Plan de
Formacion y Concienciacion

Daniel Otero Vázquez
Javier Magán Jorge

Índice

1. Introdución

O uso de Internet, redes sociais e ferramentas dixitais é habitual entre estudantes e persoal do centro, pero tamén conleva riscos para a privacidade, seguridade e responsabilidade profesional. Este plan ten como obxectivo **concienciar e formar** a todos os actores do instituto, garantindo un uso seguro, responsable e ético das tecnoloxías dixitais e da Intelixencia Artificial (IA).

---

2. Segmentación do centro e necesidades

Rol		Necesidades de formación e sensibilización
Alumnado ESO / Bacharelato		Hábitos básicos
Alumnado Ciclos	Informáticos	Seguridad técnica avanzada
	Non Informáticos	Boas prácticas dixitais
Persoal Docente		Protección de datos, uso seguro de plataformas
Persoal Non Docente		Seguridade administrativa, protección de datos

---

3. Alumnado ESO / Bacharelato

Módulos: Identidade dixital; Comunicación segura; Ciberacoso; Contrasinais; Redes sociais; Intelixencia Artificial

0. Introdución

O uso de Internet e das redes sociais é habitual entre adolescentes, pero tamén conleva riscos para a privacidade e a seguridade. Aprender a navegar de forma segura e responsable é esencial.

1. Identidade dixital

Información que compartimos en liña (fotos, comentarios, gustos…). Coidala significa pensar antes de publicar, protexer a privacidade e manter unha boa reputación.

Recomendacións:

- Comparte só a información necesaria.
- Configura a privacidade nas redes sociais.
- Evita publicar datos persoais sensibles.
- Revisa e elimina o que non queiras manter en liña.

2. Contrasinais fortes

Primeira barreira de protección.

Boas prácticas:

- Combinar letras, números e símbolos.
- Cambiar periodicamente e non compartir.
- Activar verificación en dous pasos cando sexa posible.

3. Comunicación segura

Detráis de cada pantalla hai persoas; a comunicación debe ser respectuosa.

Consellos:

- Non responder a mensaxes sospeitosas.
- Non compartir contido íntimo ou persoal.
- Informar a adultos ou profesores se hai mensaxes ameazantes.

4. Ciberacoso

Acoso a través de medios dixitais.

Lembra que detráis de cada mensaxe hai persoas; o acoso dixital afecta directamente a outras persoas.

Como actuar:

- Non participar nin responder.
- Gardar probas.
- Bloquear ao agresor.
- Informar a un adulto ou autoridade.

5. Redes sociais

Permiten comunicarse e aprender, pero poden supoñer riscos.

Recomendacións:

- Configura a privacidade.
- Non aceptar descoñecidos.
- Pensar antes de publicar ou compartir localización.
- Denunciar contido inapropiado.

6. Intelixencia Artificial (IA)

Ferramentas de IA poden apoiar os estudos ou crear contido, pero hai riscos de desinformación, plaxio ou exposición a contido inadecuado.

Recomendacións:

- Non compartir datos persoais con IA sen autorización.
- Verificar sempre a información xerada.
- Non copiar textos da IA como propios.
- Usar a IA como apoio, non como substituto do pensamento crítico.

7. Formación

- **Formación teórica:** Sesións expositivas sobre todos os módulos.
- **Formación práctica:** Talleres de creación de contrasinais, simulacións de phishing, configuración de privacidade en redes sociais, actividades de uso responsable de IA.
- **Metodoloxía:** 6 sesións de 45 min; combinación de teoría, talleres e debates.
- **Seguimento / Avaliación:** Cuestionarios en liña, exercicios prácticos, reflexión escrita ou debate final sobre aplicación dos coñecementos.

---

4. Alumnado Ciclos

A. Perfil Informático

Módulos: Redes Seguras; Criptografía; Vulnerabilidades; Intelixencia Artificial

0. Introdución

Os estudantes destes ciclos xa coñecen medidas básicas de seguridade; nesta etapa aprenderán a deseñar e xestionar sistemas seguros e a usar IA de forma responsable.

1. Redes Seguras

Garantir confidencialidade, integridade e dispoñibilidade da información.

Boas prácticas:

- Segmentar redes e controlar accesos.
- Usar cifrado e VPN.
- Actualizar software e revisar configuracións.

2. Criptografía

Protexe a información mediante técnicas matemáticas.

Aplicacións: sinaturas dixitais, certificados, protocolos seguros.

Recomendacións:

- Usar cifrado adecuado segundo a sensibilidade da información.
- Xestionar e almacenar claves de forma segura.

3. Vulnerabilidades

Debilidades que poden ser explotadas por atacantes.

Como actuar:

- Identificar e avaliar vulnerabilidades.

- Corrixir ou mitigar riscos e documentar os cambios.
- Realizar probas de penetración para comprobar seguridade.

4. Intelixencia Artificial (IA)

A IA pode optimizar sistemas, automatizar detección de ataques ou analizar datos, pero tamén se pode usar para phishing, deepfakes ou ataques automatizados.

Boas prácticas:

- Avaliar algoritmos antes de aplicalos.
- Non depender da IA para decisións críticas sen supervisión.
- Revisar datos e resultados para evitar erros ou sesgos.

5. Formación

Formación

- **Teórica:** Sesións expositivas sobre redes, criptografía, vulnerabilidades e IA.
- **Práctica:** Laboratorios de redes, implementación de cifrado, auditorías simuladas, avaliación de algoritmos de IA.

Metodoloxía: 8 sesións de 90 min; teoría e laboratorio.

Seguimento / Avaliación: Proxectos prácticos, informes de laboratorio e autoavaliación.

B. Perfil Non Informático

Módulos: Uso seguro de dispositivos e datos; Intelixencia Artificial

0. Introdución

No contorno profesional é imprescindible protexer a información, garantir a confidencialidade e utilizar ferramentas dixitais con rigor.

1. Seguridade básica en dispositivos e contas

Boas prácticas esenciais para o uso profesional de equipos e servizos en liña:

- Manter sistemas e aplicacións actualizados.
- Usar contrasinais fortes, bloqueos de pantalla e autenticación en dous pasos.
- Evitar Wi-Fi públicas e dispositivos externos non controlados.
- Realizar copias de seguridade periódicas de traballos e documentación.

2. Protección de datos e responsabilidade profesional

Conceptos fundamentais de privacidade aplicados ao ámbito empresarial:

- Tratar só datos necesarios para o servizo ou tarefa.
- Garantir confidencialidade, integridade e seguridade na súa xestión.
- Eliminar ou anonimizar datos cando xa non sexan precisos.
- Informar de maneira transparente sobre o uso dos datos cando proceda.
- Comprender obrigas legais básicas (LOPDGDD, RGPD a nivel introdución).

3. Comunicación dixital segura no ámbito laboral

Boas practicas:

- Verificar remitentes e evitar abrir ligazóns ou arquivos sospeitosos.
- Non compartir contrasinais ou información sensible por mensaxes non seguras.
- Protexer a privacidade das ferramentas colaborativas (Drive, Teams, etc.).
- Manexar con prudencia redes sociais ou mensaxería cando se represente á empresa.

4. Intelixencia Artificial aplicada ao traballo

Ferramentas de IA poden axudar a xestionar citas ou crear contido, pero hai riscos sobre privacidade e fiabilidade.

Consellos:

- Non introducir información sensible de clientes, datos persoais ou documentación interna en plataformas de IA abertas.
- Validar sempre as respostas; a IA pode xerar erro, sesgo ou contido inventado.

- Empregar a IA como apoio para mellorar produtividade, non para substituír o criterio profesional nin as obrigas éticas.

5. Formación

Formación

- **Teórica:** Sesións expositivas sobre todos os módulos.
- **Práctica:** Casos de estudo, simulación de incidentes, exercicios de uso seguro de dispositivos e IA.

Metodoloxía: 5 sesións de 60 min; combinación de teoría e práctica.

Seguimento / Avaliación: Cuestionarios, exercicios prácticos e reflexión sobre boas prácticas.

---

6. Persoal Docente

Módulos: Protección de datos; Plataformas educativas; Intelixencia Artificial

0. Introdución

O profesorado usa ferramentas dixitais e ten responsabilidade na protección de datos e no uso seguro das plataformas e da IA.

1. Protección de datos

Boas prácticas:

- Confidencialidade, finalidade, minimización, seguridade e transparencia.
- Evitar compartir datos persoais en espazos públicos.
- Bloquear pantallas e eliminar documentos correctamente.

2. Uso seguro de plataformas

Boas prácticas:

- Acceder desde dispositivos e redes seguras.
- Non compartir contrasinais.
- Revisar configuracións e usar comunicación oficial.

3. Comunicación e privacidade

Boas prácticas:

- Manter trato profesional.
- Non publicar imaxes do alumnado sen autorización.
- Supervisar espazos colaborativos.

4. Intelixencia Artificial (IA)

A IA pode apoiar docencia, xeración de contido e planificación, pero hai riscos de plaxio, privacidade e sesgos.

Boas prácticas:

- Non compartir datos do alumnado con ferramentas externas.
- Comprobar fiabilidade do contido xerado.
- Usar IA como apoio, non substituto do traballo pedagóxico.

5. Formación

Formación

- **Teórica:** Sesións expositivas sobre protección de datos, plataformas educativas e ética no uso de IA.
- **Práctica:** Talleres de configuración segura, manexo de contido do alumnado, creación de contido dixital ético.

Metodoloxía: 4 sesións de 2 h; presencial e en liña.

Seguimento / Avaliación: Test, exercicios prácticos e elaboración de plans de uso seguro de IA.

7. Persoal Non Docente

Módulos: Xestión segura de datos administrativos; Intelixencia Artificial

0. Introdución

O persoal non docente manexa información persoal e administrativa; a súa xestión segura garante privacidade e cumprimento normativo.

1. Datos administrativos

- Inclúen información de alumnado, profesorado, familias e persoal.
- Deben tratarse con confidencialidade.

2. Boas prácticas segundo perfil

Administrativos

- Gardar documentos en lugares seguros ou cifrados.
- Bloquear ordenadores ao ausentarse.
- Non compartir contrasinais nin acceso a sistemas.
- Destruír documentos innecesarios mediante trituradora ou procedemento seguro.

Conserxes

- Verificar identidade de persoas que soliciten información ou acceso ao centro.
- Custodiar correctamente chaves, rexistros e listados de entrada/saída.
- Non facilitar información sen autorización.

Limpeza/Mantemento

- Respectar confidencialidade de documentos e equipos que se atopen en aulas ou despachos.
- Non manipular ordenadores, carpetas ou documentos con información persoal.

- Comunicar inmediatamente ao responsable calquera documento extraviado ou información sensible.

3. Seguridade en equipos dixitais

Boas prácticas:

- Usar só equipos autorizados.
- Non conectar USB persoais.
- Gardar arquivos en lugares seguros.
- Pechar sesión ao finalizar.

4. Intelixencia Artificial (IA)

Ferramentas de IA poden xerar informes ou automatizar tarefas, pero hai que evitar exposición de datos sensibles ou erros de decisión automatizada.

Recomendacións:

- Non introducir información persoal en IA externas.
- Comprobar precisión de informes xerados automaticamente.
- Usar IA como apoio mantendo control humano.

5. Formación

Formación

- **Teórica:** Sesións expositivas sobre seguridade administrativa, protección de datos e uso responsable de IA.
- **Práctica:** Casos de estudo, simulacións de incidentes, role-playing sobre acceso e custodia de información sensible.

Metodoloxía: 3 sesións de 90 min; teoría e prácticas simuladas.

Seguimento / Avaliación: Quiz, informes prácticos e observación do manexo seguro da información.