La Información asegura el futuro de las empresas

Que la información es el principal activo de las empresas, lo sabemos todos. De poco sirven los mejores ordenadores o el personal mejor formado si no hay información correcta y completa con la que trabajar.

"Cada detalle medible y gestionable es información valiosa: los Datos Personales regulados por el RGPD, los de Calidad y Control regidos por las Normas ISO, la Gestión y Evaluación de Riesgos supervisados por las Normas de Compliance, la información administrativa y gerencial controlada por la Ley de Secreto Empresarial y Normas Tributarias", explica Mario Ramírez, director general de Forlopd, especialistas en seguridad de la información. Y es que el éxito de una empresa depende de cómo gestiona el ciclo de vida de sus datos, de su información. Ramírez añade que "no se puede dirigir correctamente una empresa ignorando el cumplimiento normativo y la seguridad de su información".

Pensar seriamente en el futuro de las empresas sin pensar en cumplir las normativas legales es casi una temeridad. En la responsabilidad con que se cumplen esas normativas, en la consciencia con que se protege toda esa información, es donde las empresas que perdurarán marcan el paso a seguir.

Debido a nuestra confianza natural, nos cuesta ver la inmensidad que representan las nuevas amenazas diarias que, como gigantescas olas, están lanzando los ciberdelincuentes contra los sistemas de información de las empresas.

Sabiendo lo importante que es la Información, como complemento a todo el apoyo que empresas como Forlopd dan a sus clientes en todo lo relacionado con el cumplimiento normativo, también están ayudando a mejorar significativamente su Ciberseguridad.

¿Qué es la ciberseguridad?

"La Ciberseguridad es sentido común bien informado", define Mario Ramírez. Es decir, que son las técnicas, procedimientos y procesos con los que se protege la información digital de una empresa, evitando ataques y minimizando el efecto de los que no se pueden evitar.

Y es que cada día, los Ciberataques son más intensos y sofisticados. "Lo lógico es pensar preventivamente e implementar medidas de Ciberseguridad debidamente supervisadas por personal especializado".

Mario Ramírez
Director general de Forlopd

"De poco sirven los mejores ordenadores o el personal mejor formado si no hay información correcta y completa con la que trabajar"

"La Ciberseguridad es sentido común bien informado"

¿Que son los ciberataques?

Los Ciberataques son acciones externas o internas, que aprovechan descuidos y vulnerabilidades. Se concentran en los puntos débiles del sistema, en la falta de actualizaciones o en errores del personal implicado en la gestión. Las empresas pierden tiempo, dinero, reputación y generan mala imagen ante sus clientes al sufrir ataques exitosos.

"A los atacantes los debemos llamar Ciberdelincuentes, no simplemente Hackers, porque la inmensa mayoría de los Hackers no buscan dañar a los demás ni buscan su propio beneficio", puntualiza Ramírez. "En FORLOPD estamos especializados en medidas de seguridad preventiva, bien supervisada por personal certificado y, sobre todo, prestamos especial atención a la formación y concienciación del personal".

El sentido común del ciberdelincuente

Los Ciberdelincuentes manejan el negocio del volumen, saben que tienen más éxito en el ataque de miles de empresas sin protección que en un ataque a una sola gran empresa bien Ciberprotegida, porque cuando la Ciberseguridad está bien implementada y supervisada, puede rechazar miles de ataques por minuto, cada hora, cada día y cuando alguno logre pasar, tiene efectos muy limitados y fácilmente reversibles. "Prevenir es siempre mejor que lamentar, por eso en FORLOPD cuidamos de la información y continuidad de su empresa, desde todos los ángulos normativos y defensivos", concluye Mario Ramírez, director general de Forlopd.

FORLOPD®
seguridad en la información
www.forlopd.es

ENTREVISTA **Rodolfo Fabregad** Responsable Departamento Técnico-Jurídico de Forlopd

"El triángulo tecnología-procesos-usuarios debe estar blindado ante brechas de seguridad"

En ciberseguridad se comenta que la pregunta no es si intentaran entrar, sino cuando lo han hecho…

Hoy en día, la continuidad de negocio, nos parezca evidente o no, depende total y absolutamente de los datos e información que se almacenan, procesan y fluyen de manera eficiente y veloz en los ordenadores y redes. Nos movemos en un entramado profesional, crecientemente digital y cada vez más intercomunicado. Actualmente se detectan cerca de un millón de nuevos virus informáticos al día y los organismos especializados clasifican a las empresas en dos grandes grupos: las que han sido atacadas y las que lo están siendo.

¿Qué servicios ofrecéis desde FORLOPD a vuestros clientes?

Nuestro principal interés es blindar al cliente en cuanto al cumplimiento normativo y el correcto tratamiento de los datos y su seguridad. La implantación y mantenimiento del Reglamento Europeo de Protección de Datos (R.G.P.D), auditorías, destrucción segura de documentos (físicos y digitales), formación de responsables y usuarios… Junto con la Ley de Servicios de Sociedad de la información L.S.S.I-C.E., Corporate Compliance y normas de calidad ISO. Ofrecemos a nuestros clientes el poder disponer de un gran equipo de expertos en cada una de estas disciplinas que aportan el valor de un equipo trabajando para obtener unos mismos objetivos.

¿El trabajo telemático aumenta los riesgos?

Es evidente, a mayor actividad en la red, mayor es el riesgo. Una de las medidas con mayor aplicación, en el periodo de emergencia con motivo del COVID-19, ha sido el teletrabajo. Este panorama es terreno abonado para los delincuentes que operan en la red. La presencia digital de los ciudadanos es en estos momentos más intensa que nunca, con intrusiones ilegítimas en los sistemas, tanto en empresas como en particulares. El envío de software malicioso para el secuestro de datos -historiales médicos, por ejemplo, en las actuales circunstancias- o la suplantación de la identidad digital son prácticas delictivas en auge. Se debe vigilar el remitente de los mensajes y, ante la duda, desconfiar y no abrir enlaces ni descargar archivos sin la debida cautela.

¿Cuáles son las medidas indispensables para cualquier empresa?

Es obligatorio el cumplimiento de la Ley de protección de datos para cualquier empresa o profesional liberal que maneje datos de carácter personal en el desarrollo de su actividad. Desde FORLOPD recomendamos mantener al día las políticas de seguridad y tratamiento de la información que la legislación y el reglamento europeo exigen en su articulado.

Una buena implantación y supervisión de herramientas y procedimientos que ayuden a este cumplimiento se debería considerar el Kit de Supervivencia necesario para cualquier empresa, sin dejar de prestar especial atención a la necesaria formación y concienciación del personal con acceso a la información. El triángulo que forman la tecnología, los procesos y los usuarios, debe estar completamente blindado ante las posibles brechas de seguridad que pueden poner en compromiso la seguridad de la información.