

Responsabilidad de las empresas ante un ciberataque



Donostia, 4 de junio de 2024



¿Qué es un ciberataque?



Un intento de obtener acceso no autorizado a los servicios, recursos o información del sistema, o un intento de comprometer la integridad, disponibilidad o confidencialidad del sistema” (NIST Special Publication NIST SP 800-82r3



Intento no autorizado de afectar la
integridad , disponibilidad  o
confidencialidad  de un sistema
informático

Ataques internos y ataques externos



¿Cómo podemos prepararnos para un ciberataque?



Obligaciones legales



- **Reglamento europeo sobre la resiliencia operativa digital del sector financiero (DORA)**
- **Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS 2)**
- **Reglamento General de Protección de Datos (RGPD)**
- **CRA (Cybersecurity Resilience Act). Ciberseguridad para los productos con elementos digitales**
- **IA Act. Reglamento Europeo sobre Inteligencia Artificial**



- Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
- Esquema Nacional de Seguridad
- Real Decreto-ley 7/2022, sobre seguridad de redes 5G



Hemos sufrido un
ciberataque... ¿qué
debemos hacer? 🤔

Contener la brecha

Evaluar el impacto



Investigar el origen



Notificación del incidente



BORRAR DATOS

1. RESPONSABLE DE TRATAMIENTO

RAZÓN SOCIAL:

NIF/OTRO: TELÉFONO: EMAIL:

DIRECCIÓN: CP:

PROVINCIA: LOCALIDAD: PAÍS:

ÁMBITO DE LA ORGANIZACIÓN: ORGANIZACIÓN PRIVADA ORGANIZACIÓN PÚBLICA

TIPO DE ORGANIZACIÓN:

AUTÓNOMO O MICROEMPRESA (MENOS DE 10 TRABAJ.) PEQUEÑA Y MEDIANA EMPRESA

GRAN EMPRESA O MULTINACIONAL OTROS

SECTOR DE ACTIVIDAD:

Indicar un sector de actividad de la lista de sectores en la última página.

2. ENCARGADO DE TRATAMIENTO

¿HAY OTRA ORGANIZACIÓN IMPLICADA EN LA BRECHA DE DATOS PERSONALES? SÍ NO EN SU CASO, CONSIGNE LOS DATOS DEL ENCARGADO

RAZÓN SOCIAL:

NIF/OTRO: TELÉFONO: EMAIL:

DIRECCIÓN: CP:

PROVINCIA: LOCALIDAD: PAÍS:

ÁMBITO DE LA ORGANIZACIÓN: ORGANIZACIÓN PRIVADA ORGANIZACIÓN PÚBLICA

3. DELEGADO DE PROTECCIÓN DE DATOS O PERSONA DE CONTACTO

¿TIENE EL RESPONSABLE DESIGNADO UN DELEGADO DE PROTECCIÓN DE DATOS? SÍ NO

EN SU CASO, CONSIGNE LOS DATOS DEL DPO. EN CASO CONTRARIO CONSIGNE LOS DATOS DE UNA PERSONA DE CONTACTO

NOMBRE:

NIF/OTRO: TELÉFONO: EMAIL:

DIRECCIÓN: CP:

PROVINCIA: LOCALIDAD: PAÍS:

ÁMBITO DE LA ORGANIZACIÓN: ORGANIZACIÓN PRIVADA ORGANIZACIÓN PÚBLICA

4. DATOS DE LA NOTIFICACIÓN

¿CUÁL ES SU INTENCIÓN?

NOTIFICAR UNA NUEVA BRECHA DE DATOS PERSONALES

MODIFICAR UNA NOTIFICACIÓN HECHA CON ANTERIORIDAD PARA PROPORCIONAR INFORMACIÓN RELEVANTE

EN SU CASO, DATOS DE LA NOTIFICACIÓN QUE SE MODIFICA:

REGISTRO DE ENTRADA: FECHA:

5. SOBRE EL TRATAMIENTO

¿DESDE CUANDO SE VIENE REALIZANDO EL TRATAMIENTO DE DATOS AFECTADO?

TRATAMIENTO PUNTUAL O MUY LIMITADO EN EL TIEMPO MENOS DE 1 AÑO

ENTRE 1 y 5 AÑOS MÁS DE 5 AÑOS

NÚMERO APROXIMADO DE PERSONAS FÍSICAS SOBRE LAS QUE SE RECIBE, ALMACENA O TRATA DATOS PERSONALES DE OTRA FORMA, REFERIDO EXCLUSIVAMENTE AL TRATAMIENTO SOBRE EL QUE SE HA PRODUCIDO LA BRECHA DE DATOS PERSONALES.

EL TRATAMIENTO SOBRE EL QUE SE HA PRODUCIDO LA BRECHA INCLUYE DATOS DE PERSONAS:

ÚNICAMENTE EN ESPAÑA, NIVEL LOCAL/MUNICIPAL EN UN ÚNICO ESTADO MIEMBRO, PERO NO EN ESPAÑA

ÚNICAMENTE EN ESPAÑA, NIVEL PROVINCIAL/AUTONÓMICO EN MÁS DE UN ESTADO MIEMBRO

ÚNICAMENTE EN ESPAÑA, NIVEL NACIONAL EN MÁS DE UN ESTADO MIEMBRO Y A TERCEROS PAÍSES

A NIVEL MUNDIAL / INTERNACIONAL

6. SOBRE LA BRECHA Y SUS CONSECUENCIAS

EL INCIDENTE HA SIDO:

ACCIDENTAL O SIN INTENCIONALIDAD INTENCIONADO, PARA DAÑAR AL RESPONSABLE, AL ENCARGADO O A LAS PERSONAS AFECTADAS

INTENCIONALIDAD DESCONOCIDA

EL ORIGEN DEL INCIDENTE HA SIDO:

INTERNO: PERSONAL O SISTEMAS BAJO EL CONTROL DEL RESPONSABLE DE TRATAMIENTO INTERNO: PERSONAL O SISTEMAS BAJO EL CONTROL DEL ENCARGADO DE TRATAMIENTO

EXTERNO: OTROS, AJENOS AL RESPONSABLE Y ENCARGADO DE TRATAMIENTO

¿CÓMO HA OCURRIDO LA BRECHA? PUEDE SELECCIONAR VARIAS OPCIONES:

<input type="checkbox"/> REVELACIÓN VERBAL NO AUTORIZADA	<input type="checkbox"/> DOCUMENTACIÓN PERDIDA, ROBADA O DEPOSITADA EN LOCALIZACIÓN INSEGURA	<input type="checkbox"/> CORREO POSTAL PERDIDO O ABIERTO
<input type="checkbox"/> ELIMINACIÓN INCORRECTA DE DATOS PERSONALES EN FORMATO PAPEL	<input type="checkbox"/> DATOS PERSONALES ENVIADOS POR ERROR (POSTAL O ELECTRONICAMENTE)	<input type="checkbox"/> DATOS PERSONALES MOSTRADOS AL INDIVIDUO INCORRECTO
<input type="checkbox"/> DATOS PERSONALES ELIMINADOS / DESTRUIDOS	<input type="checkbox"/> ABUSO DE PRIVILEGIOS DE ACCESO POR PARTE DE EMPLEADO PARA EXTRAER, REEMVIAR O COPIAR DATOS PERSONALES	<input type="checkbox"/> DATOS PERSONALES RESIDUALES EN DISPOSITIVOS OBSOLETOS
<input type="checkbox"/> PUBLICACIÓN NO INTENCIONADA / AUTORIZADA	<input type="checkbox"/> ENVÍO DE EMAIL A MÚLTIPLES DESTINATARIOS SIN COPIA OCULTA / LISTA DISTRIBUCIÓN	<input type="checkbox"/> DISPOSITIVO PERDIDO O ROBADO
<input type="checkbox"/> CIBERINCIDENTE: DISPOSITIVO CIFRADO / SECUESTRO DE INFORMACIÓN	<input type="checkbox"/> CIBERINCIDENTE: PHISHING / COMPROMISO DE CUENTA DE USUARIO	<input type="checkbox"/> CIBERINCIDENTE: ACCESO NO AUTORIZADO A DATOS EN SISTEMA TI
<input type="checkbox"/> INCIDENCIA TÉCNICA	<input type="checkbox"/> MODIFICACIÓN NO AUTORIZADA DE DATOS	

FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES

USO EXCLUSIVO PARA ENTIDADES NO OBLIGADAS A RELACIONARSE CON LA ADMINISTRACIÓN POR MEDIOS ELECTRONICOS O CUANDO NO ESTÉN DISPONIBLES DICHOS MEDIOS ELECTRONICOS

COMO CONSECUENCIA DEL INCIDENTE SE HA VISTO AFECTADA LA:		
<input type="checkbox"/> CONFIDENCIALIDAD: PERSONAS U ORGANIZACIONES QUE NO ESTÁN AUTORIZADAS, O NO TIENEN UN PROPÓSITO LEGÍTIMO PARA ACCEDER A LOS DATOS, HAN PODIDO ACCEDER Y/O EXTRAERLOS		
<input type="checkbox"/> DISPONIBILIDAD: SE HAN DESTRUIDO, PERDIDO O CIFRADO LOS DATOS PERSONALES, DE FORMA QUE NO PUEDEN SER TRATADOS		
<input type="checkbox"/> INTEGRIDAD: SE HAN ALTERADO LOS DATOS PERSONALES, SIGUEN SIENDO ACCESIBLES, PERO LA SUSTITUCIÓN DE DATOS PUEDE SUPONER UN DAÑO PARA LAS PERSONAS AFECTADAS		
SOLO EN CASO DE BRECHA DE CONFIDENCIALIDAD. ¿ESTÁN LOS DATOS CIFRADOS DE FORMA SEGURA, ANONIMIZADOS O PROTEGIOS DE FORMA QUE SON ININTELIGIBLES PARA QUIEN HAYA PODIDO TENER ACCESO, O NO SE PUEDE IDENTIFICAR A LAS PERSONAS?		
<input type="radio"/> SÍ	<input type="radio"/> NO	<input type="radio"/> DESCONOCIDO
SOLO EN CASO DE BRECHA DE DISPONIBILIDAD. ¿SE HA RECUPERADO LA DISPONIBILIDAD DE LOS DATOS PERSONALES DE FORMA QUE PUEDEN SER TRATADOS CON NORMALIDAD?		
<input type="radio"/> SÍ	<input type="radio"/> NO	<input type="radio"/> TODAVÍA NO, PERO SE RECUPERARÁ EN BREVE
SOLO EN CASO DE BRECHA DE INTEGRIDAD. SELECCIONE LA OPCIÓN MAS APROPIADA		
<input type="radio"/> DATOS ALTERADO, PERO SIN CONSTANCIA DE USO ILEGAL O INCORRECTO	<input type="radio"/> DATOS ALTERADOS Y USADOS DE FORMA LEGAL O INCORRECTA, PERO CON LA POSIBILIDAD DE REVERTIR/ RECUPERAR LOS DAÑOS	<input type="radio"/> DATOS ALTERADOS Y USADOS DE FORMA LEGAL O INCORRECTA, SIN POSIBILIDAD DE REVERTIR/ RECUPERAR LOS DAÑOS
¿CUÁLES PODRÍAN SER LAS CONSECUENCIAS SOBRE LAS PERSONAS FÍSICAS?		
<input type="checkbox"/> IMPOSIBILIDAD DE EJERCER ALGÚN DERECHO	<input type="checkbox"/> IMPOSIBILIDAD PARA ACCEDER A UN SERVICIO	<input type="checkbox"/> USURPACIÓN DE IDENTIDAD
<input type="checkbox"/> SER VÍCTIMA DE CAMPAÑAS DE PHISHING / SPAMMING	<input type="checkbox"/> PÉRDIDAS FINANCIERAS	<input type="checkbox"/> DAÑOS REPUTACIONALES
<input type="checkbox"/> PÉRDIDA DE CONFIDENCIALIDAD DE DATOS AFECTADOS POR SECRETO PROFESIONAL	<input type="checkbox"/> DAÑOS PSICOLÓGICOS O FÍSICOS	<input type="checkbox"/> PÉRDIDA DE CONTROL SOBRE SUS DATOS PERSONALES
<input type="checkbox"/> OTRAS CONSECUENCIAS	<input type="checkbox"/> AÚN DESCONOCIDO	
¿EN QUÉ GRADO PODRÍAN AFECTAR LAS CONSECUENCIAS IDENTIFICADAS A LAS PERSONAS FÍSICAS?		
<input type="radio"/> LAS PERSONAS PUEDEN ENFRENTAR CONSECUENCIAS MUY SIGNIFICATIVAS, O INCLUSO IRREVERSIBLES, QUE NO PUEDEN SUPERAR (EXCLUSIÓN O MARGINACIÓN SOCIAL, DIFICULTADES FINANCIERAS TALES COMO DEUDAS CONSIDERABLES O INCAPACIDAD PARA TRABAJAR, DOLENCIA PSICOLÓGICA O FÍSICA A LARGO PLAZO, MUERTE, ETC.), DAÑA DERECHOS FUNDAMENTALES Y LIBERTADES PÚBLICAS DE FORMA IRREVERSIBLE		
<input type="radio"/> LAS PERSONAS PUEDEN ENCONTRAR INCONVENIENTES IMPORTANTES, PRODUCIENDO UN DAÑO LIMITADO, QUE PODRÁN SUPERAR A PESAR DE ALGUNAS DIFICULTADES (COSTOS ADICIONALES, DENEGACIÓN DE ACCESO A SERVICIOS COMERCIALES, MIEDO, FALTA DE COMPRENSIÓN, ESTRÉS, DOLENCIAS FÍSICAS MENORES, ETC.)		
<input type="radio"/> LAS PERSONAS NO SE VERÁN AFECTADAS O PUEDEN ENCONTRAR ALGUNOS INCONVENIENTES MUY LIMITADOS Y REVERSIBLES QUE SUPERARÁN SIN NINGÚN PROBLEMA (TIEMPO DE REINGRESO DE INFORMACIÓN, MOLESTIAS, IRRITACIONES, ETC.)		
<input type="radio"/> LAS PERSONAS PUEDEN ENFRENTAR CONSECUENCIAS SIGNIFICATIVAS, QUE DEBERÍAN PODER SUPERAR AUNQUE CON SERIAS DIFICULTADES (MALVERSACIÓN DE FONDOS, LISTAS NEGRAS DE LOS BANCOS, DAÑOS A LA PROPIEDAD, PÉRDIDA DE EMPLEO, CITACIÓN JUDICIAL, EMPORRAMIENTO DE LA SALUD, ETC.), EN GENERAL CUANDO LAS CONSECUENCIAS AFECTAN A DERECHOS FUNDAMENTALES, PERO PUEDEN REVERTIRSE		
<input type="radio"/> AÚN DESCONOCIDO		
A FECHA DE ESTA NOTIFICACIÓN, ¿TIENE CONSTANCIA DE QUE SE HAYA MATERIALIZADO ALGUNO DE LAS CONSECUENCIAS IDENTIFICADAS, CON EL GRADO INDICADO EN LA CUESTIÓN ANTERIOR?		
<input type="radio"/> SÍ	<input type="radio"/> NO	
SI AÚN NO SE HA MATERIALIZADO ¿CÓMO VALORA LA PROBABILIDAD DE QUE SE MATERIALICE SOBRE LAS PERSONAS AFECTADAS?		
<input type="radio"/> IMPROBABLE	<input type="radio"/> BAJA	<input type="radio"/> ALTA
<input type="radio"/> MUY ALTA	<input type="radio"/> DESCONOCIDA	

FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES

USO EXCLUSIVO PARA ENTIDADES NO OBLIGADAS A RELACIONARSE CON LA ADMINISTRACIÓN POR MEDIOS ELECTRONICOS O CUANDO NO ESTÉN DISPONIBLES DICHOS MEDIOS ELECTRONICOS

RESUMEN DE LA BRECHA. BREVE DESCRIPCIÓN DE LO OCURRIDO Y LAS MEDIDAS CONCRETAS TOMADAS PARA MINIMIZAR EL DAÑO SOBRE LAS PERSONAS. DEBE INCLUIR DATOS PERSONALES Y FÓRMULAS DEL TIPO "un email". EN NINGÚN CASO LO AQUÍ ESCRITO PODRÁ SUPONER UNA MODIFICACIÓN SOBRE LO CONSIGNADO EN EL RESTO DEL FORMULARIO.

7. TIPOS DE DATOS AFECTADOS

SELECCIONE LOS TIPOS DE DATOS QUE SE HAN VISTO AFECTADOS, EXCLUSIVAMENTE DE PERSONAS FÍSICAS, MARQUE TODAS LAS OPCIONES APLICABLES		
<input type="checkbox"/> BIOMÉTRICOS	<input type="checkbox"/> DATOS BÁSICOS (EJ: NOMBRE, APELLIDOS, FECHA NACIMIENTO)	<input type="checkbox"/> SOBRE RELIGIÓN O CREENCIA
<input type="checkbox"/> IMAGEN (FOTOS / VIDEO)	<input type="checkbox"/> DNI, NIE, PASAPORTE O CUALQUIER DOCUMENTO IDENTIFICATIVO	<input type="checkbox"/> SOBRE CONDENAS E INFRACCIONES PENALES
<input type="checkbox"/> SOBRE AFILIACIÓN SINDICAL	<input type="checkbox"/> DATOS ECONÓMICOS O FINANCIEROS (SIN MEDIOS DE PAGO)	<input type="checkbox"/> DATOS DE MEDIOS DE PAGO (TARJETA BANCARIA, ETC.)
<input type="checkbox"/> SOBRE LA VIDA SEXUAL	<input type="checkbox"/> DATOS DE LOCALIZACIÓN / GEOLOCALIZACIÓN	<input type="checkbox"/> DATOS DE CONTACTO
<input type="checkbox"/> SOBRE ORIGEN RACIAL O ÉTNICO	<input type="checkbox"/> DATOS DE PERFILES (EJ: EN RED SOCIAL, SOLVENCIA, PSICOLÓGICO, ETC.)	<input type="checkbox"/> DATOS DE SALUD (UNICAMENTE DE EMPLEADOS, LOS IMPRESCINDIBLES PARA RELACIÓN LABORAL)
<input type="checkbox"/> DATOS DE SALUD (OTROS DATOS DE SALUD)	<input type="checkbox"/> SOBRE OPINIÓN POLÍTICA	<input type="checkbox"/> GENÉTICOS
<input type="checkbox"/> CREDENCIALES DE ACCESO O IDENTIFICACIÓN (USUARIO Y/O CONTRASEÑA)		

8. PERFIL DE LAS PERSONAS AFECTADAS

Referido exclusivamente a personas físicas. En términos de afectados no computan como tal aquellos que sean personas jurídicas, ya sean clientes, proveedores o cualquier otra relación que pueda mantener el responsable de tratamiento con ellos.

ENTRE LAS PERSONAS AFECTADAS, ¿HAY MENORES?		
<input type="radio"/> SÍ	<input type="radio"/> NO	<input type="radio"/> DESCONOCIDO
ENTRE LAS PERSONAS AFECTADAS, ¿HAY MIEMBRO DE COLECTIVOS VULNERABLES COMO SUPERVIVIENTES DE VIOLENCIA DE GÉNERO O EN RIESGO DE EXCLUSIÓN SOCIAL?		
<input type="radio"/> SÍ	<input type="radio"/> NO	<input type="radio"/> DESCONOCIDO

LAS PERSONAS AFECTADAS TIENEN LOS SIGUIENTES PERFILES:

CLIENTES / CIUDADANOS ESTUDIANTES / ALUMNOS USUARIOS

PACIENTES SUSCRIPTORES / POTENCIALES CLIENTES AFILIADOS / ASOCIADOS

MILITARES / POLICIAS EMPLEADOS OTROS

EN TOTAL, ¿CUÁNTAS PERSONAS HAN VISTO SUS DATOS AFECTADOS POR LA BRECHA?
(SI DESCONOCE EL VALOR EXACTO, INDIQUE UN VALOR APROXIMADO) (INDIQUE UNA CIFRA SUPERIOR A CERO)

9. IMPLICACIONES TRANSFRONTERIZAS

¿HAY PERSONAS AFECTADAS POR LA BRECHA EN OTROS ESTADOS MIEMBRO DE LA UNIÓN EUROPEA?

SÍ NO DESCONOCIDO

EN SU CASO, INDIQUE LOS ESTADOS EN LOS QUE HAYA PERSONAS AFECTADAS (A), EL NÚMERO DE AFECTADOS POR ESTADO Y AQUELLOS ESTADOS EN LOS QUE HAYA NOTIFICADO (N) A OTRA AUTORIDAD DE CONTROL

ESTADO	(A)	(N)	NÚMERO AFECTADOS	ESTADO	(A)	(N)	NÚMERO AFECTADOS
ALEMANIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	ITALIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
BULGARIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	LUXEMBURGO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
DINAMARCA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	POLONIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
ESLOVENIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	RUMANÍA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
IRLANDA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	BÉLGICA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
LITUANIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	CROACIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
PAÍSES BAJOS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	ESLOVAQUIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
REPÚBLICA CHECA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	FINLANDIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
AUSTRIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	HUNGRÍA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
CHIPRE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	LETONIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
FRANCIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	MALTA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
ESTONIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	PORTUGAL	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
GRECIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	SUECIA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>

10. INFORMACIÓN TEMPORAL DE LA BRECHA

INDIQUE LA FECHA DE DETECCIÓN DE LA BRECHA, ENTENDIDA COMO LA FECHA EN LA QUE EL RESPONSABLE TIENE CONSTANCIA DE QUE SE HAN VISTO AFECTADOS DATOS PERSONALES

¿CONOCE LA FECHA EN LA QUE SE INICIÓ LA BRECHA? EN SU CASO, INDIQUE LA FECHA

LA FECHA EXACTA APROXIMADA / ESTIMADA DESCONOCIDA

LA BRECHA SE HA DETECTADO MEDIANTE

MEDIOS DE DETECCIÓN IMPLEMENTADOS PROACTIVAMENTE POR EL RESPONSABLE O ENCARGADO LA ADVERTENCIA DE ALGÚN MIEMBRO DE LA ORGANIZACIÓN DEL RESPONSABLE O EL ENCARGADO COMUNICACIÓN DE ALGÚN AFECTADO

ALGÚN MEDIO DE COMUNICACIÓN UN TERCERO AJENO OTROS

11. MEDIDAS DE SEGURIDAD ANTES DE LA BRECHA

MARQUE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS EN LA ORGANIZACIÓN ANTES DEL SUCESO DE LA BRECHA (DEBERÁ PODER ACREDITAR LAS MEDIDAS INDICADAS ANTE UN EVENTUAL REQUERIMIENTO DE LA AUTORIDAD DE CONTROL)

POLÍTICAS DE PROTECCIÓN DE DATOS Y SEGURIDAD FORMACIÓN EN PROTECCIÓN DE DATOS Y SEGURIDAD AL NIVEL ADECUADO SISTEMAS DE INFORMÁTICOS ACTUALIZADOS

REGISTRO DE INCIDENTES AUDITORÍAS PERIÓDICAS CONTROL DE ACCESO FÍSICO

CONTROL DE ACCESO LÓGICO NIVELES DE ACCESO A LOS DATOS CIFRADO DE LOS DATOS

COPIA DE SEGURIDAD ANONIMIZACIÓN NINGUNA DE LAS ANTERIORES

¿SE PODRÍA HABER EVITADO LA BRECHA ADOPTANDO ALGUNA MEDIDA DE SEGURIDAD ADICIONAL?

SÍ NO DESCONOCIDO

¿SE HA PRODUCIDO EL INCIDENTE POR UN FALLO, DEFICIENCIA O INCUMPLIMIENTO DE LAS MEDIDAS IMPLEMENTADAS?

SÍ NO DESCONOCIDO

¿DISPONE DE UN ANÁLISIS DE RIESGOS DOCUMENTADO QUE JUSTIFIQUE LAS MEDIDAS DE SEGURIDAD ADOPTADAS PREVIAMENTE AL INCIDENTE?

SÍ NO

12. ACCIONES TOMADAS TRAS EL INCIDENTE

EN SU CASO, ¿HA ACTUALIZADO EL REGISTRO DE INCIDENTES CON LA INFORMACIÓN DE ESTA BRECHA DE DATOS PERSONALES?

SÍ NO DESCONOCIDO

EN SU CASO, ¿HA ADOPTADO TRAS EL INCIDENTE NUEVAS MEDIDAS DE SEGURIDAD QUE PODRÍAN HABER EVITADO LA BRECHA?

SÍ NO DESCONOCIDO

EN SU CASO, ¿HA ADAPTADO / MEJORADO SUS PROCEDIMIENTOS Y POLÍTICAS DE SEGURIDAD?

SÍ NO DESCONOCIDO

EN SU CASO, MARQUE EXCLUSIVAMENTE LAS NUEVAS MEDIDAS DE SEGURIDAD O LAS QUE SE HAYAN ACTUALIZADO

POLÍTICAS DE PROTECCIÓN DE DATOS Y SEGURIDAD FORMACIÓN EN PROTECCIÓN DE DATOS Y SEGURIDAD AL NIVEL ADECUADO SISTEMAS DE INFORMÁTICOS ACTUALIZADOS

REGISTRO DE INCIDENTES AUDITORÍAS PERIÓDICAS CONTROL DE ACCESO FÍSICO

CONTROL DE ACCESO LÓGICO NIVELES DE ACCESO A LOS DATOS CIFRADO DE LOS DATOS

COPIA DE SEGURIDAD ANONIMIZACIÓN NINGUNA DE LAS ANTERIORES

EN SU CASO, ¿HA PUESTO EL INCIDENTE EN CONOCIMIENTO DE LAS AUTORIDADES POLICIALES / JUDICIALES POR CONSIDERAR QUE ES CONSTITUTIVO DE DELITO?

SÍ NO

¿CONSIDERA QUE HA TOMADO TODAS LAS ACCIONES POSIBLES Y DA POR RESUELTA LA BRECHA?

SÍ NO DESCONOCIDO

EN SU CASO, INDIQUE LA FECHA EN LA QUE SE DIO POR RESUELTA LA BRECHA

13. COMUNICACIÓN A LOS AFECTADOS

La comunicación de la brecha a los afectados debe ser en un lenguaje claro y sencillo, incluir detalles de su ocurrencia, así como los datos de contacto a dónde dirigirse para obtener más información, las posibles consecuencias de la brecha sobre ellos, las medidas adoptadas para resolver la brecha y las medidas adoptadas y propuestas para minimizar el impacto negativo de la brecha.

¿ SE HA COMUNICADO LA BRECHA A LAS PERSONAS AFECTADAS EN LOS TÉRMINOS ANTERIORMENTE DESCRITOS?	
<input type="radio"/> SÍ	<input type="radio"/> NO, PERO SERÁN COMUNICADOS
<input type="radio"/> NO SERÁN INFORMADOS	<input type="radio"/> PENDIENTE DE DECIDIR
EN SU CASO, FECHA EN LA QUE SE COMUNICÓ O SE TIENE PREVISTO COMUNICAR	
<input type="text"/>	
EN SU CASO, NÚMERO DE PERSONAS COMUNICADAS O QUE SE TIENE PREVISTO COMUNICAR	
<input type="text"/>	
EN SU CASO, MEDIO DE COMUNICACIÓN UTILIZADO O PREVISTO	
<input type="checkbox"/> TELEFÓNICA O VERBALMENTE	<input type="checkbox"/> COMUNICACIÓN DIRIGIDA PERSONALMENTE A CADA AFECTADO (POSTAL, EMAIL, SMS O SIMILAR)
<input type="checkbox"/> COMUNICADO PÚBLICO O PUBLICACIÓN EN WEB CORPORATIVA	<input type="checkbox"/> COMUNICACIÓN DIRIGIDA PERSONALMENTE A CADA AFECTADO (POSTAL, EMAIL, SMS O SIMILAR) CON GARANTÍA DE ENTREGA Y LECTURA
<input type="checkbox"/> DIFUSIÓN EN MEDIOS DE COMUNICACIÓN	
EN SU CASO, LAS PERSONAS AFECTADAS NO SERÁN INFORMADAS PORQUE	
<input type="radio"/> NO EXISTE UN RIESGO ALTO PARA SUS DERECHOS Y LIBERTADES	<input type="radio"/> NO HAY NINGUNA ACCIÓN QUE PUEDAN LLEVAR A CABO PARA MITIGAR LOS DAÑOS
<input type="radio"/> DAÑO REPUTACIONAL PARA LA ORGANIZACIÓN SERÍA MUY ELEVADO	<input type="radio"/> LA COMUNICACIÓN SUPONE UN ESFUERZO EXCESIVO
<input type="radio"/> NO INTERFERIR EN UNA INVESTIGACIÓN POLICIAL / JUDICIAL EN CURSO	<input type="radio"/> OTROS

14. DOCUMENTACIÓN ADJUNTA

No es necesario adjunta más documentación que los datos solicitados en este formulario. De así considerarlo, la Autoridad de Control le requerirá la información adicional necesaria.

SE ADJUNTA DOCUMENTACIÓN ACREDITATIVA DE LA REPRESENTACIÓN DEL RESPONSABLE O SU AUTORIZACIÓN PARA NOTIFICAR LA BRECHA DE DATOS PERSONALES A LA AUTORIDAD DE CONTROL.

15. NOTIFICACIÓN COMPLETA O POR FASES

<p>MARQUE LA OPCIÓN MÁS ADECUADA A LA SITUACIÓN DEL RESPONSABLE EN EL MOMENTO DE LA NOTIFICACIÓN</p> <p><input type="radio"/> ESTA NOTIFICACIÓN CONTIENE TODA LA INFORMACIÓN QUE COMO RESPONSABLE SE HA PODIDO RECARBAR RESPECTO A LA BRECHA DE SEGURIDAD. A TODOS LOS EFECTOS, LA AUTORIDAD DE CONTROL PUEDE CONSIDERAR ESTA NOTIFICACIÓN COMO COMPLETA Y NO ESTÁ PREVISTO APORTAR MÁS INFORMACIÓN.</p> <p><input type="radio"/> ESTA NOTIFICACIÓN ES INICIAL A LOS EFECTOS DE CUMPLIMIENTO CON EL PLAZO DE NOTIFICACIÓN ESTABLECIDO EN EL RGPD. EN EL MÁXIMO DE 30 DÍAS SE NOTIFICARÁ INFORMACIÓN ADICIONAL. EN CASO CONTRARIO, LA AUTORIDAD DE CONTROL CONSIDERARÁ ESTA NOTIFICACIÓN COMO COMPLETA.</p>
--

Cláusula informativa sobre protección de datos:

Los datos de carácter personal serán tratados por la Agencia Española de Protección de Datos e incorporados a la actividad de tratamiento Gestión de brechas de seguridad, cuya finalidad es la gestión y evaluación de la notificación de violación de seguridad.

Finalidad basada en el cumplimiento de obligaciones legales que el Reglamento General de Protección de Datos/la Ley General de Telecomunicaciones impone a la Agencia Española de Protección de Datos.

Los datos personales podrán ser comunicados al CERT (Computer Emergency Response Team) del Centro Criptológico Nacional, a las Fuerzas y Cuerpos de Seguridad del Estado, al Comité Europeo de Protección de Datos, a las Autoridades de Protección de Datos de la Unión Europea, y a la red de equipos de respuesta a incidentes de seguridad informática («red de CSIRT», por sus siglas en inglés de «computer security incident response teams»), creada por

Responsabilidad civil





Roj: **SAP S 1527/2023 - ECLI:ES:APS:2023:1527**

Id Cendoj: **39075370022023100649**

Órgano: **Audiencia Provincial**

Sede: **Santander**

Sección: **2**

Fecha: **24/11/2023**

Nº de Recurso: **358/2022**

Nº de Resolución: **609/2023**

Procedimiento: **Recurso de apelación. Juicio ordinario**

Ponente: **LAURA CUEVAS RAMOS**

Tipo de Resolución: **Sentencia**

AUDIENCIA PROVINCIAL SECCION 2 de Santander

Apelaciones juicios ordinarios 0000358/2022

NIG: 3907542120200007801

AP004

Avda Pedro San Martin S/N Santander Tfno: 942357123 Fax: 942357142

JUZGADO DE PRIMERA INSTANCIA Nº 4 de Santander de Santander Procedimiento Ordinario

0000629/2020 - 0

Puede relacionarse telemáticamente con esta

Admón. a través de la sede electrónica.

(Acceso Vereda para personas jurídicas)

<https://sedejudicial.cantabria.es/>

SENTENCIA nº 000609/2023

Los ciberataques acercan al Ibx y la clave está en el eslabón más débil de sus defensas: sus proveedores

Ayer, Iberdrola trasladó a 650.000 clientes que había sufrido un ciberataque, un día después de que trascendiera la filtración de datos de 120.000 clientes de Telefónica



2 comentarios



Responsabilidad administrativa

De las actuaciones de investigación se desprende que, con anterioridad a la brecha de seguridad, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados, en abril del 2018 se aprobó la realización de las auditorías de cumplimiento del RGPD y se definió un Plan de Auditorías que cubriera a todas las entidades MAPFRE sujetas al RGPD e incluso se han reforzado estas medidas con motivo de la situación de pandemia, que exige posibilitar el trabajo remoto a gran parte de la plantilla.

Es reseñable que la empresa ha participado activamente la elaboración, de la “Guía para el tratamiento de los datos personales por aseguradoras” elaborada por UNESPA que, aunque no es un código de conducta, si es un mecanismo de autorregulación y contempla la necesidad de cumplir con una serie de principios específicos en materia de privacidad y protección de datos.

En cuanto al impacto, los datos que se han visto vulnerados han sido, el identificador de usuario y contraseña de acceso a los sistemas de información de MAPFRE, que tratándose datos básicos, no tienen aplicación fuera del entorno de sistemas de MAPFRE y quedaron inutilizados tras su bloqueo y el cambio de contraseñas asociadas a los mismos.

El volumen de Datos se encuentra en el rango de menos de 100 y el impacto ha sido casi nulo, pues los intentos de exfiltración fueron detectados y evitados, lo que unido a la rapidez para hacer público el ciberataque permitió la eficaz actuación de clientes, trabajadores, colaboradores y proveedores, minimizando los efectos del ciberataque. No constan reclamaciones ante esta Agencia por parte de terceros.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, lo que ha permitido la rápida identificación, análisis y clasificación de la brecha de seguridad de datos personales.

Por lo que respecta a su actuación tras la identificación de la amenaza, cabe calificarla, como de diligente reacción, con una rápida notificación tanto al Incibe como al CCN-CERT y a la Guardia Civil, así como una serie de notificaciones sobre la evolución de la incidencia a la AEPD, junto a una rápida comunicación con clientes, colaboradores, proveedores y empleados que posibilitó una eficaz reacción contra el ataque.

En relación con las medidas adoptadas para minimizar el impacto y eliminar las posibles lagunas en la seguridad que hubiese dejado el ataque, se procedió a la ejecución del Plan de Fortificación del entorno *****ENTORNO.1.**

Responsabilidad penal



Conclusiones



¡Muchas gracias! 😊

✉ andonigarcia@seinale.com
www.seinale.com

