"Hablamos de Datos", un podcast de la Escuela de Administración Pública de Cataluña y la Autoridad Catalana de Protección de Datos.

Capítulo 4: Cuestiones prácticas sobre las violaciones de seguridad de los datos.

¡Buenos días! En este cuarto capítulo de "Hablemos de datos", analizaremos un aspecto clave para los responsables del tratamiento de datos personales: las violaciones de seguridad de los datos. ¿Qué es una violación de datos en términos del Reglamento general de protección de datos? ¿Cómo debe actuar nuestra organización, cuando sufre una? En el tiempo que dura este pódcast, intentaremos resumir los pasos clave que hay que llevar a cabo en las 72 horas que marca la normativa.

Para ello, nos acompaña la Olga Rierola. L'Olga es coordinadora de la unidad de gestión de notificaciones de violaciones de seguridad de la Autoridad Catalana de Protección de Datos. Hola, Olga, y bienvenida!

Hola, ¡muchas gracias!

¡Muy bien! Empecemos, pues. Si hablamos de violaciones de la seguridad de los datos, ¿quiere decir que ya se ha producido un incidente y, por tanto, que algo ha fallado, verdad?

Efectivamente, todos sabemos que las medidas de seguridad no son 100% infalibles, y que las violaciones de datos se pueden producir. En este sentido, el Reglamento europeo exige a las organizaciones tener implementadas medidas y procedimientos para que, en caso de que sucedan, podamos reaccionar de manera adecuada. Esto incluye: detectarla y contenerla rápidamente, analizar los riesgos que supone para los titulares de los datos y determinar rápidamente si es necesario notificar la violación a la Autoridad e, incluso, si es necesario comunicarla a las personas afectadas.

En definitiva, las obligaciones sobre violaciones de datos previstas en el Reglamento tienen como objetivo proteger a las personas y evitar que este hecho pueda causarles daños. Por ello, debemos asegurarnos de que nuestra organización dispone de un plan de respuesta robusto para hacer frente a cualquier violación de seguridad, asignar su gestión a una persona o equipo de la organización y que todo el personal esté informado de ello.

Por lo tanto, queda claro que hay que estar preparados para abordar rápidamente una violación de la seguridad de los datos. Para ello, lo primero que nos hace falta es saber reconocerla.

Así es, primero de todo hay que identificarla. Para ello debemos ir a la definición del Reglamento, que establece que una violación de la seguridad de los datos es cualquier incidente de seguridad que ocasiona la destrucción accidental o ilícita, la pérdida, la alteración, la divulgación o el acceso no autorizado a los datos personales, tanto en formato papel como en digital.

En resumen, es cualquier incidente que compromete la seguridad de los datos. Por lo tanto, estas violaciones se pueden clasificar en tres tipos. En primer lugar, nos encontraremos ante una violación de la confidencialidad cuando alguien que no debía tiene o puede tener acceso a los datos; un ejemplo típico es el envío de datos personales a un destinatario erróneo, o bien el robo de un dispositivo móvil con datos personales. En segundo lugar, nos encontraremos ante una violación de la integridad cuando alguien que no debía modifica o cambia los datos; un ejemplo es la suplantación de identidad, lo que conocemos como phishing. Y, por último, nos encontraremos ante una violación de la disponibilidad cuando hay una pérdida de acceso a los datos. Esta pérdida puede ser tan temporal, si por ejemplo fallan los sistemas de un hospital y las bases de datos médicas no están disponibles durante unas horas, como definitiva, si sufrimos una infección por ransomware que encripta los datos y no tenemos copia de seguridad.

Por lo tanto, entendemos que es cualquier incidente de seguridad que afecta a los datos personales y que puede tener tanto un origen accidental como deliberado.

Efectivamente, en términos del Reglamento, es una violación tanto el hecho de que un trabajador envíe accidentalmente un correo con datos personales a la persona equivocada, como si lo hace deliberadamente. También lo es tanto si un hacker accede a los datos, como si los datos quedan al descubierto por un error de configuración. De hecho, gran parte de las violaciones que se notifican a la Autoridad tienen como origen errores humanos. De ahí, pues, la importancia primordial de la formación constante del personal, también en materia de ciberseguridad, para evitar caer en trampas.

Hay que tener en cuenta también, que una violación de datos es siempre una violación en términos del Reglamento, aunque no implique daños o perjuicios para las personas titulares de los datos. Un ejemplo sería una supresión accidental de datos si se dispone de copia de seguridad y se han podido recuperar rápidamente, o un corte breve de energía que, por unas horas, impide la prestación de servicios no esenciales. Como hemos visto, la definición de violaciones de datos no nos habla de riesgo. El riesgo aparece en las obligaciones que se derivan para los responsables, como ahora veremos.

Muy bien, ahora que ya somos capaces de reconocer una violación de los datos, ¿cómo debemos actuar cuando detectamos que hemos sufrido una?

Vamos! Intentaré resumirlo en 6 pasos, pero antes quiero resaltar algunas cuestiones, si me permites.

La primera es que, una vez que el responsable detecta que se ha producido una violación de datos, el reloj empieza a correr y la normativa establece que tenemos 72 horas para notificarlo. Sin embargo, puede ser que finalmente no lo tengamos que acabar haciendo porque, como hemos visto, no todas las violaciones implican daños o perjuicios para los titulares de los datos.

La segunda cuestión que quiero remarcar es que, cuando detectamos una violación, hay que informar rápidamente a nuestro delegado de protección de datos, que es quien nos ayudará a gestionarla y tomar las decisiones oportunas. Será, además, quien actúe como interlocutor de la Autoridad, en su caso.

Por último, hay que tener en cuenta que, si bien es el responsable del tratamiento quien tiene las obligaciones que se deriven de la notificación ante la Autoridad, si la violación la sufre su encargado del tratamiento, como la empresa TIC a quien haya contratado la prestación de servicios en la nube, este encargado tiene la obligación de comunicarla en seguida al responsable.

Perfecto, dicho todo esto, vamos ahora a los 6 pasos clave.

Muy bien. El primer paso es intentar contener rápidamente la violación y limitar los posibles efectos adversos para los titulares de los datos. La prioridad debe ser proteger a las personas. Algunos de estos ejemplos pueden ser: recuperar rápidamente los datos eliminados indebidamente o que han sido encriptados por ransomware, cambiar las contraseñas en caso de ataques o contactar rápidamente con los destinatarios de los datos y pedirles que los eliminen.

Paralelamente, hay que seguir investigando los hechos para determinar su alcance.

Seguidamente, es necesario evaluar el riesgo de la violación para los derechos y libertades de las personas; es decir, hay que determinar la probabilidad de que la violación les ocasione daños y, si es así, de qué gravedad son. El nivel de riesgo o daño determinará, pues, las siguientes actuaciones del responsable.

Por lo tanto, en caso de que sea improbable que la violación comporte daños o consecuencias adversas para las personas, no será necesario notificarla a la Autoridad. Por ejemplo, si perdemos un USB con datos personales de los trabajadores, pero está cifrado de manera segura, la clave no está comprometida

y disponemos de copia de los datos, es poco probable que les cause daños, pues no hemos perdido el acceso a los datos, y el hecho de que estén protegidas con un nivel de cifrado adecuado hace que sean ininteligibles para personas no autorizadas.

Por el contrario, si es probable que la violación les ocasione daños, habrá que notificarla a la Autoridad, y hacerlo lo antes posible y en un plazo máximo de 72 horas. Sería el caso de que el USB no estuviera cifrado y cualquier persona no autorizada pudiera acceder a los datos, de manera que existe un riesgo de daño.

Además, si es probable que la violación comporte daños importantes para las personas, es decir, en caso de alto riesgo, como si el USB contuviera datos especialmente sensibles, será necesario también comunicarlo a los afectados. Y habrá que hacerlo rápidamente, para que puedan tomar las medidas necesarias para protegerse de estos posibles daños, siguiendo siempre las recomendaciones del responsable, como estar alerta ante posibles chantajes, cambiar las contraseñas en caso de ciberataque o verificar movimientos extraños de las cuentas, dependiendo del caso.

Por último, las organizaciones deben tomar las medidas correctoras necesarias para evitar, en la medida de lo posible, que se vuelva a producir un incidente similar. Y hay que documentar todas las violaciones al registro interno de violaciones, tanto las que hay que notificar a la Autoridad como las que no. En este registro, se deben incluir todos los hechos que estén relacionados, las medidas correctoras adoptadas y las decisiones tomadas, como la razón por la que se considera que es improbable que la violación cause daños a las personas titulares de los datos. Este registro debe estar siempre a disposición de la Autoridad, que puede tener que supervisarlo.

Perfecto. Ahora bien, no me ha quedado del todo claro cómo hay que evaluar el riesgo. ¿Hay alguna fórmula para hacerlo?

No, evaluar el riesgo es una tarea compleja, ya que como hemos dicho hay violaciones que no implican daños y otras que pueden tener múltiples consecuencias adversas sobre las personas. Es decir que pueden causarles daños que pueden ser tanto físicos, materiales como inmateriales.

De acuerdo con el Reglamento, estas consecuencias pueden ser la pérdida de control sobre sus datos personales, la restricción de sus derechos, la discriminación, la usurpación de identidad o fraude, pérdidas financieras, daño para la reputación o cualquier otra desventaja económica o social. Así pues, la probabilidad de que la violación ocasione alguno de estos efectos adversos sobre los titulares de los datos debe evaluarse caso por caso.

Hay que tener en cuenta que, en el caso de que la violación afecte a categorías especiales de datos, como opinión política, religión, afiliación sindical o datos de salud, es muy probable que estas consecuencias sean muy significativas, es decir que les ocasione daños importantes. Particularmente, se considera que nos encontraremos en situaciones de alto riesgo siempre que la violación pueda causar consecuencias como suplantaciones de identidad o fraude, daño físico, angustia psicológica o humillación para las personas. Como hemos dicho, hay que evaluarlo caso por caso, en función de las circunstancias concurrentes y considerando todos los factores relevantes.

¿Me puedes poner algunos ejemplos de estos factores?

Sí, y tanto. A la hora de evaluar el riesgo, o la probabilidad de que la violación ocasione daños o consecuencias adversas sobre las personas, y su gravedad, hay que tener en cuenta, por ejemplo, los factores siguientes: el tipo de violación sufrida, es decir, si afecta a la confidencialidad, la integridad o la disponibilidad de los datos, o cualquier combinación de las tres; la naturaleza, la sensibilidad, y el volumen de datos afectados; los colectivos a los que hacen referencia, aquí hay que tener especialmente en cuenta que el hecho de que la violación afecte a colectivos vulnerables, como menores, aumentará su riesgo potencial. Otro factor es el origen de la violación, es decir, si es accidental o deliberada. No es lo mismo que los datos se hayan enviado por error a una tercera persona, especialmente si es de confianza, que si están en manos de un hacker que no sabemos qué intenciones tiene. Finalmente, también hay que analizar la facilidad o dificultad con que los terceros no autorizados pueden identificar a los titulares de los datos afectados.

Y en caso de que haya que notificar la violación a la Autoridad, ¿cómo se debe hacer y qué información hay que proporcionar?

En la sede electrónica de la APDCAT podréis encontrar el formulario de notificación. Se debe incluir, entre otras, una descripción de la violación, cuando se ha producido, el tipo de datos y colectivos afectados, las posibles consecuencias adversas para las personas, si se ha comunicado o no a los afectados y las medidas que se han tomado. Esta información permitirá a la Autoridad analizar si el responsable ha actuado adecuadamente para hacer frente a la violación, y si no es así, la Autoridad le requerirá que lo haga sin dilación. También si considera que hay que comunicar la violación a las personas afectadas.

¿Qué pasa si en el plazo de 72 horas no disponemos todavía de toda la información?

Si el responsable no tiene toda la información, puede hacer la notificación por fases: una primera notificación inicial y, después, complementarla y justificar los motivos del retraso.

¿Tiene consecuencias el hecho de no notificar a la Autoridad una violación cuando es obligatorio hacerlo?

Sí, efectivamente. Puede dar lugar a sanciones económicas muy elevadas, aparte de perjudicar la reputación de quien haya sufrido la violación de seguridad y no lo notifique. Por lo tanto, ante la duda, es mejor notificarlo o bien consultarlo a la APDCAT.

Ya para cerrar, y teniendo en cuenta todo lo que hemos hablado hasta ahora, ¿qué consideras que es imprescindible para que una organización pueda hacer frente a una violación de la seguridad de los datos personales con garantías?

Como ya he dicho al principio, es indispensable disponer de antemano de un plan de respuesta que prevea todo los pasos que hay que hacer, y de qué manera se debe hacer. Este plan de respuesta debe tener como foco la protección de las personas.

Perfecto, muchas gracias por aclararnos todas las dudas.

¡A vosotros!

Y hasta aquí el cuarto capítulo de "Hablemos de datos personales", el pódcast de la Escuela de Administración Pública de Cataluña y la Autoridad Catalana de Protección de Datos. Hoy con la Olga Rierola, coordinadora de la unidad de gestión de notificaciones de violaciones de seguridad de la Autoridad Catalana de Protección de Datos, hemos aclarado qué hay que hacer en caso de una violación de la seguridad de los datos. Una situación que, como hemos visto, nunca podremos prevenir al 100%. Y es por ello que es clave saber cómo reaccionar, si se produce, y cómo evitar que nos vuelva a pasar en un futuro. Os esperamos en el próximo capítulo de "Hablemos de datos personales", donde continuaremos profundizando en aspectos relacionados con el tratamiento y la protección de datos. ¡Hasta pronto!