¿Cómo establecer una cultura de seguridad en tu empresa?

Una cadena es tan fuerte como su eslabón más débil Esta frase tan popular significa que aunque las organizaciones inviertan mucho en dispositivos tecnológicos y en soluciones técnicas para proteger de manera adecuada los sistemas de información, si alguno de ellos falla, toda la seguridad se ve comprometida. El usuario es un eslabón más de la cadena… y la experiencia ha ido demostrando que es uno de los eslabones más débiles, por donde esta cadena de seguridad se rompe. Para cambiar esta situación, es necesario invertir también en la formación en seguridad a usuarios. Siendo conscientes de que: El usuario es el eslabón más **IMPORTANTE** de la cadena de la seguridad. Tenemos que ser conscientes de que a la hora de hablar de seguridad de la información, la tecnología nunca es suficiente. Es importante, pero a la hora de la verdad los auténticos protagonistas de la seguridad en las organizaciones son los usuarios finales que son los que gestionan y utilizan los sistemas de información de nuestra organización.

¿Cómo establecer una cultura de seguridad en la empresa?

Desarrollar e integrar una cultura de seguridad dentro de nuestra organización es uno de los objetivos más complejos de alcanzar. En primer lugar porque su aplicación requiere de unos plazos de tiempo amplios y de acciones continuadas en el tiempo; en segundo lugar, y mucho más importante, porque hablamos de personas. Conseguir que nuestros empleados interioricen en sus quehaceres cotidianos una manera de trabajar que garantice que las cosas se hacen bien en materia de seguridad de la información no es una tarea sencilla. Habitualmente los empleados ven los protocolos de seguridad que implantamos en nuestras organizaciones como una complicación o molestia.

La percepción que tienen es que la seguridad es incómoda y dificulta sus actividades cotidianas imponiendo limitaciones. Es necesario revertir esa visión negativa y abordar las acciones necesarias para conseguir crear una auténtica cultura de la seguridad dentro de nuestra empresa.

Para mantener un adecuado nivel de seguridad se debe:

- Realizar acciones de formación de seguridad.
- Establecer políticas, normativas y procedimientos de seguridad.
- Supervisar que se cumplen las buenas prácticas en seguridad.
- Realizar acciones de sensibilización y concientización en seguridad para empleados.

Realizar acciones de formación en seguridad para empleados

Tradicionalmente la seguridad de la información en las organizaciones se ha entendido como un gasto que no aporta valor al negocio, pues es muy difícil ver el retorno de la inversión en medidas que no se perciben como productivas. La formación en materia de seguridad, hasta ahora ha tenido un protagonismo casi nulo en los planes de formación de las empresas. Y si se llega a abordar, ésta se realiza de manera puntual o a un grupo reducido de empleados. De hecho, si preguntamos por iniciativas relacionadas con la formación en seguridad, veremos que únicamente se tratan acciones relacionadas con la seguridad en el puesto de trabajo y la prevención de riesgos laborales, dejando fuera los ámbitos de la seguridad de la información. De hecho, el Reglamento General de Protección de Datos (RGPD) contempla como una obligación de nuestra empresa formar a los empleados de la organización en materia de seguridad de los datos de carácter personal, garantizando así que son gestionados de una manera adecuada y conforme a la ley.

Es fundamental que seamos conscientes de la importancia de formar a nuestros empleados en materia de seguridad de la información para nuestros intereses como organización, y no sólo en materia de protección de datos personales, sino también desde el punto de vista de toda la información que trata la organización: datos de facturación, tarifas, márgenes, sistemas de producción, clientes, proveedores, acuerdos, etc. Sin embargo, no todo el personal de una organización necesita el mismo tipo ni grado de formación en materia de seguridad. La formación que necesita el personal técnico que gestiona los servidores no debe ser la misma que reciba el usuario final que sólo dispone de acceso a una pequeña parte de la información corporativa.

Fuente de información:
Instituto Nacional de Ciberseguridad