confidencialidad, control lógico del acceso y trazabilidad de los datos, como las del acceso físico a los servicios a usuarios autorizados, según las especificaciones y normas de seguridad recibidas del administrador de la red.

IC4.1 Las notificaciones de las alertas de seguridad recibidas por los canales de comunicación establecidos en las herramientas que las generan y elegidas por el administrador se atienden, usando las opciones de la misma herramienta, para iniciar la corrección de las incidencias notificadas.

IC4.2 Los dispositivos de comunicaciones se revisan para asegurar que su acceso físico y lógico está controlado, de acuerdo con los criterios de autenticación establecidos por el administrador de la red.

IC4.3 Los ficheros de auditoría de los dispositivos de comunicaciones se recogen, analizándolos para detectar posibles accesos indebidos que afecten a la confidencialidad y/o integridad de

los datos, siguiendo las indicaciones de los procedimientos de seguridad establecidos por el administrador de la red.

IC4.4 La trazabilidad de los datos en la red se comprueba, validando que se cumple con la normativa legal en relación al tratamiento de los mismos, mediante las herramientas específicas de rastreo determinadas por el administrador de la red.

IC4.5 Las actuaciones realizadas se documentan, utilizando el modelo o aplicación informática establecidos por el administrador del sistema, registrando las actividades realizadas, garantizando la propia trazabilidad de los sistemas y procesos de seguridad.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

Analizadores de red ('sniffers'). Certificadores de cableado. Herramientas manuales para trabajos eléctricos y mecánicos. Herramientas de diagnóstico. Herramientas 'software' para pruebas de conectividad. Herramientas 'software' de inventario de equipos de red. Ordenadores, impresoras y periféricos. Sistemas operativos. Conmutadores ('switches') y encaminadores ('routers'). Tarjetas de red. Cables y conectores. 'Software' de clientes de red. 'Software' de gestión de red. 'Software' de monitorización de red. Sondas de monitorización remota (RMON). 'Software' propietario de los dispositivos de red. Herramientas ofimáticas. Herramientas de auditoría. Mapa de la red. Herramientas de monitorización de la cobertura en redes inalámbricas. Sistemas de detección y prevención de intrusión inalámbrica (WIDS/WIPS).

Información utilizada o generada

Normativa aplicable de protección medioambiental, de planificación de la acción preventiva y de propiedad industrial. Normativa aplicable de protección de datos. Mapas de la red. Inventario 'hardware' y de configuración de la red. Partes de trabajo. Histórico de incidencias y averías. Documentación de red. Especificaciones operativas de la organización. Manual de calidad. Plan de mantenimiento. Plan de seguridad. Manuales de instalación de los dispositivos. Manuales de configuración de los dispositivos. Manual de las herramientas de monitorización.