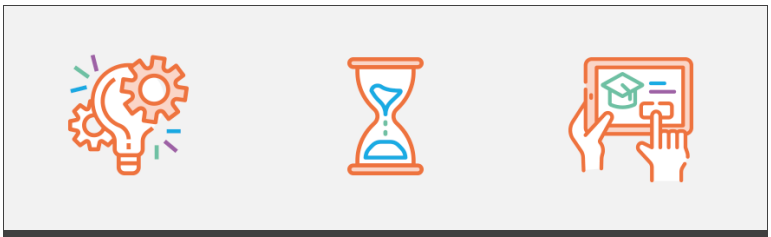
Seguridad en dispositivos electrónicos



Área: INFORMÁTICA
Duración: 80h
Metodología: online

Objetivos

Concienciar de las distintas tipologías de amenazas en los contextos digitales.
Empoderar al alumnado para responsabilizarse de la autoprotección.
Extender la seguridad a los dispositivos personales.
Desarrollar decálogos y hábitos saludables en las interacciones.
Configurar servicios de seguridad y control de acceso a equipos.
Aprender los derechos y deberes en el uso de datos personales.
Compartir de forma segura datos personales.
Implantar medidas de privacidad de datos.
Implantar sistemas de navegación privados.
Identificar posibles brechas en la trazabilidad y autenticidad de la información/datos que se manejan.
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.
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 y estructura del curso

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

2. 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

3. Conceptos previos

4. 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

5. Conceptos previos

6. Dispositivos corporativos en el contexto doméstico

7. Recomendaciones

8. Riesgos informáticos derivados del teletrabajo II
    1.1 VPN y configuración de servicios de seguridad

9. Dispositivos en teletrabajo

10. Control de acceso a equipos informáticos

11. Recomendaciones
    4.1 Contraseñas
    4.2 Implementación de Doble Factor de Autenticación.
    4.3 Control de dispositivos
    4.4 Gestión de permisos y roles

12. Derechos y deberes en el uso personal
    1.1 Antecedentes
    1.2 Ley Orgánica de Protección de Datos (LOPD)

13. Normativas de aplicación
    2.1. El Reglamento General de Protección de Datos
    2.2 La Agencia Española de Protección de Datos

14. El Reglamento general de protección de datos

15. Derechos y deberes.

16. Compartición segura de datos personales
    1.1 La huella digital

17. Responsabilidad individual

18. ¿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

19. Sencillas mejoras en la seguridad

20. Educación y concienciación
    5.1 Ejemplos de programas o recursos

21. Compartición segura de datos personales propios y ajenos

22. ¿Qué es la compartición segura de datos?
    2.1 Los términos de servicio y las políticas de privacidad
    2.2 Compartir información personal sensible

23. La privacidad de las cuentas en las redes sociales
    3.1 Configurar las opciones de privacidad
    3.2 Poner en valor nuestra privacidad

24. Usar aplicaciones y programas de seguridad en dispositivos móviles y ordenadores

25. Los correos electrónicos y mensajes de texto sospechoso

26. Respetar la privacidad de los demás
    6.1 El consentimiento
    6.2 Evaluar si realmente se necesita compartir información personal

27. Las últimas tendencias en seguridad y privacidad

28. Conceptos y elementos de privacidad y seguridad en línea
    1.1 Navegar sin dejar rastro

29. Herramientas de acceso a la información
    2.1 Dirección IP
    2.2 Buscadores
    2.3 Navegadores

30. Sistemas de navegación privada
    3.1 Introducción a los sistemas de navegación privada

3.2 Cómo funcionan
3.3 Cómo configurarlos y utilizarlos

31. 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

32. Seguridad en el navegador
    5.1 Cómo proteger la privacidad y seguridad en el navegador

33. Comunicaciones seguras
    6.1 Cómo proteger la privacidad y seguridad
    6.2 Otras posibilidades de fácil acceso

34. 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

35. Conceptos clave

36. 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

37. 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

38. ¿Qué es la cadena de custodia?
    4.1 ¿Cuál es el procedimiento para mantener la Cadena de custodia?
    4.2 Los requisitos específicos

39. 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

40. Tecnologías y herramientas para garantizar la cadena de custodia y veracidad de la información

41. Ejemplos de buenas prácticas en la cadena de custodia en la industria

42. Identificación y actuación ante los riesgos para la salud
    1.1 Riesgos físicos
    1.2 Riesgos psicológicos
    1.3 Riesgos externos

43. Ergonomía en el puesto de trabajo y con dispositivos móviles
    2.1 Puesto de trabajo
    2.2 Dispositivos móviles

44. Medidas para la desconexión digital

45. La inclusión digital

46. 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

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

48. Cómo alargar la vida de los dispositivos

49. Clasificación de los dispositivos según su impacto ambiental

50. Protocolos de reciclaje de dispositivos eléctricos y electrónicos

51. Sistemas colectivos de Responsabilidad Ampliada del Productor
    5.1 Cadena de reciclaje
    5.2 Puntos de entrega de los Residuos electrónicos y eléctricos

Metodología

En Criteria creemos que para que la formación e-Learning sea realmente exitosa, tiene que estar basada en contenidos 100% multimedia (imágenes, sonidos, vídeos, etc.) diseñados con criterio pedagógico y soportados en una plataforma que ofrezca recursos de comunicación como chats, foros y conferencias...Esto se logra gracias al trabajo coordinado de nuestro equipo e-Learning integrado por profesionales en pedagogía, diseño multimedia y docentes con mucha experiencia en las diferentes áreas temáticas de nuestro catálogo.

Perfil persona formadora

Esta acción formativa será impartida por un/a experto/a en el área homologado/a por Criteria, en cumplimiento con los procedimientos de calidad, con experiencia y formación pedagógica.

En Criteria queremos estar bien cerca de ti, ayúdanos a hacerlo posible:
¡Suscríbete a nuestro blog y síguenos en redes sociales!

Blog de Criteria