

#1.2 - DETECCIÓN Y COMUNICACIÓN DE BRECHAS



Eric Serrano Marín

CETI Normativa de Ciberseguridad

INDICE

1. Eres el responsable de datos de una empresa.....	2
2. Documentar y simular los pasos de resolución en la herramienta Comunica-Brecha AEPD de una hipotética brecha de seguridad producida en los datos personales de los empleados ayer y que permitan concluir que finalmente debe ser notificada a la Autoridad de Control. Detallar capturas de pantalla generadas que señalen los detalles sobre la brecha de seguridad, origen del incidente o la naturaleza del mismo, etc.	3
3. Utiliza la sede electrónica de la AEPD para rellenar el formulario que permita comunicar este incidente sin presentar finalmente la solicitud.	6

1. Eres el responsable de datos de una empresa.

Indicar en tu respuesta:

- Nombre y sector de la actividad a que se dedica
 - Salud+, es una empresa que se dedica a la sanidad, más en concreto es una consulta privada.
- Tareas, funciones o proyectos desempeñados
 - Evaluación y Diagnóstico, Atención Preventiva, Especialidades Médicas, Análisis Clínicos, Servicios de Telemedicina, Atención a Enfermedades Crónicas, Cuidado Maternal y Prenatal, Atención Geriátrica, Rehabilitación Física, Programas de Bienestar y Educación para la Salud.
- Número de empleados
 - 20 empleados.
- Ubicación en el mapa y datos de contacto
 - Nombre de la empresa: Salud+
Dirección de la Oficina: 123 Calle de la Salud Rubí,
Barcelona, 08191
Teléfono principal: (555)123-4567 Correo
Electrónico: info@saludplus.com Sitio Web:
www.saludplus.com
Redes Sociales: @saludplus

➤ Ubicación en el mapa



2. Documentar y simular los pasos de resolución en la herramienta Comunica-Brecha AEPD de una hipotética brecha de seguridad producida en los datos personales de los empleados ayer y que permitan concluir que finalmente debe ser notificada a la Autoridad de Control. Detallar capturas de pantalla generadas que señalen los detalles sobre la brecha de seguridad, origen del incidente o la naturaleza del mismo, etc.

El sector de nuestra empresa es Sanidad.

Sobre el responsable

Indique el sector de actividad del responsable de tratamiento: *

En mi caso, una persona entró a robar en la consulta.

Sobre la brecha de seguridad de los datos personales

El incidente ha sido: *

- ☐ Accidental o sin intencionalidad
- ☒ Intencionado
- ☐ Desconocido

El origen del incidente ha sido: *

- ☐ Interno: Personal o sistemas del responsable de tratamiento
- ☐ Interno: Personal o sistemas del encargado de tratamiento
- ☒ Externo: Otros, ajenos al responsable y encargado de tratamiento

¿La brecha de seguridad es consecuencia de un ciberincidente?: *

- ☐ Sí
- ☒ No

La persona que entró a robar, se llevó cajas con papeles con información personal de los pacientes y sus problemas de salud.

Como consecuencia del incidente: *

- ☒ Personas u organizaciones que no están autorizadas, o no tienen un propósito legítimo para acceder a los datos, han podido acceder y/o extraerlos.
- ☐ Se han destruido, perdido o cifrado datos personales, de forma que no pueden ser tratados.
- ☐ Se han alterado los datos personales y el tratamiento con datos alterados/inexactos puede suponer un daño para los afectados.

Referido específicamente a los datos afectados. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso o no se puede identificar a las personas? *

- ☐ Sí
- ☒ No
- ☐ Desconocido

El grado en el que podría afectar a las personas es desconocido.

¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas afectadas?: *

- ☐ 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, dolencias psicológicas o físicas a largo plazo, muerte, etc.). Daño derechos fundamentales y libertades públicas de forma irreversible.
- ☐ 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, empeoramiento de la salud, etc.). En general cuando las consecuencias afectan a derechos fundamentales, pero pueden revertirse.
- ☐ 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.)
- ☐ 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.)
- ☒ Aún desconocido

Los tipos de datos afectados van desde datos básicos, DNI... hasta de salud.

Tipos de datos afectados

Seleccione los tipos de datos que se han visto afectados, exclusivamente de personas físicas, marque todas las opciones aplicables: *

- ☒ Datos básicos (Ej: nombre, apellidos, fecha de nacimiento)
- ☒ Documento identificativo (Ej: DNI, NIE, pasaporte)
- ☒ Datos de contacto (Ej: teléfono, email, dirección postal)
- ☒ Datos de localización (Ej: geolocalización)
- ☐ Credenciales de acceso o identificación (Ej: usuario y/o contraseña)
- ☐ Sobre religión o creencia
- ☐ Sobre la vida sexual
- ☒ De salud (exclusivamente de empleados, los imprescindibles para relación laboral)
- ☐ Sobre opinión política
- ☐ Sobre condenas e infracciones penales
- ☒ Imagen y/o audio (Ej: fotografía, vídeo, grabaciones)
- ☐ Datos económicos o financieros (sin medios de pago)
- ☐ Datos de medios de pago (Ej: tarjeta bancaria)
- ☐ Datos de perfiles (Ej: perfil en red social, perfil de solvencia patrimonial, perfil psicológico, etc)
- ☐ Biométricos
- ☐ Sobre afiliación sindical
- ☐ Sobre el origen racial o étnico
- ☒ De salud (otros datos de salud)
- ☒ Genéticos

En cuanto al perfil de afectados, a nuestra clínica vienen personas de todas las edades y colectivos vulnerables.

Perfil de los afectados, referido exclusivamente a personas físicas

Entre las personas afectadas, ¿hay menores?: *

- ☒ Sí
- ☐ No
- ☐ Desconocido

Entre las personas afectadas, ¿hay miembros de colectivos vulnerables como víctimas de violencia de género o en riesgo de exclusión social?: *

- ☒ Si
- ☐ No
- ☐ Desconocido

En total, ¿cuántas personas han visto sus datos afectados por la brecha de seguridad? (Si desconoce el valor exacto, indique un número aproximado/estimado): *

1500

Vamos a decir que estoy rellenando el cuestionario el mismo día en el que he sido robado. Así que vamos a poner que conocemos la fecha exacta y que ha sido hoy.

Información temporal de la brecha

Indique la fecha de detección de la brecha, entendida como la fecha en la que el responsable tiene la certeza de que se han visto afectados datos personales: *

31/10/2023

¿Conoce la fecha en la que se inició la brecha?: *

- ☒ La fecha exacta
☐ Aproximadamente / Estimada
☐ Desconocida

Indique la fecha de inicio de la brecha: *

31/10/2023

3. Utiliza la sede electrónica de la AEPD para rellenar el formulario que permita comunicar este incidente sin presentar finalmente la solicitud.

Y el resultado ha sido el siguiente: Sí, deberíamos comunicar la brecha de seguridad a los afectados conforme al art.34 del RGPD.

Resultado

Según los datos facilitados,

DEBERÍA COMUNICAR LA BRECHA DE SEGURIDAD A LOS AFECTADOS

conforme al art. 34 del RGPD al apreciarse que puede existir un riesgo alto o muy alto para los derechos y libertades de los sujetos afectados por la brecha de seguridad.

Si la comunicación a los afectados supone un esfuerzo desproporcionado, podrá optar por una comunicación pública o medida semejante por la que se informe de manera igualmente efectiva a los interesados, en virtud del artículo 34.2c del RGPD.

Anterior

Siguiente