La seguridad en los Sistemas Internos de Información

LINK DE LA NOTICIA

Fuente: Economist & Jurist

La Evaluación de Impacto de Protección de Datos debe contemplar todos y cada uno de estos aspectos de seguridad.

La selección de un gestor o instructor adecuado es clave para garantizar la confiabilidad, la integridad y confidencialidad del Sistema Interno de Información.

Se deben examinar los riesgos del factor humano que afectan a la pérdida de la autonomía e independencia necesaria del canal. Enumero algunos de ellos, que deben ser contemplados en las EIPD: las debilidades humanas sistémicas, que fueron definidas bajo el acrónimo “MICE” (Dinero, Ideología, Compromiso y Ego) por la CIA; el mal uso de dispositivos y herramientas digitales; la ausencia de habilidades cognitivas, psicológicas, jurídicas y de tareas; la capacidad de identificación de vulnerabilidades y amenazas del SII y de fases críticas de peligro para la seguridad, y la sobrecarga de información, de trabajo y cognitiva.

No es fácil ser gestor. **Es una irresponsabilidad asumir la designación sin capacitación ni formación adecuada.** Dejo para un análisis posterior la responsabilidad del gestor por la frustración del proceso. ¿Cuál es la responsabilidad del gestor-instructor por exponer la información a terceros? ¿Qué pasa si atentan contra la vida del informante? ¿Existe responsabilidad penal por comisión por omisión al mantener una posición de garante?

También tiene que conocer cómo proteger al informante de forma real y práctica, desarrollar la empatía e inteligencia emocional, para acompañar a los informantes en el proceso, el cual a veces resulta traumático y causa ansiedad y estrés postraumático.

Por tanto, el gestor de canal necesitará formación en cómo investigar guardando los derechos y garantías de las partes, conocimientos sobre las garantías procesales de investigación e instrucción, saber distinguir entre prueba válida y prueba ilícita, advertir de las investigaciones prospectivas y atender al respeto máximo al principio “in dubio pro reo” y de los derechos a la presunción de inocencia, a un un proceso justo y sin dilaciones indebidas, al derecho de defensa y de asistencia de letrado de los investigados, a su derecho a la información de la acusación formulada, de su derecho a la prueba y a no confesarse culpables y, en consecuencia, cómo se deben de obtener pruebas válidas confesorias.

Pero también, la exposición de motivos nos indica que “la configuración del Sistema Interno de Información debe reunir determinados **requisitos,** entre otros, su uso asequible, las garantías de confidencialidad, las prácticas correctas de seguimiento, investigación y protección del informante”.

Los gestores del canal SII son normalmente juristas y necesitan, por tanto, formación y capacitación en buenas prácticas de seguridad de la información.

Por último, hay que señalar el factor humano en la gestión y que, como he dicho al principio de este artículo y sin ánimo de ofender, los abogados y *Compliance Officer* somos "iletrados" informáticos en materia de privacidad y ciberseguridad. Tal como señalé en mi presentación sobre la asignatura olvidada, el *website privacy compliance*, **los juristas necesitamos formación teórica y práctica sobre privacidad y ciberseguridad** para distinguir lo que hay que hacer, lo que se puede hacer y lo que no se debe hacer.

El factor humano en el SII

Mantener un kit de dispositivos hardware y software garantes de la privacidad desde el diseño y por defecto es obligación del gestor e instructor de un Sistema Interno de Información.

Tampoco son recomendables **entornos de trabajo con telemetría e inteligencia artificial aplicada.** En otras palabras, trabajar con dispositivos que tengan los sistemas Windows, Android e IOS que capturan información de las actividades de los usuarios, en este caso los gestores.

Otra consecuencia es que no deberían utilizarse los **espacios cloud de trabajo** como Office365 y OneDrive o Google Cloud, que son muy cómodos, pero sobre los que se aplica la monitorización de la actividad, el seguimiento y telemetría del proveedor y de la organización. Además, normalmente están asociados a las urls bajo dependencia del Órgano de Dirección. Y es que, nuevamente, el superadministrador puede acceder a toda la información, dejando de ser confidencial.

Y es que el principio de mínimos privilegios obliga a establecer jerarquías sobre quién puede acceder a cada nivel de información, de menor a mayor confidencialidad. Esta es la forma de evitar fugas de información y de minimizar los riesgos de abuso de posición para un uso incorrecto de sus privilegios. Por ello, desde mi perspectiva aconsejo que la empresa cree un dominio que se asigne al órgano de *Compliance* o al *Compliance Officer*, quienes normalmente asumen el rol y la responsabilidad de la gestión del canal SII.

Para los profanos, existe lo que se llama la **clave del superadministrador**, que personalmente aconsejo que la tenga el Consejero Delegado o el Administrador Único, o a lo sumo un máximo de tres personas. Con esta clave se puede acceder a todos los correos y archivos digitales de la empresa y leerlos, modificarlos y borrarlos. En consecuencia, la persona que asuma el rol de gestor del canal no puede usar el correo corporativo principal de la organización o empresa para la finalidad de gestión del canal.

Dotar de independencia y autonomía al canal o canales de comunicación interna. Interno significa que tiene que estar bajo el control corporativo o de la organización, pero este canal no puede pertenecer al sistema común de información. En otras palabras, y simplificando, el canal SII no puede estar en el mismo dominio común URL de la empresa, puesto que si lo está ni es independiente, ni autónomo y, mucho menos, confidencial.

La selección del canal SII. El canal seleccionado deberá asegurar el cumplimiento de la misión del Responsable o del Encargado cumpliendo los requisitos regulados en el artículo 29 de la Directiva (UE) 2016/680). Quiero destacar entre ellos, el control de accesos y permisos, que debe ser compatible con la disponibilidad de la información y el principio de minimización de privilegios. La disponibilidad de la información requiere que las personas autorizadas puedan acceder a los datos siempre que quieran, y que además si ocurre un incidente de seguridad o un ataque esta información se podrá recuperar (back–ups). Asimismo, se debe contemplar una política de mínimos privilegios, puesto que no todos los miembros de una organización deberían acceder a toda la información de ésta y una política de control de acceso cerrado por defecto.

En otras palabras, el responsable del tratamiento o el gestor encargado del tratamiento tiene que **realizar prácticas correctas para garantizar la exhaustividad, integridad y confidencialidad de la información**, impedir el acceso a ella por el personal no autorizado y permitir un almacenamiento duradero de la misma. ¿Y cuáles son las consecuencias de todo esto?

La Exposición de Motivos de la Ley 2/2023 nos explica que se debe de “dotar de independencia y autonomía al canal o canales de comunicación externa pasa por garantizar la exhaustividad, integridad y confidencialidad de la información, impedir el acceso a ella por el personal no autorizado y permitir un almacenamiento duradero de la misma”.

La independencia y autonomía en el SII

Con todos estos parámetros y requerimientos del sistema, comenzaremos a realizar nuestra **Evaluación de Impacto de Protección de Datos (EIPD),** cuya metodología es adecuada para examinar si se cumplen los requisitos legales de garantizar el anonimato y la protección del informante.

¿Qué es una INFORMACIÓN CONFIDENCIAL? Aquella que debe conservarse y que no se puede modificar ni transferirse sin permiso.

¿Qué es la SEGURIDAD DE INFORMACIÓN? La seguridad de la información tiene por objetivo la protección de la confidencialidad, integridad y disponibilidad de los datos de los sistemas de información de cualquier amenaza y de cualquiera que tenga intenciones maliciosas. Las propiedades involucradas serán la autenticidad, la responsabilidad, el no repudio y la confiabilidad. La evaluación de riesgos deberá contemplar las amenazas y vulnerabilidades del sistema de información.

¿Qué es la INTEGRIDAD DE LA INFORMACIÓN? La exactitud y consistencia general de los datos o, expresado de otra forma, la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios. Es decir, la información en un SII se tiene que mantener exactamente como fue ingresada en operaciones tales como la captura de datos, el almacenamiento, la recuperación, la actualización o la transferencia.Por el contrario, la corrupción o alteración de los datos puede ocurrir de forma accidental (por ejemplo, a través de errores de programación) o maliciosamente (por ejemplo, a través de infracciones o hacks). Para evitar o minimizar la posibilidad de corrupción de los datos, el SII contendrá una serie de herramientas y controles tales como: el cifrado de datos; las copias de seguridad; los controles de acceso y asignación de permisos; la validación de entrada para evitar la entrada incorrecta de datos y la validación de datos, para certificar transmisiones sin corrupción de datos.

¿Qué es un SISTEMA DE INFORMACIÓN? Un conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información

Hasta aquí lo que dicen las normas, pero para entender el significado de garantizar la integridad y la seguridad de los datos tenemos que acercarnos a las **normas de estandarización de la seguridad de los sistemas de información** y a sus definiciones. Y, de esta forma, entenderemos los requerimientos del sistema SII (ISO/IEC 27000).

Los registros registrarán la recopilación, la modificación, la consulta, la comunicación (incluida la transmisión), la combinación o la supresión de datos. Los datos identificativos de la persona que consulta o comunica los datos personales deben quedar registrados y, a partir de dichos datos, debe ser posible establecer **la justificación de las operaciones de tratamiento.**

Para demostrar que se cumple lo dispuesto en la Directiva, el responsable o el encargado del tratamiento debe mantener registros relativos a todas las categorías de actividades de tratamiento que se lleven a cabo bajo su responsabilidad. Estos registros estarán a disposición de las autoridades. Tal como señala el ordenamiento, **los registros diarios o de otro tipo servirán para demostrar la licitud del tratamiento**, permitirán el autocontrol y garantizarán la integridad y la seguridad de los datos.

Además, en aplicación del RGPD y de la Directiva 2016/680, t**odo intercambio o transmisión de información por parte de las instituciones, órganos, empresas u organismos no recopilará datos personales** cuya pertinencia no resulte manifiesta para tratar una denuncia específica o, si se recopilan por accidente, se eliminarán sin dilación indebida (Principio de minimización de datos y Principio de protección al informante).

La Ley establece que tanto el responsable (la empresa, organización o corporación pública) como el encargado del tratamiento (el gestor y/o el instructor) adoptarán las **medidas técnicas y de organización necesarias para garantizar un nivel de seguridad adecuado al riesgo**, teniendo en cuenta el estado de la técnica y los costes de aplicación, así como la naturaleza, el

alcance, el contexto y los fines del tratamiento. Igualmente, hay que tener presente el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, sobre todo en lo que se refiere al tratamiento de las categorías especiales de datos personales previstas en el artículo 10. Estas medidas técnicas incluyen de conformidad con el RGPD, observar la soberanía de datos y el cumplimiento en el iter de la denuncia (desde donde se sitúa el enlace al acceso al canal) del art. 5 (3) de la Directiva e-Privacy, lo que obliga a no posibilitar la descarga de cookies y trackers desde la página corporativa sin consentimiento previo.

De conformidad con el art. 17 de la Directiva Whistlebowing, el tratamiento de datos personales en los SII debe ajustarse a las previsiones del Reglamento General de Protección de Datos (UE) 2016/679 y la Directiva (UE) 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Los requisitos de seguridad que debe tener un Sistema de Información para garantizar la confidencialidad e integridad

Pero tener un canal SII y un gestor no es suficiente para cumplir la Ley. Y es que, a mi juicio, más grave que no tener un SII es que este no sea seguro o ciberseguro o esté gestionado o gobernado por personas inapropiadas (el factor humano). De hecho, el art. 63.1.c) de la Ley regula como **infracción** "c) Vulnerar las garantías de confidencialidad y anonimato previstas en esta ley, y de forma particular cualquier acción u omisión tendente a revelar la identidad del informante cuando este haya optado por el anonimato, aunque no se llegue a producir la efectiva revelación de la misma".

La exigencia legal del SII ha venido a democratizar el *compliance* en el sector público y en la empresa. Para los que creemos en el cumplimiento normativo, la ética y la transparencia ha sido una bendición. Y es que la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, e**xige a los obligados tener al menos un canal SII y un gestor de canal**, ambos autónomos e independientes. La Ley tipifica que no tener un canal SII es una infracción muy grave con sanciones de más de 600.000 euros para la persona jurídica.

Hace un mes finalizó la **IV semana del *Compliance*** organizada por Cumplen, la *World Compliance Association* y el Instituto de Oficiales de Cumplimiento. El tema estrella fue el **"Sistema Interno de Información"** (en adelante, SII) tras la aprobación de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. Entró en vigor el pasado 13 de marzo de 2023 e impone a diversas entidades públicas, organizaciones y empresas la **implantación de canales de denuncias.** El segundo tema estrella fue el ***cibercompliance***.

Se examina el riesgo de seguridad de los sistemas internos de información más conocidos como canales éticos o de denuncia.