Los controles para mitigar los riesgos asociados a la propiedad intelectual

En mi post anterior hablé sobre los diferentes riesgos relacionados con la propiedad intelectual. Estuvimos hablando tanto de los riesgos externos como de los internos y recordamos que ambos son de igual importancia, es decir, no podemos dejar de contemplar ni a los unos ni a los otros.

En este post quiero hablar sobre los diferentes controles que se pueden aplicar en las empresas para estos riesgos. Estos controles nos servirán de escudo contra estas amenazas y les servirán a las empresas para saber si están fallando (en caso de que éstas los estén empleando) o si simplemente no se están aplicando.

Los controles que os iré mencionando y recomendando en este post son algunos de los muchos que están presentes en la ISO 27002. Esta ISO es un estándar para la seguridad de la información publicado por la Organización Internacional de

Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). También deciros que la última versión de este estándar se publicó en el año 2013; con esto lo único que pretendo es concienciaros de que no es un estándar obsoleto y en desuso.

Retomando el tema de los controles, ¿qué tipo de controles aplicaríamos contra los riesgos externos? ¿Y contra los riesgos internos? ¿Qué controles tendríamos que aplicar para mitigar los riesgos relacionados con los ciberataques? ¿Y para mitigar aquellos relacionados con el espionaje corporativo?

En este post os iré dando una serie de recomendaciones sobre qué controles aplicar para mitigar los riesgos que mencioné en mi anterior post: ciberataques (riesgo externo) y espionaje corporativo (riesgo interno). Para ello, seguiremos los controles que nos proporciona el estándar ISO 27002.

Para mitigar los riesgos relacionados con los **ciberatques** os recomiendo aplicar (como mínimo) los siguientes controles del estándar:

- 12.2.1 Controles contra el código malicioso: asegurarnos de que el código que se utiliza en la empresa está libre de virus o esté infectado desde el exterior.
- 13.1 Gestión de la seguridad en las redes: aplicar todos los controles relacionados con la seguridad de las redes de la empresa.
- 13.2.1 Políticas y procedimientos de intercambio de información: establecer claramente cuáles son las políticas y procedimientos seguros para el intercambio de información.
- 11.2.1 Emplazamiento y protección de equipos: asegurarnos de que los equipos que se utilicen estén bien protegidos.
- 11.2.3 Seguridad de cableado: comprobar que el cableado esté correctamente securizado.
- 11.2.4 Mantenimiento de los equipos: comprobar que los

equipos estén siendo actualizados gracias a un buen mantenimiento; que no tengan versiones obsoletas de antivirus y cosas por el estilo.

- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones: que todos los equipos y activos que se utilicen fuera de las instalaciones, pero, que forman parte de la empresa y acceden a recursos de la empresa estén debidamente protegidos de los ataques externos.
- 16.1.2 Notificación de los eventos de seguridad de la información: que se notifiquen debidamente los diferentes eventos de seguridad que se produzcan en la empresa.
- 16.1.3 Notificación de los puntos débiles de seguridad: que se notifiquen debidamente los diferentes puntos débiles que tenga la empresa.
- 16.1.5 Respuesta a los incidentes de seguridad: asegurarse de que haya una respuesta a cada incidencia que se produzca en el sistema de información de la empresa.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información: que haya un proceso de aprendizaje de las incidencias que se comentan en la empresa.

Por último, para mitigar los riesgos relacionados con el **espionaje corporativo** os recomiendo aplicar (como mínimo) los siguientes controles del estándar:

- 7.1.1 Investigación de antecedentes: previo a la contratación de cualquier empleado, investigar bien los antecedentes de la persona entrevistada para obtener pistas sobre si puede ser o no un espía corporativo enviado desde otra compañía (normalmente desde una compañía de la competencia).
- 11.1.2 Controles físicos de entrada: que se realicen controles físicos para asegurarnos de que no entre ninguna persona autorizada a las instalaciones (por ejemplo, el trabajado de una compañía de la

competencia).

- 11.1.3 Seguridad de oficinas despachos y recursos: del mismo modo que en el anterior, que las oficinas, despachos y recursos estén protegidos contra las persona que no tengan una autorización para acceder a dichos lugares.
- 11.1.4 Protección contra amenazas externas y ambientales: protegerse contra amenazas externas (que puedan venir del exterior) como son los espías corporativos.
- 9.1 Requisitos de negocio para el control de acceso: todos los controles relacionados con los requisitos mínimos que hay que cumplir para acceder al sistema de la empresa (se evita que entre al sistema quién no deba).
- 9.4.1 Restricción de acceso a la información: del mismo modo que en algún punto anterior, con este control se evitar que personas sin autorización puedan acceder a ciertas partes de la información.
- 13.2.4 Acuerdos de confidencialidad y secreto: en los contratos, acordar este tipo de acuerdos para que en caso de que la persona contratado lo incumpla y desvele secretos de tu empresa a otra compañía; tu empresa pueda denunciar lo ocurrido y no verse tan perjudicada.