EXTENSIÓN DE CIBERSEGURIDAD

El objetivo de esta extensión es verificar que los profesionales tienen un nivel suficiente de alfabetización en conceptos de Ciberseguridad. Esto implica que deben identificar tanto las técnicas habituales de ataque cibernético como las prácticas para proteger los dispositivos y los datos, así como conocer las medidas para proteger su información personal y privacidad en línea. En términos generales, permite verificar que:

- Conoce las amenazas existentes más habituales y los riesgos asociados a las mismas.
- Entiende cómo mantener seguros los datos, los dispositivos y el software que utiliza, con la aplicación de técnicas, controles y medidas de seguridad.
- Identifica y aplica prácticas para la protección de los datos personales, asegurando la privacidad y confidencialidad de estos.

Área competencial	Objetivos de aprendizaje
BÚSQUEDA Y GESTIÓN DE	• Identificación de fuentes confiables. Comprobar que los resultados de búsqueda y la información que se consume y comparte proviene de fuentes confiables. Verificar las citas y el contenido de artículos, blogs, publicaciones, etc. para evitar

INFORMACIÓN Y DATOS	la propagación de información falsa. Conocer la importancia de descargar archivos solo de sitios web seguros y remitentes confiables. • Reconocimiento de peligros. Reconocer las distintas técnicas de ingeniería social (Phishing, Scareware, Clickjacking o Spear phishing) utilizadas por estafadores y hackers. Revisar correos electrónicos para comprobar su veracidad. • Phishing Homógrafo. Saber comprobar que el nombre de un dominio es legítimo utilizando herramientas como Verisign, Internname, A.Tools, u otras similares, que revelan caracteres especiales utilizados en el nombre de dominio. • Ransomware. Reconocer los ataques de Ransomware, cómo prevenirlos y mitigar sus efectos. • Identificar protocolos de comunicación segura en las conexiones. Tener conocimiento sobre los fundamentos del protocolo seguro y saber distinguir entre HTTPS o HTTP. Conocer los protocolos que utiliza una red Wi-fi y el grado de seguridad que brindan. • Conocimientos sobre tecnologías de navegación segura. Conocer los beneficios del uso de una red privada virtual (VPN) y entender qué implicaciones tiene en la navegación. Saber cómo configurar manualmente la conexión a través de una red privada virtual. • Evaluar la validez de un certificado SSL. Reconocer la entidad emisora de un certificado SSL y comprobar su validez. • Conceptos sobre navegación privada y anónima. Tener conocimientos sobre el fin y funcionamiento de las Cookies, así como los trackers y/o identificadores de usuario. Saber acceder a los paneles de control de Cookies y revocar los permisos de almacenamiento. • Herramientas para navegación privada y anónima. Identificar y saber utilizar herramientas (Ghostery, uBlock Origin, Adblock Plus, etc.) que automatizan el bloqueo tanto de anuncios como rastreadores del comportamiento del usuario. • Entender las Políticas de Privacidad. Saber localizar las políticas de privacidad, entender su importancia y revisar los permisos que se solicitan. Conocer la existencia y la aplicación de las leyes que regulan las políticas de privacidad (GDPR y LOPD). • Realización de backups. Saber determinar la frecuencia apropiada, la red desde la cual realizarlos y el lugar de almacenamiento seguro en función del tipo de información (privada o pública).

	• Verificar la integridad de archivos. Entender el concepto de hashing, conocer la existencia de algoritmos de hash criptográficos como SHA256 o MD5. Identificar y usar herramientas para el cálculo del hash (HashMyFiles, QuickHash, Itoolkit, etc.). • Analizar archivos o URLs. Saber cómo utilizar herramientas de verificación (como VirusTotal) para subir un archivo sospechoso o una URL, interpretar los resultados y tomar decisiones informadas sobre la seguridad de los elementos analizados. • Control de permisos sobre documentos y directorios (local & cloud). Saber gestionar quién tiene acceso a documentos y carpetas tanto en sistemas locales como en la nube.
COMUNICACIÓN Y COLABORACIÓN	• Contraseñas robustas. Conocer las buenas prácticas para la creación y gestión de contraseñas. • Información sensible. Identificar cuáles son datos sensibles y entender la importancia de utilizar medios y canales seguros para compartirlos. Conocer la gestión de datos sensibles en cumplimiento con normativas como GDPR, HIPAA u otras leyes de protección de datos. • Certificados y firmas digitales. Saber lo que es y para qué sirve un certificado digital y ser capaz de utilizarlo. Verificar que los documentos importantes recibidos o enviados estén firmados digitalmente para garantizar su autenticidad y no repudio. • Identidad digital. Disponer de conocimiento sobre la importancia de la protección y gestión de la identidad digital. Saber gestionar la identidad digital en diferentes plataformas, webs y redes sociales. Configurar adecuadamente perfiles personales y profesionales, manteniéndolos separados. • Mantener la privacidad. Evaluar los permisos solicitados por aplicaciones y servicios online para evitar el acceso innecesario a datos personales (revisar, limitar y revocar los permisos). • Certificado personal. Conocer cómo solicitarlo, instalarlo y utilizarlo en el navegador. Saber cómo acceder y utilizar servicios públicos digitales que requieran el certificado personal digital. • Firma de documentos digitales. Firmar documentos con firma digital utilizando aplicaciones como por ejemplo Microsoft Acrobat o herramientas como Idazki de Izenpe. • Seguridad en pagos. Ser consciente de los posibles riesgos que puede implicar el uso de tecnologías como NFC si no se toman las medidas de seguridad apropiadas.

	• Herramientas seguras de colaboración. Identificar herramientas seguras para la compartición de información y desarrollo colaborativo. Controlar los accesos y monitorizar la actividad compartida.

CREACIÓN DE CONTENIDOS DIGITALES	• Revisar las referencias incluidas en contenidos. Conocer la importancia que tiene comprobar la veracidad de las referencias utilizadas, si provienen de fuentes fiables, y la seguridad de los enlaces incluidos (accesos a sitios seguros).
	• Proteger los datos mediante contraseñas. Identificar la información sensible e incluir contraseñas robustas y únicas para el acceso a cada una de las plataformas de compartición de contenido digital.
	• Gestión de permisos. Hay que asegurar que los contenidos estén protegidos y sólo las personas autorizadas puedan acceder a ellos. Saber crear roles y asignar permisos en las distintas plataformas de colaboración en la nube (Google Drive, Dropbox, OneDrive, etc.).
	• Uso de Redes Seguras. Conocer la importancia de la utilización de una red segura al subir contenido a una web o plataforma.
	• En Programación, conocer la utilización de prácticas seguras:
	  ○ Validación de Entradas. Validar los datos de entrada a la aplicación para evitar inyecciones de código y otros ataques.
	  ○ Control de Acceso. Implementar el control de acceso adecuado, para evitar usuarios no autorizados.
	  ○ Gestión de Errores. Incluir gestión de errores en el código y manejar los errores de manera segura sin revelar información sensible sobre el sistema.
	  ○ Uso de Librerías Seguras. Mantenerlas actualizadas para evitar vulnerabilidades.
	  ○ Revisión y Validación. Realizar revisiones de código estático para identificar y corregir posibles vulnerabilidades.
	• Cifrado de Datos compartidos. Al crear contenido como, por ejemplo, infografías y presentaciones, saber utilizar software que permita la encriptación y protección con contraseña como Canva o Microsoft PowerPoint.

SEGURIDAD	• Actualización de software. Conocer la importancia de instalar actualizaciones y parches de seguridad regularmente de cara a evitar las posibles vulnerabilidades. • Autenticación y gestión de contraseñas. Utilizar el doble factor de autenticación (2FA) y herramientas como Authenticator, para añadir una capa extra de seguridad cuando sea necesario. Conocer la identificación biométrica, uso de llaves, ficheros clave, etc. Utilizar gestores de contraseñas (LastPass, 1Password, Keepass, etc.) para almacenar las contraseñas de forma segura.

	• Uso correcto del antivirus y anti-malware. Comprender la necesidad de disponer de software de seguridad en los dispositivos que ayude a detectar y bloquear amenazas antes de que puedan causar daño. • Tratamiento de la información sensible. Conocer la importancia sobre el cifrado de los datos sensibles tanto en tránsito como en reposo. Comprobar que los archivos multimedia compartidos no contengan metadatos sensibles. • Uso de herramientas de cifrado. Conocer los fundamentos de cifrado y cómo aplicar el cifrado para proteger documentos, datos sensibles y unidades de almacenamiento, utilizando herramientas como BitLocker, FileVault o similares. • Cifrado en comunicaciones. Implementar el cifrado en correos electrónicos y mensajería con herramientas como ProtonMail, Signal, Microsoft Outlook o similares. • Correos electrónicos y enlaces sospechosos. Detectar técnicas comunes para robar información personal (phishing), analizar los contenidos y tomar decisiones de actuación ante sospechas de fraude.
RESOLUCIÓN DE PROBLEMAS	• Técnicas de ciberataque. Conocer los conceptos relacionados con los principales ciberataques como pueden ser: ataques de denegación de servicio (DDoS), Man in the Middle (MitM), Phishing, Malware, Ransomware, ataques de ingeniería social, hacking de contraseñas, ataques de inyección SQL, ataques de fuerza bruta, etc. • Identificación de amenazas. Saber detectar señales que pueden sugerir un posible ataque o amenaza. Saber revisar y analizar el consumo de recursos (RAM y CPU) de las aplicaciones para detectar consumos anómalos. • Medidas de seguridad habilitadas. Conocer la importancia de mantener las medidas de seguridad y escaneos habilitados a pesar de tener problemas en el equipo. • Fiabilidad del software de rescate. Importancia de asegurar que el software de rescate (utilizado para poder reiniciar el equipo y solucionar los fallos) no está comprometido y está libre de malware. • Evaluación de soluciones. Actuación ante un posible problema de ciberseguridad. Saber tomar las acciones adecuadas para evitar el riesgo de propagación. • Optimización avanzada y automatización de entornos digitales. Disponer de información actualizada con las últimas tendencias, herramientas y tecnologías en ciberseguridad (incluyendo, por ejemplo, inteligencia artificial y machine learning).

	• Validación de herramientas de ciberseguridad. Conocer la importancia de investigar y comparar diferentes herramientas disponibles en el mercado ajustadas a las necesidades tecnológicas del usuario. Realizar pruebas piloto para validar la efectividad de las herramientas seleccionadas antes de su implementación completa. • Configuración personalizada. Ajustar las configuraciones de seguridad de los dispositivos, herramientas y aplicaciones para satisfacer las necesidades específicas de la organización y del propio usuario.