LA SEGURIDAD EN EL SEGMENTO DE AUTÓNOMOS Y PYMES

Manuel Sánchez Gómez-Merelo | Consultor Internacional de Seguridad

LA EFICACIA EN MATERIA DE SEGURIDAD NO SE CONSIDERA UNA PRIORIDAD

SI BIEN HAY UNA SEGURIDAD SUBJETIVA Y UNA SEGURIDAD OBJETIVA, LA PRIMERA ES UNA PERCEPCIÓN Y LA SEGUNDA UNA REALIDAD A LA QUE, COMO OBJETIVO NOS HEMOS DE ENFRENTAR TODOS LOS DÍAS Y, EN ESTE SENTIDO, HAY TANTOS FACTORES QUE REPERCUTEN EN SU GESTIÓN EN LAS PEQUEÑAS EMPRESAS, COMO EN LAS DE MAYOR TAMAÑO, Y REQUIEREN IGUALMENTE DE UN RIGUROSO TRATAMIENTO.

En la aplicación de la seguridad hay dificultades para su regulación, dado que suelen ser heterogéneas y están diseminadas. Así mismo, las restricciones presupuestarias se traducen a menudo en falta de recursos para implantar iniciativas e intervenciones para una necesaria y adecuada seguridad patrimonial y laboral.

Al contar con menos recursos se reduce la realización de programas y acciones preventivas.

La eficacia en materia de seguridad en las PYMEs y en los autónomos no se considera una prioridad.

La identificación, análisis y evaluación de los riesgos pueden resultar costosas y confusas, en especial si la empresa carece de recursos o de conocimientos especializados para hacerlo con eficacia.

El catálogo de riesgos es amplio y complejo

En general, como es sabido, si la seguridad total no existe, nuestro planteamiento debe ir dirigido a realizar el esfuerzo por la reducción del daño o pérdida, caso de producirse o materializarse el riesgo.

Toda actividad industrial o comercial conlleva una serie de riesgos, unos inherentes a la propia actividad y otros a la situación, entorno o circunstancias de la empresa.

En cualquier caso, y con independencia de su tamaño y actividad, las PYMEs pueden presentar en general un amplio catálogo de riesgos derivados de la naturaleza (seísmos, inundaciones, tormentas, etc.), riesgos técnicos (fuego, corrosión, toxicidad, explosión, averías, etc.), riesgos laborales (herramientas, instalaciones, manipulación, ambiente, transporte, etc.) o derivados de actividades antisociales o deliberados (fraude, robo, atraco, agresión, vandalismo, manipulación de datos, etc.).

Estos riesgos, en todos los casos, han de identificarse, analizarse y evaluarse y tomar posición frente a ellos. Del análisis podemos determinar contra qué es necesario protegerse y qué es necesario proteger, en un entorno donde igualmente hay que identificar y analizar las propias vulnerabilidades de nuestra actividad y circunstancias.

Tras el análisis y la evaluación, los riesgos se presentarán en tres bloques: los posibles de evitar o minimizar, los que conviene reducir y aquellos que no son fácilmente mejorables y que se han de asumir.

La seguridad integral, una inversión y no un gasto

La seguridad, debe integrar dos aspectos básicos como son la prevención y la protección. La prevención, tiene como objetivo primario la eliminación o reducción de las circunstancias o causas desencadenantes del riesgo o amenaza. La protección pone en marcha los medios contra el propio incidente o accidente cuyo objetivo primario es evitar o reducir los daños o pérdidas que se pueden generar, una vez que se ha materializado el riesgo.

De forma tradicional, para aplicar un esquema de seguridad integral, primero se deben identificar y relacionar los riesgos y las amenazas de forma pormenorizada y exhaustiva, después los relacionaremos con los escenarios y mediremos su recurrencia, prevalencia y posibles consecuencias, valorando igualmente las vulnerabilidades para, finalmente, determinar los medios y medidas de prevención y protección más ajustadas a nuestras necesidades

En este sentido, los nuevos retos y las nuevas exigencias para la seguridad requieren que los recursos destinados a la protección de activos e información de las empresas, se integren en todos y cada uno de los procesos productivos, como un eslabón más de la cadena de valor.

Implementar un nivel de seguridad adecuado en función de los riesgos y vulnerabilidades a los que está expuesta la empresa (financieros, operativos, deliberados, comerciales, medioambientales, etc.) y de los requisitos de cumplimiento (legales, regulatorios, contractuales, etc.) es un reto permanente a tener en cuenta y que requerirá de un mínimo sistema de control basado en la implementación de medidas de seguridad que han de ser técnicas y organizativas.

TODA ACTIVIDAD INDUSTRIAL O COMERCIAL CONLLEVA UNA SERIE DE RIESGOS, UNOS INHERENTES A LA PROPIA ACTIVIDAD Y OTROS A LA SITUACIÓN, ENTORNO O CIRCUNSTANCIAS.

Con todo ello, obtendremos beneficios como:

- **Reducción de riesgos**. Minimizar o eliminar los riesgos para el negocio, resultantes de la materialización de las amenazas evaluadas.

- **Optimización de costes**. Racionalización de los recursos en base a la eliminación de inversiones innecesarias debidas al desconocimiento de los riesgos.

- **Cumplimiento de la legislación vigente**. Aseguramiento del cumplimiento del marco legal que protege a la empresa eliminando los riesgos y sanciones.

- **Competitividad en el mercado**. Mejora de la confianza en el negocio entre clientes y proveedores con los que se comparte la información y actividad.

Tenemos que asegurar una actuación coherente, proporcionada y eficaz ante cualquier incidencia de riesgo o vulnerabilidad entendiendo como uno de los problemas a atender en seguridad el de la sensación subjetiva de inseguridad, y lo debemos de combatir sin dejarnos llevar por aquellos que desean solamente, aportar seguridad a cualquier precio.

La Seguridad hoy presenta nuevas amenazas, nuevos retos y por tanto, nuevas exigencias que requieren de nuevos conceptos, pues tenemos: Nuevos escenarios para la seguridad, nuevos riesgos derivados de la globalización (sin excluir a los ya existentes) y una nueva dimensión de las inseguridades.

En este sentido, la seguridad ha ido creciendo en paralelo al progreso aunque, habitualmente, se ha visto más como un coste o gravamen y no como un beneficio o inversión inmovilizada.

Por otro lado, quizá el mayor nivel de vulnerabilidad se consiga a partir del hecho constatado de que necesitamos unos cuantos años para darnos cuenta de la amenaza que representan para nuestros bienes y nuestra privacidad las nuevas tecnologías y los medios de comunicación puestos a nuestra disposición.

Como conclusión tenemos que la organización de seguridad debe ser flexible y adaptable día a día en su visión de los riesgos, amenazas y vulnerabilidades así como sus soluciones.

La aplicación de estas en la empresa o sociedad debe ser un proceso continuo de realimentación.

La información, el bien más preciado

Capítulo aparte, merece hablar de la necesaria ciberseguridad, pues muchas empresas pequeñas y medianas creen que los problemas derivados de las vulnerabilidades en la protección de la información no son de su incumbencia y no son un objetivo de los ciberdelincuentes, al sentirse libres del riesgo de sufrir ataques por parte de estos.

Recientes ataques cibernéticos han puesto de manifiesto que el mapamundi de la piratería digital se presenta como escalofriante, y no vale pensar que es un problema de otros.

Bajo la amenaza de "paga o destruimos tus datos", este formato delictivo ha encontrado un caldo de cultivo extraordinario en la sociedad de la comunicación y la información, que ha revelado así su extrema vulnerabilidad.

BAJO LA AMENAZA DE "PAGA O DESTRUIMOS TUS DATOS", ESTE FORMATO DELICTIVO HA ENCONTRADO UN CALDO DE CULTIVO EXTRAORDINARIO EN LA SOCIEDAD DE LA COMUNICACIÓN Y LA INFORMACIÓN, QUE HA REVELADO ASÍ SU EXTREMA VULNERABILIDAD.

Lo cierto es que las graves consecuencias de estos riesgos, amenazas y vulnerabilidades han sido manifestadas mediante un simple 'ransomware', con un cibersecuestro de datos y archivos que los encripta de manera que no se puede acceder a ellos. Los ciberdelincuentes o presuntos terroristas han extorsionado a los afectados, a los que han exigido un rescate económico para liberar -descifrar- sus propios archivos.

Finalmente, no hemos de olvidar que, en general, la información es el bien más preciado de nuestras empresas y, aunque no existe la protección total o garantía de no poder ser afectado, con la permanente actualización y control de nuestros sistemas, se consigue evitar graves sucesos como los ocurridos o, al menos, minimizar el importante nivel de impacto que pueden tener.

www.manuelsanchez.com