PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

ESTÁNDAR DE COMPETENCIAS PROFESIONALES "ECP0230_3: Administrar la infraestructura de red telemática"

LEA ATENTAMENTE LAS INSTRUCCIONES

Conteste a este cuestionario de **FORMA SINCERA**. La información recogida en él tiene CARÁCTER RESERVADO, al estar protegida por lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Su resultado servirá solamente para ayudarle, **ORIENTÁNDOLE** en qué medida posee la competencia profesional del "ECP0230_3: Administrar la infraestructura de red telemática".

No se preocupe, con independencia del resultado de esta autoevaluación, Ud. TIENE DERECHO A PARTICIPAR EN EL PROCEDIMIENTO DE EVALUACIÓN, siempre que cumpla los requisitos de la convocatoria.

Nombre y apellidos del trabajador/a: NIF:	Firma:
Nombre y apellidos del asesor/a: NIF:	Firma:

INSTRUCCIONES CUMPLIMENTACIÓN DEL CUESTIONARIO:

Las actividades profesionales aparecen ordenadas en bloques desde el número 1 en adelante. Cada uno de los bloques agrupa una serie de actividades más simples (subactividades) numeradas con 1.1., 1.2.,…, en adelante.

Lea atentamente la actividad profesional con que comienza cada bloque y a continuación las subactividades que agrupa. Marque con una cruz, en los cuadrados disponibles, el indicador de autoevaluación que considere más ajustado a su grado de dominio de cada una de ellas. Dichos indicadores son los siguientes:

1. No sé hacerlo.
2. Lo puedo hacer con ayuda.
3. Lo puedo hacer sin necesitar ayuda.
4. Lo puedo hacer sin necesitar ayuda, e incluso podría formar a otro trabajador o trabajadora.

1: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1: Configurar los equipos de la infraestructura de red de datos, 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.	☐	☐	☐	☐
1.2: Configurar las subredes VLAN, aplicando el diseño previo para el aislamiento de segmentos de red.	☐	☐	☐	☐
1.3: Elaborar la documentación de configuración, incluyendo todos los valores de configuración implantados y las definiciones topológicas implícitas en modo de esquema gráfico.	☐	☐	☐	☐
1.4: Salvaguardar las configuraciones de "software" y "hardware", 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.	☐	☐	☐	☐

2: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1: Garantizar la estabilidad y disponibilidad eléctrica de los componentes y/o equipos de red, configurando los parámetros asociados, prestando especial atención a los recursos disponibles.	☐	☐	☐	☐
2.2: Elegir los medios de identificación de accesos a la red y a la administración de los equipos tales como usuarios, perfiles, roles u otros, 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.	☐	☐	☐	☐
2.3: Configurar los dispositivos de red para incluir autenticación 8021x, definiendo un servidor Radius u otro sistema de autenticación.	☐	☐	☐	☐
2.4: Configurar los equipos de la infraestructura de red de datos para su acceso por medio de aplicaciones que aíslen y garanticen la seguridad del sistema frente a accesos indebidos.	☐	☐	☐	☐
2.5: Configurar los mecanismos de control de acceso del equipo de red de forma que sólo puedan ser modificados desde los puntos permitidos y por los administradores autorizados.	☐	☐	☐	☐
2.6: Aplicar la configuración de seguridad en el ámbito de red, garantizando el funcionamiento de punto 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").	☐	☐	☐	☐
2.7: Configurar los equipos que proporcionen redundancia a la red troncal, 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.	☐	☐	☐	☐
2.8: Salvaguardar las configuraciones de "software" y "hardware" relativas a la seguridad, 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.	☐	☐	☐	☐
	☐	☐	☐	☐

2: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.9: Elaborar la documentación de configuración de seguridad, incluyendo todos los valores de configuración implantados.				

3: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1: Probar la continuidad de red extremo a extremo, la carga y las aplicaciones clientes de la infraestructura de red, verificando que se ajustan a lo planificado en la etapa de diseño.	☐	☐	☐	☐
3.2: Probar la cobertura y calidad de la señal desde diferentes puntos de la zona de cobertura, teniendo en cuenta la ubicación de los puntos de acceso y las características arquitectónicas del edificio.	☐	☐	☐	☐
3.3: Verificar la funcionalidad, según lo planificado en la etapa de diseño, de forma que se garantice la estabilidad de la red en casos extremos.	☐	☐	☐	☐
3.4: Verificar el "software" de red conjuntamente con los equipos, empleando las técnicas y herramientas que se adapten a cada situación a comprobar.	☐	☐	☐	☐
3.5: Comprobar la sincronización de todos los dispositivos, asegurando que se encuentran bajo un único servicio NTP, para garantizar la correlación de eventos.	☐	☐	☐	☐
3.6: Elaborar la documentación final de verificación y prueba, incluyendo las actividades realizadas y los resultados obtenidos, adjuntando esquemas, información sobre cobertura inalámbrica y rendimientos esperados/conseguidos.	☐	☐	☐	☐

4: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.1: Comprobar los sistemas redundantes de manera separada ("failover"), para establecer que se garantiza la continuidad del servicio en caso de contingencia de algún dispositivo.	☐	☐	☐	☐
4.2: Comprobar la seguridad del acceso mediante usuarios/contraseñas en todos los dispositivos "hardware"/"software", asegurando que las contraseñas por defecto del sistema se han cambiado por otras seguras.	☐	☐	☐	☐
4.3: Comprobar la autenticación por Radius u otro sistema, provocando fallos para verificar su funcionamiento.	☐	☐	☐	☐
4.4: Elaborar la documentación final de verificación y prueba de la seguridad, incluyendo las actividades realizadas y los resultados obtenidos.	☐	☐	☐	☐

5: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
5.1: Seleccionar los procesos y componentes a monitorizar con criterios de disponibilidad, estado de carga y seguridad, comprobando que los "firmware" se han actualizado.	☐	☐	☐	☐
5.2: Seleccionar los umbrales de los procesos y componentes que se van a monitorizar de acuerdo con el nivel de servicio requerido y las especificaciones de los fabricantes.	☐	☐	☐	☐
5.3: Seleccionar las alarmas previstas de forma que estén relacionadas entre sí para facilitar el análisis a los operadores.	☐	☐	☐	☐
5.4: Agrupar los monitores de elementos de red que configuren un servicio determinado por tipo de dispositivo para facilitar la comprensión por los operadores de red.	☐	☐	☐	☐

5: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
5.5: Configurar el sistema definiendo los parámetros que habiliten la generación de los eventos para la gestión de alarmas o grupos de alarmas.	☐	☐	☐	☐
5.6: Establecer las alarmas relativas a nuevas actualizaciones para alertar de manera temprana sobre la necesidad de instalar la versión más reciente de los fabricantes.	☐	☐	☐	☐
5.7: Registrar las alarmas y eventos 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.	☐	☐	☐	☐

6: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
6.1: Definir los puntos de fallo de alta disponibilidad (redundancia) de sistemas críticos para que las alarmas avisen automáticamente en caso de contingencia grave de forma automática o semiautomática.	☐	☐	☐	☐
6.2: Configurar las alarmas relativas al estado de sistemas antimalware y de protección, asignando valores a los parámetros de cada herramienta.	☐	☐	☐	☐
6.3: Monitorizar las intrusiones, vigilando la autenticación 8021x mediante un sistema de detección automatizado.	☐	☐	☐	☐
6.4: Registrar las alarmas y eventos de seguridad 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.	☐	☐	☐	☐

7: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
7.1: Planificar las acciones de mantenimiento, ejecutándolas de acuerdo a los procedimientos y horarios y de forma que minimicen el impacto en la producción.	☐	☐	☐	☐
7.2: Diagnosticar los problemas, analizando los resultados de las comprobaciones previas y localizando el punto de fallo.	☐	☐	☐	☐
7.3: Realizar las copias de seguridad de los dispositivos a configurar 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.	☐	☐	☐	☐
7.4: Comprobar las actualizaciones lanzadas por los fabricantes antes de su despliegue ejecutándolas en un entorno o segmento de red aislado.	☐	☐	☐	☐
7.5: Aplicar la acción de mantenimiento, corrigiendo los problemas diagnosticados en el punto de fallo.	☐	☐	☐	☐
7.6: Probar la infraestructura de red de datos con posterioridad a cada acción de mantenimiento de forma que se verifique el funcionamiento.	☐	☐	☐	☐
7.7: Registrar las acciones de mantenimiento, elaborando la documentación o incluyéndola en la herramienta al efecto, siguiendo criterios que faciliten la consulta y la trazabilidad de incidencias.	☐	☐	☐	☐

8: Atender las incidencias, diagnosticando las causas de disfuncionalidad del sistema y adoptando medidas para el rápido restablecimiento de la operatividad del mismo.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
8.1: Verificar la incidencia, reproduciendo el comportamiento indicado en el parte de avería, precisando el efecto de la misma y recogiendo la secuencia de eventos producidos.	☐	☐	☐	☐

8: Atender las incidencias, diagnosticando las causas de disfuncionalidad del sistema y adoptando medidas para el rápido restablecimiento de la operatividad del mismo.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
8.2: Aislar el segmento o red afectado por incidencias de ciberseguridad, interrumpiendo su conexión al resto de la red.	☐	☐	☐	☐
8.3: Diagnosticar la avería del sistema, 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.	☐	☐	☐	☐
8.4: Ajustar los dispositivos y/o equipos sustituidos conforme al diseño siguiendo los procedimientos recogidos en la documentación de mantenimiento, restaurando en su caso la configuración desde la copia de seguridad.	☐	☐	☐	☐
8.5: Probar el sistema, 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.	☐	☐	☐	☐
8.6: Aplicar las actualizaciones de seguridad de "hardware" y "software" 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.	☐	☐	☐	☐
8.7: Elaborar el informe de reparación de averías o incidencias 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.	☐	☐	☐	☐