20200720, Nota Informativa, sobre cómo responder ante un incidente de seguridad.

En virtud de mis compromisos contractuales, seguidamente paso a informar de un protocolo básico para poder responder cuando suframos un incidente de seguridad. No obstante lo que sigue, recordar que cuando se produzca cualquier incidente de seguridad se me ha de comunicar a mí para poder decidir las medidas a tomar.

1. Prevención. En primer lugar debemos elaborar los protocolos de actuación y formar un equipo de responsables que van a gestionar los incidentes, son los denominados *"procedimientos de respuesta a incidentes".* Dentro de dichos protocolos, sería recomendable determinar aquellas vulnerabilidades más relevantes (análisis de riesgos) o si la gestión del incidente será interna o externa.

También se debe nombrar a las personas encargadas de actuar y la formación al resto de empleados que pueda prevenir en la medida de lo posible los ciberataques.

Esto es, debemos tener presentes las medidas de seguridad implantadas (contraseñas complejas en todos los equipos informáticos, copia con contraseña de los archivos de datos, programas antivirus completos y actualizados,…) y comunicarme a mí, como DPD, cualquier incidente que se produzca.

2. Detección, identificación y clasificación

Antes de aplicar cualquier tipo de protocolo, debemos detectar el incidente. Para ello se podrán utilizar indicadores como alertas, que el servicio vaya más lento de lo habitual o la caída de un servidor.

Identificado el incidente, se deberá clasificar en función de su gravedad y priorizar las actuaciones. En esta fase se debe determinar si se trata

de una brecha de los datos de carácter personal descrita en el RGPD, y el nivel de riesgo al que se enfrenta la organización (que va desde el nivel crítico que afecta a un importante número de datos siendo el ataque en muy poco tiempo, hasta el nivel bajo, con un riesgo mínimo) y clasificarlo en función de las posibles consecuencias.

Según la guía publicada por la Agencia Española de Protección de datos e INCIBE, una brecha de seguridad puede ser catalogada en tres categorías distintas,

Brecha de confidencialidad: Tiene lugar cuando partes que no están autorizadas, o no tienen un propósito legítimo para acceder a la información, acceden a ella.

Brecha de integridad: se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo

Brecha de disponibilidad: su consecuencia es que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal, o permanente (los datos no pueden recuperarse).

En esta fase se debe analizar, si la amenaza es externa o interna, el número y tipología de sistemas dañados y perfil de usuarios afectados, con todo ello se dará prioridad de actuación, si se hubiesen producido varios incidentes.

3. Notificación

Dicho procedimiento de notificación debe realizarse tanto internamente, a aquellas personas que puedan mitigar los daños, como externamente. El RGPD establece la obligación (art. 33) de notificar a la Autoridad de Control (en nuestro caso la AEPD) si se ha producido una brecha de seguridad de los datos personales. Dicha situación debe hacerse sin dilaciones indebidas, y de ser posible, en el plazo de 72

horas. En estos casos, en cuanto se tenga constancia del incidente, de forma inmediata se me debe comunicar para que valore la necesidad o no de notificarlo a la AEPD y para tomar las medidas adicionales que sean necesarias.

También se regulan los supuestos en los que se debe notificar a los afectados, en los casos en los que la brecha conlleve un alto riesgo para los derechos y libertades de las personas físicas. La forma de notificación a los afectados se determinará conforme a las circunstancias concretas y será obligación del responsable de tratamiento, aunque supervisada y siguiendo mis orientaciones como DPD.

4. Plan de actuación

En primer lugar se debe contener y frenar el incidente, con medidas como puede ser deshabilitar servicios o desconectar la red, se deberá pasar a la fase de recuperación de los sistemas.

Dentro de las actividades de resolución, tenemos actuaciones como la instalación de parches de seguridad o cambios en los cortafuegos. Como actividades de recuperación, se podrá restaurar información contenida en las copias de seguridad, cambios de contraseñas o el reemplazo de componentes afectados.

5. Seguimiento y cierre

Mitigado el incidente de seguridad, resulta recomendable documentar todas las actuaciones llevadas a cabo, incluso disponer de un *registro de incidentes,* con ello se deberán adoptar políticas de mejora, e identificar nuevos patrones que eviten nuevas brechas.

De hecho, y como hemos comentado en varias ocasiones, cualquier incidente relacionado con la protección de los datos personales, por

muy pequeño que sea, me debe ser comunicado, para poder determinar el alcance del mismo y dejarlo registrado.

Es muy improbable que se filtre la información acerca del incidente de seguridad, por lo que se deberá analizar el impacto mediático que va a tener para la compañía sólo en el caso de que éste se produzca. Para ello se deberá analizar la información filtrada en los medios de comunicación, ver las reacciones y valorar la posibilidad de emitir un comunicado oficial. Pero este supuesto, insisto, **es muy infrecuente**.

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho conforme a mi leal saber y entender, en Manilva a 20 de julio de 2020,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2020.07.20 08:48:58 +02'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)