

La seguridad pasa porque nos concienciamos de su importancia



Estamos viviendo un imparable crecimiento y evolución de las capacidades tecnológicas y de comunicaciones tanto en el ámbito empresarial como personal. Cada vez demandamos una mayor "conexión" y esto nos lleva a un punto de convergencia de nuestro entorno digital: laboral y particular.

Esto altera el perímetro de seguridad y hace que los riesgos y las vulnerabilidades crezcan exponencialmente; también los medios y mecanismos para proteger la información pero **hay un componente no tecnológico que representa la mayor grieta: el factor humano**. Somos nosotros mismos, en un alto porcentaje, los responsables de los incidentes de seguridad con más impacto en las empresas, y **de ahí que un buen plan de concienciación de los usuarios sea una prioridad para las compañías**.

A principios de mes, **AUTELSI** (Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información) celebraba un evento, en el que se presentó un interesante **estudio** elaborado por el grupo de Calidad y Seguridad de esta asociación: "**Concienciación en seguridad de la información**", que incluye una **guía de buenas prácticas**, aborda asuntos como las implicaciones que tienen en los negocios los incidentes de seguridad, los retos futuros en esta materia como el crecimiento imparable de BYOD (*Bring Your Own Device*) y, sobre todo, la cada vez más acuciante importancia de la concienciación de los usuarios para poder reducir los riesgos.

El objetivo del estudio, en el que ha colaborado Telefónica, es conseguir un nivel adecuado de conocimiento, por parte de cada empleado de las compañías, de la conducta que ayuda a conseguir el nivel de seguridad de la información que se necesita.

En este informe se tratan, entre otros muchos aspectos, los indicadores que miden el grado de concienciación de las empresas, qué departamentos participan o lo impulsan, y sobre qué ámbitos aplica. También tiene en cuenta la dificultad que supone la implantación de un proceso de este tipo y los beneficios que se obtienen.

En el día de su presentación, los responsables de seguridad y CISOs de Mediaset, Renfe y Repsol compartieron con la audiencia sus experiencias a la hora de planificar su estrategia en materia de concienciación y qué tipo de herramientas o soluciones aplican, o tienen previsto aplicar, para lograr este objetivo.

Me resultó interesante el enfoque de que **la normativa de seguridad hay que explicarla, pero es necesario hacer un importante trabajo previo**. Se trata de **acercar el área de seguridad a toda la organización**, de forma que se transmita ese conocimiento de manera divulgativa y el mensaje no resulte críptico. **El plan de concienciación debe estar promovido por un equipo multidisciplinar**.

En ocasiones falla el lenguaje –se dijo–, ocurre que los **directivos no dan ejemplo y falta *engagement* con las personas**. La forma en que se comunica para concienciar en seguridad es fundamental y también en esto la innovación ayuda: la "**gamificación**" y el **humor** se presentaron como herramientas probadas de éxito.

Sensibilización, concienciación, formación y capacitación serían los **pasos para modificar el comportamiento de los empleados**. De cada uno de ellos porque **la información es el activo más importante de una empresa y cualquier persona la gestiona**, por lo que todos debemos aplicar medidas de seguridad.

La seguridad, además, no lo olvidemos, es dinámica y la concienciación debe ir a la par

"Concienciación en seguridad de la información" de Autelsi, convergencia entre entorno personal y laboral, crecimiento de BYOD, el factor humano es una grieta en seguridad, Gamificación, humor, la información como el activo más importante de una empresa, normativa de seguridad, nuevo perímetro de seguridad, sensibilización y concienciación de los empleados en materia de seguridad