LOS CIBERATAQUES

(LA SEGURIDAD DE LA INFORMACIÓN)

Una de las noticias estrella de este fin de semana ha sido el **ciberataque** que se ha producido en 150 países y sobre infinidad de importantes empresas, como es el caso de **Telefónica**. Otras entidades como la **Ciudad de la Justicia de Valencia**, como medida preventiva, tuvieron que prescindir de los sistemas informáticos en las guardias de los juzgados de instrucción, según apuntaba la prensa.

Por los nombres utilizados de “ciberataque”, “ciberterrorismo”, etc., tal vez muchas pequeñas empresas consideren que no son objetivo estratégico de bandas organizadas de delincuencia informática, y que la seguridad informática es para los Estados, grandes corporaciones e instituciones.

Sin embargo, tal vez no se hayan parado a pensar en que si bien es cierto, y el efecto mediático de atacar los sistemas informáticos de grandes instituciones de los Estados, por ejemplo la Agencia Tributaria Española, la Tesorería de la Seguridad Social, o cualquier ministerio, sí que pueden enfrentarse en los próximo años a los “chorizos informáticos”, es decir, pequeños delincuentes (como existen delincuentes dedicados a pequeños delitos como tirones de bolsos, carteristas, etc.) que introduzcan virus en sus sistemas informáticos exigiendo una cantidad (tal vez no muy elevada) para permitirles seguir trabajando. Algo así como un “secuestro exprés” aunque sin la violencia de este tipo de delitos y con unas mayores garantías de impunidad por las dificultades de soslayar el anonimato de la Red.

¿**Hasta cuánto estaría dispuesta a pagar una pequeña empresa para poder seguir trabajando sin que se paralizara su actividad**?

Sin duda aluna esto nos debe hacer reflexionar de forma inminente sobre los riesgos que tienen las empresas.

Muchas veces no se es consciente de la importancia que tiene la información dentro de las empresas y organizaciones; prácticamente la totalidad de actividades que se desarrollan generan información y se necesita información para trabajar.

Sin embargo, no siempre se le presta la atención adecuada, pues controlar adecuadamente toda esa información es un esfuerzo, un coste, que no parece que tenga rentabilidad alguna hasta que se produce un error y no se encuentra determinada información.

La **norma ISO 27001** aporta unas pautas para controlar y gestionar adecuadamente toda la información que se genera en la empresa, tanto en soporte papel como en soporte electrónico. Es perfectamente compatible con la norma ISO 9001 o ISO 14001; participa de los mismos principios y fundamentos.

Obliga a realizar un análisis de todos los flujos de información y de toda la información (registros) que se genera en la organización para poder establecer unas pautas de actuación, que van más allá de las habituales copias de seguridad, con lo que hoy en día parece que queda resuelto todo el problema de la seguridad de la información.

Una vez definidos todos los flujos de información y conocidas todas las informaciones que se generan, se podrán establecer las pautas de actuación, que podrán ir, dependiendo de la empresa, de su complejidad, del tipo de información, etc. desde definir niveles de confidencialidad y dar accesibilidad a la información a cada persona dependiendo de su jerarquía, hasta minimizar los efectos que pueden provocar actos de sabotaje por parte de algún empleado u otra persona.

Las posibilidades son muchas; habrá que compaginar siempre seguridad con operatividad, pues medidas de seguridad excesivamente complejas en organizaciones simples pueden provocar un parón importante.

Un **sistema de seguridad de la información** puede ayudar de manera importante al cumplimiento de la normativa sobre protección de datos de carácter personal, aunque el sistema de seguridad de la información representa un escalón más, pues no sólo abarca a los datos de carácter personal, sino a toda la información de la organización.

La norma ISO 27001 puede servir de guía y orientación en esta tarea de optimizar la información. No deja de ser una aplicación específica del control de los registros de la norma ISO 9001 o de la norma ISO 14001.

La certificación puede ser una exigencia de algunos clientes que confían información a sus proveedores y subcontratistas y quieren tener garantía de que dicha información será adecuadamente custodiada, en algunos casos por motivos de confidencialidad (accesibilidad) y otras veces por meros motivos de seguridad, pueden confiar determinada información cuya pérdida podría ser costosa de recuperar (piénsese por ejemplo en un despacho de abogados al que se le confían determinados documentos originales).

Infórmate sin compromiso si te interesa que te asesoremos, o quieres ampliar información sobre el tema de la seguridad de la información en tu empresa (comercial@ivac.es 96 394 39 05).