

El usuario y la seguridad de la información

El usuario y la seguridad de la información

Introducción

Aunque las tecnologías de la información son un elemento indispensable en cualquier organización, deben utilizarse de forma adecuada para evitar riesgos de seguridad en la gestión de la información.

Por ello, es importante considerar que el usuario final, tiene un papel crucial en la seguridad de la información, ya que los usuarios son quienes manejan, almacenan, transfieren, y gestionan finalmente la información de una organización.

En ese sentido, en el ámbito de la ciberseguridad se tiene como uno de los objetivos para fortalecer la seguridad, que el factor humano y su formación sea el eslabón más fuerte para proteger la información ya que son precisamente los usuarios, el blanco de los ciberdelincuentes, para ejecutar un delito.

Los pilares de la seguridad de la información.

La seguridad de la información se basa en tres dimensiones, que son los pilares sobre los que se busca aplicar las medidas de protección de la información:

Disponibilidad de la información: significa que la información esté accesible cuando la necesitemos. Algunos ejemplos de falta de disponibilidad de la información son: cuando no se puede acceder al correo electrónico institucional por un error de configuración, o bien, cuando se presenta un ataque de denegación de servicio, en el que el sistema «cae» impidiendo accesos legítimos. En ambos casos se tienen consecuencias graves.

Integridad se refiere a que la información sea correcta y esté libre de modificaciones y errores. La información puede ser alterada intencionalmente o ser incorrecta y la institución puede basar sus decisiones en ella.

La alteración malintencionada en los archivos del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas, son algunos ejemplos de que se ha perdido la integridad de la información.

Confidencialidad implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know, es decir que la información solo puede darse a conocer por las personas, entidades o sistemas autorizados para su acceso. El robo de información confidencial de un atacante a través de Internet, la divulgación no autorizada a través de las redes sociales de información confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener acceso, son algunos ejemplos de que la confidencialidad de la información se ha afectado.

El usuario y la seguridad de la información



Pilares de la información. imagen tomada del documento formativo del consejo 1 del kit de Metared.

Para conservar y proteger estos 3 pilares de la información, la Universidad debe realizar una evaluación de todos los activos de información para determinar las medidas, controles y mecanismos que deben implementar y que permitan garantizar la seguridad de la información.

Sin embargo, más allá de la inversión que realice una organización en todas esas medidas técnicas para proteger sus sistemas y la información que maneja, la seguridad depende por completo de un único filtro, el usuario. Por ello, es fundamental que los usuarios adquieran una cultura y formación en materia de seguridad para proteger todo el conjunto de información que maneja una organización, con la finalidad de evitar posibles brechas de seguridad.

REFERENCIAS

1. INCIBE - Protección de la información

https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf