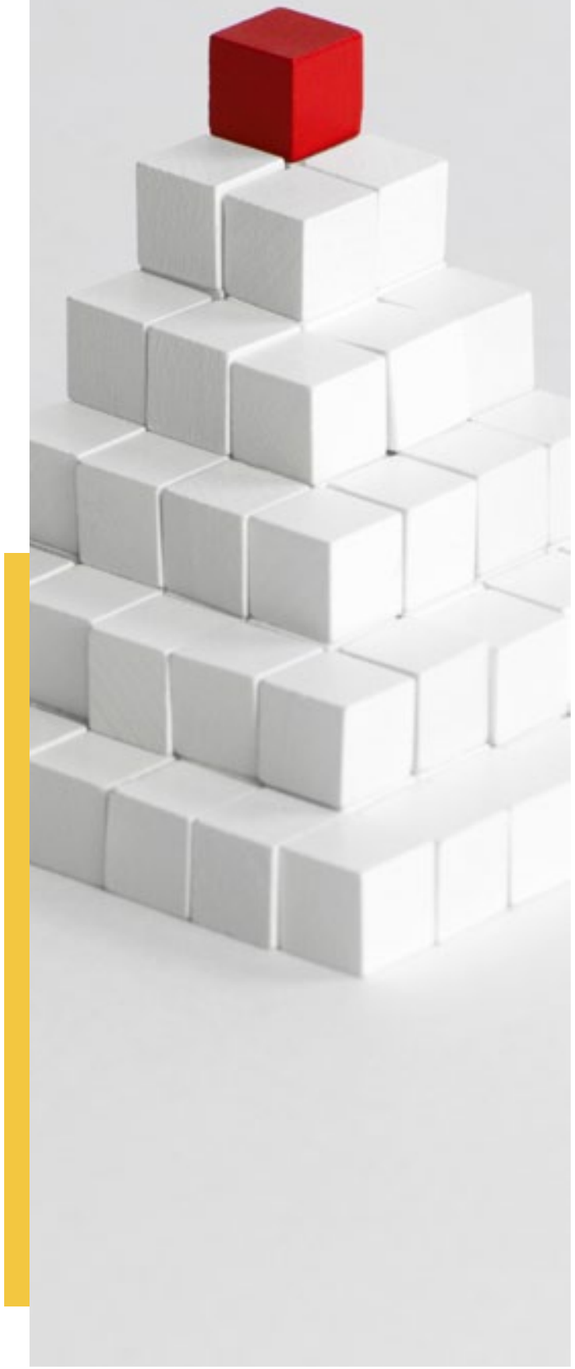


El Compliance IT, la gestión de seguridad de la información como piedra angular del sistema.

Joaquín Hernández García
IT & Data Protection Lawyer
Risk & Compliance
Ecija Law & Technology

En la actualidad, existen una serie de conductas delictivas relacionadas con los sistemas de información, y en particular con los datos de carácter personal, que exigen dotar a los programas de prevención de delitos (o compliance) de las personas jurídicas de un sistema de gestión de seguridad de la información (SGSI), para que puedan servir como eximentes de la responsabilidad penal.

Un sistema de información es, según la definición dada por la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información, *todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.*

No obstante, nuestra reflexión no puede únicamente estar centrada en términos de exención. La información se ha convertido en uno de los principales activos de cualquier empresa, y su falta de disponibilidad, integridad y confidencialidad podría afectar al normal funcionamiento de nuestra actividad.

Pensemos que en la actualidad los ciberataques son una de las principales preocupaciones de cualquier empresa, fraude, hacking, virus, fugas y robos de información, phishing, espionaje industrial, denegación de servicio, son acciones dirigidas a vulnerar los sistemas de información de las empresas.

Centrándonos en las conductas recogidas en el CP, de las que puede responder una persona jurídica, el artículo 197 quinquies indica que una persona jurídica podría ser responsable penalmente por la comisión de ciertos delitos relativos al descubrimiento y revelación de secretos.

Especial atención merecen las conductas consistentes en el apoderamiento, interceptación, utilización, modificación, difusión y cesión de información que contenga datos de carácter personal (art. 197.2 CP) para descubrir los secretos o vulnerar la intimidad de otro, constituyendo tipos agravados dichas conductas si los datos reservados se hubieran difundido, cedido o revelado a terceros, y los hechos o si los hechos se realizasen con fines lucrativos.

Datos de carácter personal son *toda información sobre una persona física identificada o identificable (el interesado), indicando a continuación que se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*

> ***“Datos de carácter personal son toda información sobre una persona física identificada o identificable”***

El tipo básico hace únicamente referencia a la realización del hecho punible por personas no autorizadas a acceder a los datos personales, por lo que parecería –siguiendo el principio de interpretación restrictiva de la ley penal- que una persona autorizada a acceder, utilizar o modificar los datos personales, no podría ser condenada por la comisión de este delito, lo que parece un sin sentido.

Otro tipo cualificado por su gravedad que implica una pena más gravosa para su autor viene configurado atendiendo precisamente a la condición del autor. En efecto cuando las conductas punibles se cometan por los responsables o encargados de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, y sin consentimiento del titular de los datos de carácter personal.

También se imponen penas en su mitad superior cuando las conductas descritas anteriormente afecten a datos especialmente protegidos, es decir, aquellos que *revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.*

Existen otra serie de conductas, cuyo bien jurídico protegido no es la propia privacidad de los interesados, sino los sistemas de información en sí mismos, sin que sea exigible que esta conducta permita en alguna forma el conocimiento de información de carácter íntimo o reservado. Pero parece relevante citarlas, pues de su comisión puede derivarse la facilitación de la comisión de las conductas previamente descritas. Se trata del acceso ilícito a sistemas informáticos, o su facilitación, vulnerando las medidas de seguridad, así como la interceptación ilegal de datos informáticos en transmisiones no públicas.

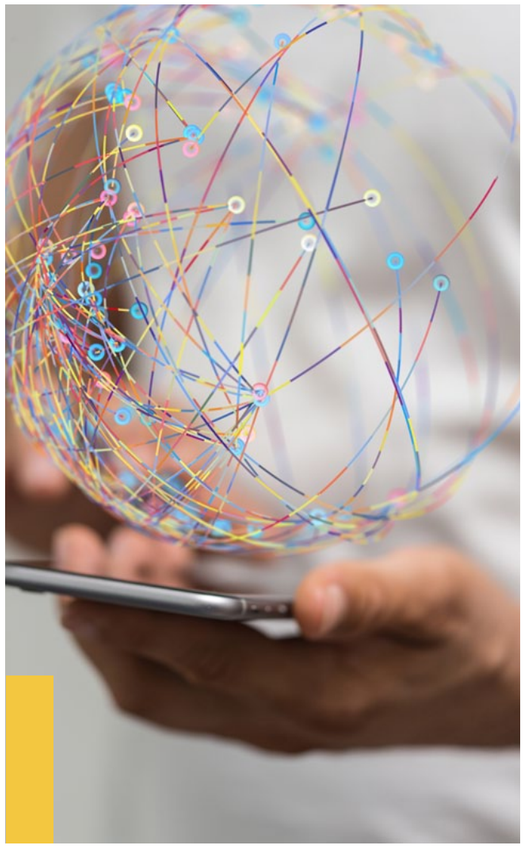
Igualmente punible, y continuando con el sistema de información como bien jurídico protegido, resulta la conducta de producción o facilitación a terceros de programas informáticos o contraseñas con la intención de realizar alguna de las conductas previamente descritas. Es importante destacar que este tipo de conductas deberán ser claramente utilizadas para cometer actos ilícitos, pues no en vano son numerosas las empresas que utilizan estas herramientas con fines legítimos, para auditar seguridad de sistemas, programas o aplicaciones, detectar vulnerabilidades, garantizar la solidez o fiabilidad de contraseñas o sistemas de seguridad.

Las diferentes responsabilidades derivadas de la comisión de estas conductas recaerán, individual o colectivamente, sobre el responsable del fichero, el responsable de seguridad, o en su caso el Delegado de Protección de Datos, o sobre aquellas otras personas relacionadas directa o indirectamente a quienes, por sus funciones o actos, pudieran serle atribuidas. Estas conductas podrían ser cometidas en el seno de una organización por cualquiera de sus empleados, en función de los accesos autorizados a cada usuario, y los permisos otorgados a los mismos, ya sea únicamente de mera consulta o de modificación de los datos.

Además de las consecuencias penales, la persona jurídica asumiría la responsabilidad civil derivada de los actos propios u omisiones, contemplados en las normas civiles. Es por ello que resulta imprescindible la existencia de medidas de seguridad y controles que protejan los sistemas de información de nuestra empresa.

Hasta la aprobación del Reglamento General de Protección de Datos (RGPD) el pasado 27 de abril de 2016, y que será aplicable a partir del 25 de mayo de 2018, las medidas de seguridad estaban tasadas por nuestro Reglamento de Desarrollo 1720/2007, que en función del nivel de los datos de carácter personal (básico, medio o alto), establecía una serie de medidas a adoptar por cualquier entidad que tratara datos personales.

El RGPD no recoge un listado tasado, si no que establece que las medidas de seguridad técnicas y organizativas se deberán adoptar teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, para garantizar un nivel de seguridad adecuado al riesgo.



Es por ello que la implantación de las normas ISO 27000, para sistemas de gestión de seguridad de la información, sería un instrumento ideal para dar cumplimiento a esta exigencia de seguridad para la protección de los datos de carácter personal. Así, a partir de un análisis de riesgos, cada entidad deberá en función de estos últimos establecer aquellas medidas que considere oportuno.

La nueva normativa europea, el RGPD, nos obligará también a tratar los datos personales de tal manera que sea posible garantizar la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Debiendo ser el responsable capaz de demostrar que ha establecido dichas medidas, dentro de lo que se denomina la "responsabilidad proactiva", entre las que se incluiría la adopción de medidas como la privacidad desde el diseño y/o por defecto, la realización de evaluaciones de impacto, la notificación de brechas de la seguridad o la formación continua entre otras. Como vemos, esta gestión del cumplimiento no se aleja de los modelos de gestión y organización a los que hace referencia el artículo 31 bis del CP.

La no implantación de este tipo de medidas podría dar lugar a sanciones administrativas por incumplimiento de la normativa sobre protección de datos, que podrían ser de hasta 20 millones de euros o el 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Un SGSI nos ayudaría a evitar que se produjeran conductas que pudieran acarrear sanciones tanto administrativas como penales a nuestra organización, si bien, debemos matizar que la seguridad no existe 100%, por lo que el principal objetivo sería mitigar al máximo la probabilidad de ocurrencia de dichos ilícitos, así como ser capaces de ser lo más reactivo posible ante la conducta.

Un registro de actividades relacionadas con la información nos permitirá obtener evidencias de las posibles conductas antijurídicas, pudiendo así atribuir responsabilidades individualizadas.

Los principales pasos a seguir para la implantación de un SGSI serían el análisis del sistema de información, el inventario de activos relevantes, la identificación de posibles amenazas, la definición de riesgos asumibles y no asumibles, la implementación de contramedidas y métodos de trabajo seguros, que redundarían en una mejora de la imagen empresarial y satisfacción de los clientes, consiguiendo así además una posible mejora en los resultados.

Es requisito indispensable que los representantes legales, administradores y directivos de una organización tomen conciencia de la importancia de llevar a cabo la implantación de un SGSI, y se hagan responsables de implementar una serie de políticas y objetivos de seguridad en los que se sustentará todo el SGSI. Se definirá una gestión de recursos económicos, de personal y de capacidad, acordes al tamaño de la organización.

Deberemos conocer el estado de situación de nuestra organización, lo que nos permitirá definir el alcance del SGSI. Definiremos el equipo de trabajo encargado de la implantación y mantenimiento, que debería estar compuesto por varios miembros (o equipos en función del tamaño empresarial), con la acreditada experiencia en el cumplimiento de estas funciones, con especial importancia del perfil de aquellos que tengan responsabilidad directa sobre los sistemas de información. El responsable de seguridad deberá ser capaz de coordinar la seguridad entre los diferentes departamentos, con un perfil a veces más de gestión. Un responsable experto tecnologías de la información con un perfil más técnico. Un especialista de comunicación, para controlar las consecuencias en caso de crisis de reputación. Un abogado experto en derecho de tecnologías de la información que controlará la legalidad de todas las actuaciones y defenderá los intereses de la empresa. Pudiendo algunos

de estos roles depender de una misma persona.

Una vez analizados los flujos de información a través de los sistemas de información, soportes, aplicaciones, activos, red y documentación, podremos evaluar las amenazas que en función de la probabilidad de ocurrencia y riesgo, puedan explotar una vulnerabilidad, comprometiendo la confidencialidad, integridad o disponibilidad de la información. En función de los riesgos detectados definiremos las políticas y procedimientos más específicos en los que se sustentará el SGSI, y cuyo objetivo será establecer protocolos de trabajo que garanticen la seguridad de la información. Tendremos procedimientos más organizativos y otros más técnicos basados en una serie de controles establecidos por la norma, y que tratan de abordar diferentes áreas clave para una seguridad de la información eficaz: políticas de seguridad de la información, organización de la seguridad de la información, seguridad relativa a los recursos humanos, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, seguridad de las operaciones, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento de los sistemas de información, relación con proveedores, gestión de incidentes de seguridad de la información, aspectos de seguridad de la información para la gestión de la continuidad del negocio y cumplimiento.

Este SGSI deberá ser constantemente medido, manteniendo en todo momento unos indicadores de eficacia denominados métricas, auditado y revisado, para adoptar acciones correctivas, preventivas y de mejora del mismo.

Una vez cometidos en el seno de una entidad los delitos relacionados con datos de carácter personal, o la facilitación de mecanismos para la comisión de estos, la implantación de un SGSI podría ser por un lado utilizada ante un Tribunal con la intención de lograr la exención de la persona jurídica, dado que formaría parte del modelo de organización y gestión que incluye las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión, evitando además responsabilidades administrativas y civiles.

Por otro lado, el SGSI prevendría que se dieran situaciones en las que se viera afectada la propia imagen de la empresa, su posición de mercado o el impacto en la confianza de su público objetivo, siendo difícilmente cuantificable el daño reputacional asociado a la falta de garantía de la privacidad y derechos fundamentales de sus clientes.