AcreditaPRO

MANUAL DE ESTUDIO

Seguridad Digital y Protección de Datos Básica (RGPD para Empleados)

Material de apoyo para la preparación del examen

Formación impartida conforme al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), alineada además con el Área 4: Seguridad del Marco Europeo de Competencias Digitales DigComp 3.0.

Generado el 18/11/2026

© AcreditaPro

Índice

1. 1. Introducción y objetivos del curso
2. 2. ¿Qué es la seguridad digital y por qué importa?
3. 3. Principales amenazas digitales
4. 4. Contraseñas seguras: cómo crearlas y gestionarlas
5. 5. Phishing: cómo reconocerlo y evitarlo
6. 6. Malware y ransomware
7. 7. Seguridad en el correo electrónico
8. 8. Seguridad en dispositivos móviles
9. 9. Redes seguras: Wi-Fi y VPN
0. 10. ¿Qué es el RGPD y a quién aplica?
11. 11. Principios clave del RGPD
12. 12. Derechos de los ciudadanos bajo el RGPD
13. 13. Obligaciones del empleado en materia de datos personales
4. 14. Categorías especiales de datos: mayor protección
5. 15. Brechas de seguridad: qué hacer si ocurre una
6. 16. El Delegado de Protección de Datos (DPO)
17. 17. Protección de datos en el trabajo remoto
8. 18. Buenas prácticas de seguridad digital en la empresa
9. 19. Resumen de puntos clave
0. 20. Anexo normativo: legislación aplicable
21. 21. Glosario de términos

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

Este curso acredita competencias en seguridad digital y protección de datos personales, conforme al Marco Europeo de Competencias Digitales DigComp 3.0 (Área 4: Seguridad) y al Reglamento (UE) 2016/679 (RGPD). Es una acreditación de competencias profesionales orientada a la concienciación de empleados, no a la certificación como Delegado de Protección de Datos (DPO).

1. Introducción y objetivos del curso

La seguridad digital y la protección de datos personales son responsabilidad de todos los empleados, no solo del departamento de informática. Un solo clic en un enlace malicioso o un fichero adjunto incorrecto puede comprometer toda la información de una empresa. Conocer las amenazas y saber cómo actuar es la primera línea de defensa.

Al finalizar este curso, serás capaz de:

- Identificar las principales amenazas digitales y cómo protegerte de ellas.
- Crear y gestionar contraseñas seguras.
- Reconocer intentos de phishing y otras técnicas de ingeniería social.
- Entender qué es el RGPD y qué obligaciones implica para tu trabajo diario.
- Actuar correctamente ante una posible brecha de seguridad.

2. ¿Qué es la seguridad digital y por qué importa?

La seguridad digital es el conjunto de medidas técnicas, organizativas y personales que protegen la información y los sistemas contra accesos no autorizados, daños o pérdidas.

En el entorno empresarial, un incidente de seguridad puede tener consecuencias graves: pérdida de datos de clientes, daño reputacional, sanciones legales (el RGPD permite multas de hasta 20 millones de euros o el 4% de la facturación anual global), interrupción de la actividad y costes de recuperación.

La mayoría de incidentes de seguridad tienen un factor humano: phishing, contraseñas débiles, dispositivos sin actualizar o información compartida sin cuidado. Por eso la formación de los empleados es tan importante como los sistemas técnicos.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

3. Principales amenazas digitales



Las amenazas más frecuentes que puede encontrar un empleado son:

- **Phishing**: emails o webs falsas que simulan ser de empresas legítimas (banco, correos, gestoría) para robar credenciales o datos personales.
- **Malware**: software malicioso que se instala en el dispositivo sin consentimiento — incluye virus, troyanos, spyware y adware.
- **Ransomware**: tipo de malware que cifra todos los ficheros del sistema y exige un pago (rescate) para devolver el acceso.
- **Ingeniería social**: técnicas de manipulación psicológica para conseguir que la víctima revele información o realice una acción (llamadas haciéndose pasar por soporte técnico, por ejemplo).
- **Contraseñas débiles**: el acceso no autorizado más sencillo — contraseñas cortas, comunes o reutilizadas en múltiples servicios.

4. Contraseñas seguras: cómo crearlas y gestionarlas



Una contraseña segura debe tener:

- Al menos **12 caracteres** (cuanto más larga, mejor).

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

- **Mayúsculas y minúsculas**.
- Al menos un **número**.
- Al menos un **símbolo** (!@#$%^&*...).
- **Sin datos personales**: sin tu nombre, fecha de nacimiento, nombre de mascota, ni palabras del diccionario.

Gestores de contraseñas: aplicaciones como Bitwarden, 1Password o el gestor integrado del navegador guardan todas tus contraseñas de forma cifrada — solo necesitas recordar una contraseña maestra. Son la solución más práctica para tener contraseñas únicas y seguras en todos los servicios.

Autenticación en dos factores (2FA): además de la contraseña, el sistema pide un segundo factor de verificación (código enviado al móvil, aplicación de autenticación). Actívalo en todos los servicios que lo permitan.

5. Phishing: cómo reconocerlo y evitarlo

El phishing es el ataque más común. Señales de alerta en un email:

- **Remitente sospechoso**: el email viene de una dirección parecida pero no igual a la real (por ejemplo, soporte@amaz0n.com en vez de amazon.com).
- **Urgencia artificial**: "Tu cuenta será bloqueada en 24 horas si no actúas".
- **Enlace que no coincide**: al pasar el ratón por encima del enlace (sin hacer clic) aparece una URL diferente a la que muestra el texto.
- **Errores de redacción**: traducciones deficientes o errores ortográficos que una empresa real no cometería.
- **Solicitud de datos sensibles**: ninguna empresa legítima te pide contraseñas, datos bancarios o DNI por email.

Si recibes un email sospechoso: no hagas clic en ningún enlace, no descargues adjuntos, y contacta directamente con la empresa (buscando su número en su web oficial, no en el email).

6. Malware y ransomware

El malware se instala habitualmente a través de:

- Adjuntos de email maliciosos (sobre todo .exe, .zip, .docm, .xlsm).
- Descargas de webs no confiables o software pirata.
- Dispositivos USB de origen desconocido.
- Actualizaciones falsas de software.

Para protegerte: mantén el sistema operativo y los programas actualizados, usa un antivirus activo, y desconfía de cualquier software descargado fuera de los canales oficiales.

El **ransomware** es especialmente grave porque una vez que cifra los ficheros, recuperarlos sin la clave (que tiene el atacante) es prácticamente imposible. Las copias de seguridad desconectadas

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

de la red (backups offline) son la única defensa real contra el ransomware.

7. Seguridad en el correo electrónico

El correo electrónico es el principal vector de ataque en las empresas. Buenas prácticas:

- **No abras adjuntos inesperados** aunque vengan de contactos conocidos — su cuenta puede estar comprometida.
- **Verifica por otra vía** los emails que piden acciones urgentes o transferencias de dinero (llama al remitente antes de actuar).
- **Cifra los emails** que contengan información sensible si tu cliente de correo lo permite.
- **No uses el correo corporativo para asuntos personales**: reduce el riesgo de recibir spam y phishing en la cuenta de trabajo.
- **Cuidado con el "Responder a todos"**: puede revelar información a personas que no deben tenerla.

8. Seguridad en dispositivos móviles

Los smartphones y tablets contienen tanta información como un ordenador, pero suelen tener menos protección. Medidas básicas:

- **Bloqueo de pantalla**: usa PIN, contraseña, huella dactilar o reconocimiento facial.
- **Actualizaciones**: instala las actualizaciones del sistema operativo y de las aplicaciones en cuanto estén disponibles.
- **Solo aplicaciones de tiendas oficiales**: App Store o Google Play, no de fuentes externas.
- **Localización y borrado remoto**: activa la función "Encontrar mi dispositivo" para poder borrarlo a distancia si se pierde o te lo roban.
- **Bluetooth y Wi-Fi**: desactívalos cuando no los uses para evitar conexiones no autorizadas.

9. Redes seguras: Wi-Fi y VPN

Las redes Wi-Fi públicas (cafeterías, aeropuertos, hoteles) son especialmente peligrosas porque cualquiera en la misma red puede interceptar el tráfico no cifrado.

Reglas básicas:

- **Nunca accedas a cuentas bancarias o sistemas de empresa** desde Wi-Fi pública sin VPN.
- **VPN (Red Privada Virtual)**: cifra todo el tráfico entre tu dispositivo y el servidor de destino, protegiéndolo de interceptaciones. Si tu empresa proporciona VPN, úsala siempre que trabajes fuera de la oficina.
- **Verifica el nombre de la red**: los atacantes pueden crear redes Wi-Fi falsas con nombres similares a los legítimos ("Starbucks_Guest" vs "Starbucks_Free").

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

10. ¿Qué es el RGPD y a quién aplica?

El **Reglamento General de Protección de Datos** (Reglamento UE 2016/679, RGPD) es la principal norma europea sobre protección de datos personales. Entró en vigor el 25 de mayo de 2018 y aplica a cualquier organización que trate datos personales de personas en la Unión Europea, independientemente de dónde esté ubicada la organización.

Dato personal: cualquier información que permita identificar a una persona física, directa o indirectamente — nombre, email, DNI, dirección, IP, número de teléfono, etc.

¿A quién aplica? A todas las empresas, autónomos y organizaciones que traten datos personales: tiendas, clínicas, bufetes de abogados, pymes, freelances... El tamaño no importa.

11. Principios clave del RGPD



El RGPD establece varios principios que deben respetarse al tratar datos personales:

- **Licitud**: solo se pueden tratar datos si existe una base legal (contrato, obligación legal, interés legítimo o consentimiento del afectado).
- **Transparencia**: el afectado debe ser informado de cómo se usan sus datos.
- **Limitación de finalidad**: los datos recogidos para un fin no pueden usarse para otro diferente.
- **Minimización**: solo se deben tratar los datos estrictamente necesarios.
- **Exactitud**: los datos deben estar actualizados y ser correctos.
- **Limitación del plazo de conservación**: no se pueden guardar los datos más tiempo del necesario.
- **Integridad y confidencialidad (seguridad)**: hay que proteger los datos con medidas técnicas y organizativas adecuadas.

12. Derechos de los ciudadanos bajo el RGPD

El RGPD reconoce varios derechos a cualquier persona cuyos datos son tratados:

- **Derecho de acceso**: saber qué datos se tienen sobre ti.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

- **Derecho de rectificación**: corregir datos incorrectos o incompletos.
- **Derecho de supresión ("derecho al olvido")**: solicitar que se borren tus datos.
- **Derecho de limitación**: solicitar que se deje de usar tus datos temporalmente.
- **Derecho de portabilidad**: recibir tus datos en un formato estructurado para trasladarlos a otro servicio.
- **Derecho de oposición**: oponerte a que se traten tus datos para determinados fines.

Como empleado, tu empresa también tiene obligaciones hacia ti como interesado — en tu nómina, en los registros de vacaciones, en las cámaras de seguridad, etc.

13. Obligaciones del empleado en materia de datos personales

Como empleado que trata datos personales en su trabajo diario, tienes obligaciones concretas:

- **Solo trata los datos que necesitas** para hacer tu trabajo — no accedas a información de clientes o compañeros que no es necesaria para tu tarea.
- **No compartas datos personales** con terceros no autorizados — ni por email, ni verbalmente, ni en documentos impresos.
- **Protege los documentos físicos**: no dejes documentos con datos personales a la vista de personas no autorizadas; usa la trituradora para destruirlos.
- **Pantalla limpia**: no dejes tu sesión abierta sin supervisión — bloquea el ordenador al alejarte (Ctrl+L en Windows o Command+L en Mac).
- **Notifica cualquier incidente** a tu responsable o al DPO inmediatamente si sospechas que ha habido una brecha de datos.

14. Categorías especiales de datos: mayor protección

El RGPD establece una protección reforzada para ciertos tipos de datos especialmente sensibles:

- Origen racial o étnico
- Opiniones políticas
- Creencias religiosas o filosóficas
- Afiliación sindical
- Datos genéticos y biométricos
- Datos de salud
- Vida u orientación sexual
- Datos de condenas e infracciones penales

Estas categorías están sometidas a restricciones adicionales: en general, no pueden tratarse salvo excepciones muy específicas (consentimiento explícito, necesidad médica, etc.). Como empleado, si manejas este tipo de datos, debes extremar las precauciones.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

15. Brechas de seguridad: qué hacer si ocurre una

Una brecha de seguridad es cualquier incidente que afecte a la confidencialidad, integridad o disponibilidad de datos personales: pérdida de un portátil con datos de clientes, envío de un email a la persona equivocada, acceso no autorizado a una base de datos, etc.

Qué debes hacer si detectas o sospechas una brecha:

1. **No lo silencies**: notifícalo inmediatamente a tu responsable o al DPO, aunque no estés seguro de si ha habido un problema real.
2. **No intentes resolverlo tú solo** si no tienes los conocimientos técnicos.
3. La empresa tiene **72 horas** para notificar la brecha a la Agencia Española de Protección de Datos (AEPD) si puede causar riesgos para los afectados.

16. El Delegado de Protección de Datos (DPO)

El DPO (Data Protection Officer) es la figura responsable de supervisar el cumplimiento del RGPD dentro de una organización. No todas las empresas están obligadas a tener uno (el RGPD lo exige a organismos públicos, a empresas que tratan datos a gran escala o que tratan categorías especiales de datos de forma sistemática; además, el artículo 34 de la LOPDGDD obliga a designar DPO a determinados sectores, como colegios, centros sanitarios, banca, seguros o seguridad privada, al margen del volumen de datos).

El DPO es tu punto de contacto para cualquier duda sobre protección de datos: qué datos puedes tratar, cómo responder a una solicitud de ejercicio de derechos, cómo notificar una brecha, etc. No tiene poder sancionador sobre los empleados — su función es de asesoramiento y supervisión.

17. Protección de datos en el trabajo remoto

El trabajo remoto (teletrabajo) introduce riesgos adicionales que hay que gestionar:

- **Usar los dispositivos de empresa** para el trabajo, no los personales — los dispositivos de empresa tienen las medidas de seguridad configuradas por el departamento de IT.
- **Red segura**: usa la VPN corporativa siempre que accedas a sistemas de la empresa desde casa o desde una red Wi-Fi que no controlas.
- **Entorno de trabajo**: asegúrate de que nadie ajeno a la empresa puede ver tu pantalla o escuchar conversaciones con información confidencial.
- **Documentos físicos**: si imprimes documentos con datos personales en casa, triturálos al acabar — no los tires enteros a la basura.
- **Bloqueo del dispositivo**: aunque estés en casa, bloquea el ordenador cuando te alejes.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

18. Buenas prácticas de seguridad digital en la empresa

- **Política de escritorio limpio**: no dejes documentos con información confidencial sobre la mesa al salir — guárdalos o destruyelos.
- **Actualizaciones**: instala siempre las actualizaciones de seguridad del sistema operativo y las aplicaciones.
- **Backups**: asegúrate de que tu trabajo queda incluido en las copias de seguridad de la empresa.
- **Software autorizado**: instala solo software aprobado por el departamento de IT — el software no autorizado puede ser fuente de malware o generar problemas de licencias.
- **Incidentes**: si algo te parece sospechoso (un email raro, un comportamiento inusual del ordenador), repórtalo al departamento de IT antes de intentar resolverlo tú.

19. Resumen de puntos clave

- La mayoría de incidentes de seguridad tienen un factor humano: phishing, contraseñas débiles o información compartida sin cuidado.
- Una contraseña segura tiene al menos 12 caracteres, mayúsculas, minúsculas, números y símbolos.
- El RGPD aplica a cualquier empresa que trate datos personales de personas en la UE.
- Como empleado, solo debes tratar los datos que necesitas para tu trabajo y notificar cualquier incidente inmediatamente.
- La verificación en dos factores (2FA) es la medida de seguridad más efectiva tras la contraseña.

20. Anexo normativo: legislación aplicable

- **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo** (RGPD), de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Aplicable desde el 25 de mayo de 2018.
- **Ley Orgánica 3/2018, de 5 de diciembre**, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): adapta el RGPD al ordenamiento jurídico español e introduce derechos digitales específicos.
- **DigComp 3.0** (Comisión Europea, diciembre 2025): Área 4 (Seguridad), que incluye la protección de dispositivos, de datos personales y de la privacidad.

El certificado que acredita la superación de este curso es un documento privado de formación orientado a la concienciación de empleados en materia de seguridad y protección de datos. No certifica al titular como Delegado de Protección de Datos (DPO) ni equivale a ninguna habilitación oficial.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

21. Glosario de términos

- **RGPD**: Reglamento General de Protección de Datos (Reglamento UE 2016/679); principal norma europea sobre tratamiento de datos personales, aplicable desde mayo de 2018.
- **Dato personal**: cualquier información que permita identificar a una persona física directa o indirectamente (nombre, email, DNI, dirección IP, etc.).
- **DPO (Delegado de Protección de Datos)**: responsable de supervisar el cumplimiento del RGPD en una organización; punto de contacto para dudas sobre protección de datos.
- **Phishing**: técnica de ataque que usa emails o webs falsas para engañar a las víctimas y robarles credenciales o datos personales.
- **Malware**: software malicioso diseñado para dañar, infectar o tomar el control de un dispositivo sin el consentimiento del usuario.
- **Ransomware**: tipo de malware que cifra los ficheros del sistema y exige un pago (rescate) para devolver el acceso.
- **Ingeniería social**: técnicas de manipulación psicológica para conseguir que una persona revele información confidencial o realice una acción perjudicial.
- **Autenticación en dos factores (2FA)**: mecanismo de seguridad que requiere un segundo factor de verificación (código en el móvil, app de autenticación) además de la contraseña.
- **VPN (Red Privada Virtual)**: tecnología que cifra el tráfico entre el dispositivo y el servidor, protegiendo la información en redes no seguras como el Wi-Fi público.
- **Brecha de seguridad**: incidente que afecta a la confidencialidad, integridad o disponibilidad de datos personales (pérdida de dispositivo, acceso no autorizado, envío a destinatario equivocado).
- **Minimización de datos**: principio del RGPD que establece que solo deben tratarse los datos personales estrictamente necesarios para el fin perseguido.
- **Consentimiento**: base legal del RGPD por la que el afectado autoriza expresamente el tratamiento de sus datos para un fin concreto.
- **Derecho al olvido**: derecho reconocido por el RGPD que permite solicitar la supresión de los propios datos personales.
- **Categorías especiales de datos**: datos con protección reforzada bajo el RGPD (salud, biométricos, origen racial, opiniones políticas, vida sexual, etc.).
- **LOPDGDD**: Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales; adapta el RGPD al ordenamiento jurídico español.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.