SEGURIDAD EN DISPOSITIVOS ELECTRÓNICOS

CÓDIGO	AUTOR/A	DURACIÓN ESTIMADA	NIVEL DE FORMACIÓN
07B04C01	Marcos Garasa	80 h	Medio/Avanzado

Dirigido a

Profesionales de cualquier sector que quieran mejorar sus habilidades y capacitación digital.

Descripción

Con este contenido de formación basado en el Marco Europeo de Competencias Digitales (DigComp 2.2), el alumnado aprenderá aspectos relacionados con la seguridad de dispositivos y protección de datos en el ámbito digital.

COMPETENCIAS

1. Conocer las amenazas del entorno digital para evitar riesgos.
2. Conocer las diferentes ciberamenazas para poder actuar ante ellas.
3. Aprender medidas y protección de seguridad para mis dispositivos.
4. Conocer los diferentes riesgos informáticos que pueden surgir del teletrabajo para poder evitarlos.
5. Aprender a configurar sistemas de seguridad para nuestros equipos informáticos.
6. Conocer el marco normativo en el uso de los datos personales para un correcto uso el entorno digital.
7. Aprender a compartir los datos personales de forma segura en el entorno digital para evitar riesgos.
8. Establecer medidas de privacidad propia y ajena para el intercambio de datos.
9. Aprender sistemas de navegación privada y comunicación encriptada para un intercambio de datos más seguro.
10. Conocer el mantenimiento de la cadena de custodia y veracidad de la información para una navegación segura en el entorno digital.
11. Conocer los riesgos para la salud que pueden suponer el uso en exceso de las Nuevas tecnologías de la información para evitarlos en nuestro día a día.

12. Conocer el impacto ambiental que pueden suponer el uso de las tecnologías digitales para así poder establecer medidas de ahorro y eficiencia en el uso de los dispositivos.

CRITERIOS DE EVALUACIÓN (Objetivos)

1. Concienciar de las distintas tipologías de amenazas en los contextos digitales.
2. Empoderar al alumnado para responsabilizarse de la autoprotección.
3. Extender la seguridad a los dispositivos personales.
4. Desarrollar decálogos y hábitos saludables en las interacciones.
5. Configurar servicios de seguridad y control de acceso a equipos.
6. Aprender los derechos y deberes en el uso de datos personales.
7. Compartir de forma segura datos personales.
8. Implantar medidas de privacidad de datos.
9. Implantar sistemas de navegación privados.
10. Identificar posibles brechas en la trazabilidad y autenticidad de la información/datos que se manejan.
11. Concienciar de los perjuicios físicos y mentales derivados del uso laboral de las nuevas tecnologías. Descubrir las enfermedades profesionales derivadas del puesto de trabajo. Concienciar de la necesidad de la focalización y reducción del estrés.
12. Concienciar del impacto medioambiental de las tecnologías. Empoderar al alumnado como parte integrante del cambio y mejoras. Entender parte de la función pública como embajadores de la sostenibilidad medioambiental y energética.

CONTENIDOS

Unidad 1. Desmontando el área de seguridad

1. Desmontando el área de seguridad
   1.1 Conocimiento , habilidades y actitudes
   1.2 Conocimiento previos
   1.3 Ejemplo de uso

Unidad 2. Asegura tus dispositivos

1. Asegura tus dispositivos
   1.1 Introducción a la ciberseguridad
   1.2 Conceptos clave
   1.3 Tipología de ciberamenazas: malware, phishing, ransomware, etc.
   1.4 Actuación ante peligros y amenazas

Unidad 3. Asegura tus dispositivos II

0. Conceptos previos
1. Medidas de protección y seguridad de mis dispositivos
   1.1 Protección contra el malware
   1.2 Protección de accesos
   1.3 Protección ante ingeniería social y técnicas con malware
   1.4 Cómo actuar si sospechas que ya has sido víctima

Unidad 4. Riesgos informáticos derivados del teletrabajo

1. Conceptos previos
2. Dispositivos corporativos en el contexto doméstico
3. Recomendaciones

Unidad 5. Riesgos informáticos derivados del teletrabajo II

1. Riesgos informáticos derivados del teletrabajo II
   1.1 VPN y configuración de servicios de seguridad
2. Dispositivos en teletrabajo
3. Control de acceso a equipos informáticos
4. Recomendaciones
   4.1 Contraseñas
   4.2 Implementación de Doble Factor de Autenticación.
   4.3 Control de dispositivos
   4.4 Gestión de permisos y roles

Unidad 6. Derechos y deberes en el uso de datos personales

1. Derechos y deberes en el uso personal
   1.1 Antecedentes
   1.2 Ley Orgánica de Protección de Datos (LOPD)
2. Normativas de aplicación
   2.1. El Reglamento General de Protección de Datos
   2.2 La Agencia Española de Protección de Datos
3. El Reglamento general de protección de datos
4. Derechos y deberes.

Unidad 7. Compartición segura de datos personales

1. Compartición segura de datos personales
   1.1 La huella digital
2. Responsabilidad individual
3. ¿Qué puedo hacer para protegerme?
   3.1 Utilizar un software de seguridad
   3.2 Examinar antes de hacer clic en los enlaces
   3.3 No compartir información personal sensible
   3.4 Utilizar una conexión segura
   3.5 Sitios web no seguros
4. Sencillas mejoras en la seguridad
5. Educación y concienciación
   5.1 Ejemplos de programas o recursos

Unidad 8. Cuidado de la privacidad propia y ajena

1. Compartición segura de datos personales propios y ajenos
2. ¿Qué es la compartición segura de datos?
   2.1 Los términos de servicio y las políticas de privacidad
   2.2 Compartir información personal sensible
3. La privacidad de las cuentas en las redes sociales
   3.1 Configurar las opciones de privacidad
   3.2 Poner en valor nuestra privacidad
4. Usar aplicaciones y programas de seguridad en dispositivos móviles y ordenadores
5. Los correos electrónicos y mensajes de texto sospechoso
6. Respetar la privacidad de los demás
   6.1 El consentimiento
   6.2 Evaluar si realmente se necesita compartir información personal
7. Las últimas tendencias en seguridad y privacidad

Unidad 9. Sistema de navegación privada y comunicación encriptada

1. Conceptos y elementos de privacidad y seguridad en línea
   1.1 Navegar sin dejar rastro
2. Herramientas de acceso a la información
   2.1 Dirección IP
   2.2 Buscadores
   2.3 Navegadores
3. Sistemas de navegación privada
   3.1 Introducción a los sistemas de navegación privada
   3.2 Cómo funcionan
   3.3 Cómo configurarlos y utilizarlos
4. Herramientas de encriptación
   4.1 Introducción a las herramientas de encriptación
   4.2 Cómo funcionan
   4.3 Qué ventajas ofrecen
   4.4 Cómo configurarlas y utilizarlas
5. Seguridad en el navegador
   5.1 Cómo proteger la privacidad y seguridad en el navegador
6. Comunicaciones seguras
   6.1 Cómo proteger la privacidad y seguridad
   6.2 Otras posibilidades de fácil acceso
7. Retirar información personal de Internet
   7.1 La privacidad en línea y la retirada de información personal
   7.2 Regulaciones actuales sobre la retirada de información personal

Unidad 10. Mantenimiento de la cadena de custodia y veracidad de la información

1. Conceptos clave
2. Control de acceso y registro de cambios
   2.1 Garantizar el control de acceso a los datos y registro
   2.2 Las modificaciones realizadas en un proceso
3. Las técnicas y procedimientos para garantizar la integridad de los datos
   3.1 Técnicas y procedimientos para garantizar la integridad de los datos
   3.2 Registros y las copias de seguridad
4. ¿Qué es la cadena de custodia?
   4.1 ¿Cuál es el procedimiento para mantener la Cadena de custodia?
   4.2 Los requisitos específicos
5. Auditorías y documentación

5.1 Cómo llevar a cabo una auditoría para verificar la integridad de los datos y registros
5.2 Introducción sobre la documentación necesaria para mantener la cadena de custodia
6. Tecnologías y herramientas para garantizar la cadena de custodia y veracidad de la información
7. Ejemplos de buenas prácticas en la cadena de custodia en la industria

Unidad 11. Identificación y actuación ante los riesgos para la salud

1. Identificación y actuación ante los riesgos para la salud
   1.1 Riesgos físicos
   1.2 Riesgos psicológicos
   1.3 Riesgos externos
2. Ergonomía en el puesto de trabajo y con dispositivos móviles
   2.1 Puesto de trabajo
   2.2 Dispositivos móviles
3. Medidas para la desconexión digital
4. La inclusión digital
5. Adicciones y trastornos psicológicos ante la exposición prolongada con RRSS, herramientas digitales y comunicaciones 2.0
   5.1 Adicción a los dispositivos
   5.2 Adicción a las tecnologías

Unidad 12. Reglas y configuraciones para el ahorro de energía en dispositivos móviles

1. Reglas y configuraciones para el ahorro de energía en dispositivos móviles
2. Cómo alargar la vida de los dispositivos
3. Clasificación de los dispositivos según su impacto ambiental
4. Protocolos de reciclaje de dispositivos eléctricos y electrónicos
5. Sistemas colectivos de Responsabilidad Ampliada del Productor
   5.1 Cadena de reciclaje
   5.2 Puntos de entrega de los Residuos electrónicos y eléctricos