

ÍNDICE

I. INTRODUCCIÓN

II. EL ERROR EN LOS TRATAMIENTOS DE PROTECCIÓN DE DATOS: GUÍA PRÁCTICA PARA PREVENIR INCIDENTES EN LAS ORGANIZACIONES

I. Comunicaciones electrónicas

1. Enviar un correo al destinatario equivocado
2. Usar CC en vez de CCO en envíos masivos
3. Adjuntar un archivo incorrecto con datos de terceros
4. Reenviar hilos completos de correo sin depuración previa
5. Responder a todos sin necesidad
6. Incluir datos innecesarios en copia
7. Enviar documentos sin cifrado
8. Compartir enlaces abiertos sin restricción de acceso
9. No proteger con contraseña archivos sensibles
10. Facilitar datos personales por teléfono sin verificar la identidad del interlocutor
11. Enviar bases de datos completas sin justificación funcional
12. Utilizar el correo electrónico personal para el tratamiento de datos corporativos
13. Enviar capturas de pantalla con datos personales visibles innecesariamente
14. No eliminar los metadatos de los documentos antes de su envío
15. Compartir enlaces sin fecha de expiración
16. Copiar a terceros en comunicaciones sin base jurídica
17. Remitir nóminas por error a otro empleado
18. Enviar contratos sin anonimizar los anexos que contienen datos de terceros
19. Usar plataformas de transferencia de ficheros no autorizadas
20. No comprobar los destinatarios antes de enviar comunicaciones con datos personales
21. Reenviar currículums vitae sin autorización del candidato
22. Compartir listados internos por error
23. Enviar información sensible sin verificar el cifrado TLS del canal de comunicación
24. Incluir datos personales en el campo del asunto del correo electrónico
25. No retirar el acceso tras compartir un enlace con un destinatario

II. Gestión documental física

26. Dejar documentos en la impresora

27. Abandonar expedientes en mesas de trabajo
28. No cerrar archivadores con llave
29. Trasladar expedientes al domicilio particular sin autorización
30. Tirar o eliminar los documentos con datos personales en la papelera común
31. Archivar documentación en ubicación incorrecta
32. Permitir el acceso de visitantes a zonas con documentación personal sin control
33. Extraviar un expediente físico
34. Fotografiar documentos con datos personales con el teléfono móvil personal
35. No aplicar la política de mesa limpia
36. Imprimir documentación innecesaria con datos personales
37. Olvidar documentación en salas de reuniones
38. Enviar la correspondencia postal con datos personales a una dirección errónea
39. No registrar el préstamo de expedientes físicos
40. Duplicar copias de documentos sin control
41. No destruir borradores impresos de documentos con datos personales
42. Etiquetar carpetas o archivadores con datos personales visibles
43. No custodiar adecuadamente el libro de visitas
44. Permitir el acceso al archivo a personal no autorizado
45. Mezclar expedientes de distintos interesados
46. No verificar el destinatario en envíos por mensajería física
47. Guardar documentación sensible en cajones sin llave
48. Abandonar el portátil abierto con datos visibles en la pantalla
49. No recoger documentos del puesto de trabajo al finalizar la jornada laboral
50. Transportar la documentación con datos personales sin un sobre cerrado o en un contenedor no seguro

III. Credenciales y accesos

51. Compartir contraseñas entre empleados
52. Anotar contraseñas en papeles visibles o post-it
53. No cambiar la contraseña periódicamente en sistemas críticos
54. Utilizar la misma contraseña para todos los sistemas
55. No bloquear la pantalla al ausentarse del puesto de trabajo
56. Acceder a datos personales sin una necesidad funcional justificada
57. Consultar datos personales por curiosidad personal
58. Mantener el acceso a sistemas tras un cambio de puesto o de departamento
59. Permitir el uso de la sesión activa de otro empleado

- 60. No activar el doble factor de autenticación en sistemas con datos sensibles
- 61. Crear cuentas de usuario genéricas o compartidas
- 62. Facilitar códigos OTP a terceros
- 63. No comunicar el robo o pérdida de credenciales de acceso
- 64. Acceder a los sistemas fuera del horario habitual sin causa justificada
- 65. Mantener privilegios de acceso excesivos respecto a las funciones del empleado
- 66. Utilizar credenciales de un ex empleado
- 67. No revisar periódicamente los permisos de acceso asignados
- 68. Acceder a datos personales de familiares o personas conocidas
- 69. No cerrar la sesión remota al finalizar el trabajo
- 70. No registrar los accesos extraordinarios a datos personales
- 71. Compartir un token físico de acceso
- 72. No revocar accesos temporales tras finalizar su justificación
- 73. Conectarse a sistemas corporativos desde dispositivos no autorizados
- 74. No informar de intentos sospechosos de acceso a los sistemas
- 75. No separar los perfiles de prueba y de producción

IV. Dispositivos y tecnología

- 76. Usar USB personal sin cifrado para almacenar datos corporativos
- 77. Descargar bases de datos completas al escritorio local del ordenador
- 78. Trabajar en redes Wi-Fi públicas sin VPN
- 79. Instalar software no autorizado en dispositivos corporativos con datos personales
- 80. No actualizar el sistema operativo y el software en dispositivos con datos personales
- 81. Usar servicios de nube personal para almacenar datos corporativos con datos personales
- 82. No cifrar el portátil corporativo que contiene datos personales
- 83. No reportar la pérdida o robo de un dispositivo corporativo
- 84. Conectar discos externos sin un análisis antivirus previo
- 85. Sincronizar datos personales corporativos en dispositivos móviles personales sin MDM
- 86. Compartir pantalla durante videollamadas mostrando datos personales innecesarios
- 87. Grabar reuniones con datos personales sin informar a los participantes
- 88. Mantener copias locales no autorizadas de datos personales
- 89. No borrar los datos personales antes de desechar o reparar un equipo informático
- 90. Prestar el portátil corporativo a un tercero ajeno a la organización

- 91. No activar el bloqueo automático de pantalla en dispositivos con datos personales
- 92. Enviar datos personales a través de aplicaciones de mensajería personal no corporativas
- 93. No separar el entorno laboral del personal en dispositivos de uso mixto
- 94. Guardar datos personales en el escritorio del ordenador en carpetas sin protección
- 95. Transferir datos personales a través de Bluetooth sin cifrado
- 96. Usar herramientas de IA generativa con datos personales sin autorización previa
- 97. Copiar bases de datos para pruebas sin anonimizar los datos personales
- 98. Subir documentos internos con datos personales a plataformas externas no autorizadas
- 99. No proteger adecuadamente el router doméstico utilizado para el teletrabajo
- 100. Imprimir datos personales en impresoras domésticas compartidas durante el teletrabajo

V. Recogida y tratamiento

- 101. Solicitar datos personales excesivos en formularios y procesos de recogida de datos
- 102. No entregar una cláusula informativa en el momento de la recogida de datos personales
- 103. Recoger un consentimiento inválido como base jurídica del tratamiento
- 104. No documentar el consentimiento obtenido
- 105. Reutilizar los datos personales para una finalidad distinta a la original sin base jurídica
- 106. Registrar datos inexactos o desactualizados
- 107. No actualizar los datos tras una solicitud de rectificación
- 108. Crear hojas de cálculo o bases de datos paralelas no autorizadas
- 109. No aplicar el principio de minimización en el diseño de nuevos tratamientos
- 110. Conservar datos personales más allá del plazo de retención establecido
- 111. Tratar datos de categoría especial sin una base jurídica suficiente
- 112. No anonimizar datos en análisis estadísticos cuando es técnicamente posible
- 113. Recoger datos de menores sin verificar la edad ni obtener el consentimiento del titular de la patria potestad
- 114. Usar datos laborales de los empleados con fines comerciales sin una base jurídica
- 115. No revisar los formularios online desde la perspectiva de la protección de datos
- 116. No diferenciar el tratamiento de datos ordinarios y categorías especiales
- 117. No aplicar la seudonimización cuando técnicamente procede y reduce el riesgo
- 118. No verificar la legitimación antes de lanzar una campaña comercial
- 119. No bloquear datos personales cuando su conservación está sujeta a limitación

- 120. No eliminar datos personales tras la baja o desvinculación de un cliente
- 121. No revisar periódicamente las cesiones a terceros
- 122. No informar a los interesados sobre transferencias internacionales de datos
- 123. No verificar que el encargado del tratamiento cumple con el RGPD antes de contratarle
- 124. No formalizar el contrato de encargado del tratamiento con los proveedores
- 125. Reutilizar bases de datos antiguas sin revisar su legitimidad actual

VI. Derechos de los interesados

- 126. Ignorar una solicitud de acceso
- 127. Superar el plazo legal de respuesta
- 128. Exigir una documentación excesiva al interesado
- 129. No verificar la identidad del solicitante
- 130. Facilitar datos a una persona incorrecta
- 131. No registrar la solicitud recibida
- 132. Responder de forma incompleta
- 133. Denegar un derecho sin fundamento
- 134. No informar del derecho a reclamar ante la autoridad de control
- 135. No comunicar la rectificación a terceros
- 136. No ejecutar la supresión de los datos personales de una manera efectiva
- 137. No atender la oposición al marketing directo
- 138. No informar de la limitación del tratamiento
- 139. No permitir la portabilidad cuando procede
- 140. Retrasar la respuesta por desorganización interna

VII. Gestión de brechas

- 141. No comunicar el incidente de seguridad detectado
- 142. Minimizar el impacto de una filtración
- 143. No conservar evidencias del incidente
- 144. Borrar correos relevantes tras el error
- 145. No informar al superior inmediato
- 146. No colaborar en la investigación interna
- 147. Ocultar un incidente por miedo
- 148. No participar en el análisis posterior
- 149. Repetir la conducta tras advertencia
- 150. No seguir el protocolo interno de brechas de seguridad

VIII. Cultura y conducta ética

- 151. Comentar datos personales en el ascensor
- 152. Publicar imágenes sin autorización
- 153. Etiquetar empleados en redes sociales sin consentimiento
- 154. Priorizar las ventas sobre la confidencialidad
- 155. No asistir a la formación obligatoria en protección de datos
- 156. Ignorar los protocolos aprendidos en la formación
- 157. Acceder a datos por curiosidad personal
- 158. Compartir currículums vitae sin anonimizar
- 159. Difundir rankings con datos identificativos
- 160. Utilizar datos internos para fines personales
- 161. Grabar conversaciones laborales sin legitimación
- 162. Presionar a compañeros para facilitar datos
- 163. Reenviar nóminas sin protección
- 164. No consultar al DPD ante una duda razonable
- 165. Normalizar prácticas incorrectas
- 166. Utilizar datos para conflictos personales
- 167. Divulgar información médica de un compañero
- 168. No advertir el error detectado
- 169. Utilizar datos para fines políticos internos
- 170. Compartir bases de datos por comodidad

IX. Supuestos adicionales de riesgo avanzado

- 171. Exportar datos personales para un análisis sin anonimizar
- 172. Usar datos reales en entornos de prueba
- 173. Integrar datos en herramientas externas sin evaluación previa
- 174. Automatizar decisiones sin una supervisión humana
- 175. No revisar los registros de acceso cuando procede
- 176. No aplicar el principio de limitación de finalidad
- 177. No aplicar la privacidad desde el diseño en nuevos procesos
- 178. Copiar datos en presentaciones comerciales
- 179. Exponer datos en pizarras visibles
- 180. Utilizar datos para elaborar perfiles no autorizados
- 181. Enviar datos a proveedores no evaluados
- 182. No revisar la configuración de la privacidad en el software

183. No restringir las descargas masivas desde el CRM u otros sistemas de gestión
184. No anonimizar datos en informes internos
185. No aplicar la segmentación adecuada en campañas de comunicación comercial
186. Permitir el acceso remoto sin una autenticación fuerte
187. No revisar los contratos de confidencialidad con empleados y colaboradores
188. No documentar las decisiones sobre el tratamiento de datos personales
189. No aplicar la destrucción certificada de soportes físicos con datos personales
190. No registrar los incidentes menores repetidos
191. Utilizar datos para fines disciplinarios sin una base legal suficiente
192. Compartir datos con la sociedad matriz sin legitimación clara
193. No bloquear datos tras una reclamación judicial o requerimiento formal
194. Conservar datos personales en copias de seguridad sin control de plazo
195. No supervisar las prácticas de protección de datos en el teletrabajo
196. No revisar los permisos de acceso tras una auditoría interna
197. No formar a los nuevos empleados en materia de protección de datos
198. No actualizar los protocolos internos tras cambios normativos relevantes
199. No aplicar un control de versiones en documentos sensibles
200. Desatender las recomendaciones expresas del Delegado de Protección de Datos
201. Incorporar datos personales en prompts de herramientas de IA generativa sin anonimización previa
202. Subir bases de datos reales a entornos sandbox externos sin autorización formal
203. Exportar listados completos para un análisis personal fuera del entorno corporativo
204. Realizar pruebas técnicas utilizando datos reales de clientes
205. Compartir dashboards con datos identificativos sin restringir el acceso
206. No configurar correctamente los permisos en herramientas colaborativas
207. Crear carpetas compartidas accesibles a toda la organización sin necesidad funcional
208. No limitar las descargas masivas desde el CRM
209. Enviar informes con datos agregados sin verificar la posibilidad de reidentificación
210. Publicar estadísticas internas que permitan inferir datos individuales
211. Transferir datos a un proveedor extranjero sin verificar las cláusulas contractuales tipo
212. No comprobar el nivel de seguridad del proveedor antes de compartir información
213. Subcontratar servicios que implican tratamiento de datos sin comunicarlo internamente

214. Enviar datos personales a un asesor externo sin contrato de encargado del tratamiento vigente
215. No revisar las políticas de privacidad de nuevas herramientas antes de usarlas
216. Usar aplicaciones gratuitas para gestionar datos de clientes
217. Integrar datos en plataformas de marketing sin evaluación de impacto
218. No desactivar los accesos de un proveedor tras la finalización del contrato
219. Compartir accesos de proveedores entre empleados de la organización
220. No verificar la identidad de técnicos externos que acceden a sistemas con datos personales
221. Trabajar desde espacios de coworking sin protección visual de pantalla
222. Atender llamadas con datos personales en lugares públicos
223. Imprimir documentación confidencial en copisterías externas
224. Dejar dispositivos sin supervisión en aeropuertos o transporte público
225. Conectar un ordenador portátil corporativo a ordenadores o puertos de carga públicos
226. No utilizar filtros de privacidad en pantallas durante el teletrabajo
227. Compartir dispositivos corporativos con familiares
228. Guardar documentación laboral en carpetas compartidas del hogar
229. No proteger adecuadamente los archivos descargados durante el teletrabajo
230. Realizar videollamadas mostrando documentación física confidencial en el entorno doméstico
231. No aplicar criterios de privacidad desde el diseño en nuevos proyectos
232. No consultar al DPD antes de iniciar un nuevo tratamiento de datos
233. Implementar nuevas funcionalidades sin revisar el impacto en datos personales
234. No documentar las decisiones relativas a la base jurídica del tratamiento
235. Omitir la evaluación de riesgos antes de automatizar procesos con datos personales
236. No revisar las cláusulas informativas tras un cambio de finalidad
237. No actualizar el consentimiento tras modificar las condiciones del servicio
238. Integrar las bases de datos de distintas áreas sin un análisis previo de compatibilidad de finalidades
239. No revisar los registros de auditoría tras detectar anomalías en los sistemas
240. No documentar los incidentes reiterados de bajo impacto
241. Utilizar datos personales para formación interna sin anonimización previa
242. Proyectar listados con nombres en sesiones formativas abiertas
243. Usar ejemplos reales identificables en presentaciones comerciales
244. Publicar casos de éxito con datos identificativos sin autorización

- 245. Compartir fotografías de eventos corporativos sin revisar las autorizaciones
- 246. Difundir en la intranet información médica de empleados
- 247. Utilizar datos internos para las investigaciones disciplinarias sin una base jurídica suficiente
- 248. No bloquear los datos tras una orden judicial o una reclamación formal
- 249. Conservar los datos en copias de seguridad sin un control de plazo de retención
- 250. Desoír las recomendaciones expresas del Delegado de Protección de Datos en materia de seguridad o de legitimación

III. ALGUNAS CONCLUSIONES

IV. BIBLIOGRAFÍA