## CONTENIDOS DE LA UNIDAD, CRITERIOS DE EVALUACIÓN Y RESULTADOS DE APRENDIZAJE

La siguiente tabla responde al REAL DECRETO 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo. Se incluye también una columna con las unidades didácticas que forman el curso, en las que se desarrollas los diferentes bloques de contenidos.

| CONTENIDOS | CRITERIOS DE EVALUACIÓN | RESULTADOS DE APRENDIZAJE | UNIDAD DIDÁCTICA |
|---|---|---|---|
| **Bloque 1** | | | |
| Diseño de planes de securización:<br>− Análisis de riesgos.<br>− Principios de la Economía Circular en la Industria 4.0.<br>− Plan de medidas técnicas de seguridad.<br>− Políticas de securización más habituales.<br>− Guías de buenas prácticas para la securización de sistemas y redes.<br>− Estándares de securización de sistemas y redes.<br>− Caracterización de procedimientos, instrucciones y recomendaciones.<br>− Niveles, escalados y protocolos de atención a incidencias. | a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.<br>b) Se ha evaluado las medidas de seguridad actuales.<br>c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización.<br>d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.<br>e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.<br>f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización. | 1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes. | 1, 2 |
| **Bloque 2** | | | |
| Configuración de sistemas de control de acceso y autenticación de personas:<br>− Mecanismos de autenticación. Tipos de factores. | a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.<br>b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques. | 2. Configura sistemas de control de acceso y autenticación de personas preservando la | 1, 3 |

| | | | |
|---|---|---|---|
| – Autenticación basada en distintas técnicas. | c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.<br>d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.<br>e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques. | confidencialidad y privacidad de los datos. | |
| **Bloque 3** | | | |
| Administración de credenciales de acceso a sistemas informáticos:<br>– Gestión de credenciales.<br>– Infraestucturas de Clave Pública (PKI).<br>– Acceso por medio de Firma electrónica.<br>– Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red).<br>– Gestión de cuentas privilegiadas.<br>– Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros. | a) Se han identificado los tipos de credenciales más utilizados.<br>b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.<br>c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.<br>d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.<br>e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service). | 3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos. | 4 |
| **Bloque 4** | | | |
| Diseño de redes de computadores seguras:<br>– Segmentación de redes.<br>– Subnetting.<br>– Redes virtuales (VLANs).<br>– Zona desmilitarizada (DMZ).<br>– Seguridad en redes inalámbricas (WPA2, WPA3, etc.). | a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.<br>b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).<br>c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes. | 4. Diseña redes de computadores contemplando los requisitos de seguridad. | 5, 6, 7 |

| | | | |
|---|---|---|---|
| − Protocolos de red seguros (IPSec, etc.). | d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).<br>e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas. | | |
| **Bloque 5** | | | |
| Configuración de dispositivos y sistemas informáticos:<br>− Seguridad perimetral. Firewalls de Próxima Generación.<br>− Seguridad de portales y aplicativos web. Soluciones WAF (Web Aplication Firewall).<br>− Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware.<br>− Seguridad de entornos cloud. Soluciones CASB.<br>− Seguridad del correo electrónico<br>− Soluciones DLP (Data Loss Prevention)<br>− Herramientas de almacenamiento de logs.<br>− Protección ante ataques de denegación de servicio distribuido (DDoS).<br>− Configuración segura de cortafuegos, enrutadores y proxies.<br>− Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).<br>− Monitorización de sistemas y dispositivos.<br>− Herramientas de monitorización (IDS, IPS).<br>− SIEMs (Gestores de Eventos e Información de Seguridad).<br>− Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs. | a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.<br>b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.<br>c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.<br>d) Se han implementado contramedidas frente a comportamientos no deseados en una red.<br>e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización. | 5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. | 6, 7 |

| | | | |
|---|---|---|---|
| **Bloque 6** | | | |
| Configuración de dispositivos para la instalación de sistemas informáticos:<br>− Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros.<br>− Seguridad en el arranque del sistema informático, configuración del arranque seguro.<br>− Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros. | a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.<br>b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.<br>c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.<br>d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.<br>e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad. | 6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques. | 8 |
| **Bloque 7** | | | |
| Configuración de los sistemas informáticos:<br>− Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.<br>− Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.).<br>− Eliminación de protocolos de red innecesarios (ICMP, entre otros).<br>− Securización de los sistemas de administración remota.<br>− Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).<br>− Configuración de actualizaciones y parches automáticos.<br>− Sistemas de copias de seguridad.<br>− Shadow IT y políticas de seguridad en entornos SaaS. | a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.<br>b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.<br>c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.<br>d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.<br>e) Se han instalado y configurado sistemas de copias de seguridad. | 7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques. | 9 |

Este módulo profesional contiene la formación necesaria para desempeñar la función de bastionado de los sistemas y redes de la organización.

La función de bastionado incluye aspectos como la administración de los sistemas y redes contemplando la normativa, tanto a nivel nacional como internacional, de ciberseguridad en vigor.

Las actividades profesionales asociadas a esta función se aplican en el diseño de planes de securización y en el diseño de las redes contemplando los requisitos de seguridad que apliquen a la organización.