Dato versus información

Información y datos, son conceptos muy usados dentro de la informática. Aunque se relacionen, ambos cuentan con diferentes significados, repasemos algunos y veamos sus diferencias:

Un dato puede ser un número, una letra o un hecho sin mayor descripción. Es decir, sirve para cuantificar, pero por si solos los datos no reflejan un análisis.

Por su parte, la información comprende el conjunto de datos que, luego de ser procesados, indican un mensaje revelador que contribuye a la toma de decisión, al momento de tener que generar hipótesis o resolver un problema.

En resumen, mientras más información se tenga, más conocimiento logramos sobre un tema.

¿Y … entoces?

- ***Los datos*** suelen ser individuales, concretos y específicos, mientras que la información está integrada por un conjunto de datos distintos o no, y agrupados en gran extensión para poder producir análisis.
- ***La información*** tiene por objeto comunicar algo, mientras que el dato no muestra mensaje alguno, es decir, por sí solo y de manera aislada no produce un mensaje coherente.

¿Qué es la Seguridad Informática?

La Seguridad Informática es la disciplina que se encarga de proteger la confidencialidad, integridad y disponibilidad de la información dentro un sistema informático.

Defensa en profundidad

La defensa en profundidad apunta a implementar varias medidas de seguridad con el objetivo de proteger un mismo activo. Utiliza varias capas, en las que cada una provee un nivel de protección adicional a las demás.

Dicha estrategia ha sido formulada por la NSA (National Security Agency), de Estados Unidos, como un enfoque para la seguridad informática y electrónica. De forma original, este concepto se usó como una estrategia militar para retrasar más que prevenir el avance del enemigo, lo que permitía ganar tiempo muy valioso en el campo de batalla.

Debemos implementar dichas medidas basándonos en el paradigma de Proteger, Detectar y Reaccionar. Esto significa que, además de incorporar mecanismos de protección, debemos estar preparados para recibir ataques, e implementar métodos de detección y procedimientos que nos permitan reaccionar y recuperarse de dichos ataques.

Es muy importante balancear el foco de las contramedidas en los tres elementos primarios de una organización:

- Personas.
- Tecnología.
- Operaciones.

Personas

Alcanzar un nivel de seguridad óptimo empieza con el compromiso de la alta gerencia, basado en un claro entendimiento de las amenazas; el cual debe ser seguido por la creación de políticas y procedimientos, la asignación de roles y responsabilidades, asignación de recursos y capacitación a los empleados. Además, es necesaria la implementación de medidas de seguridad física y control de personal para poder monitorizar las instalaciones críticas para la organización.

Tecnología

Para asegurar que las tecnologías implementadas son las correctas, deben ser establecidas políticas y procedimientos para la adquisición de la tecnología. Debemos implementar varios mecanismos de seguridad entre las amenazas y sus objetivos. Cada una debe incluir mecanismos de protección y detección.

Operaciones

Se enfoca en las actividades necesarias para sostener la seguridad de la organización en las tareas del día a día. Este tipo de medidas incluye las que enumeramos a continuación: mantener una clara política de seguridad, documentar todos los cambios hechos en la infraestructura, realizar análisis de seguridad periódicos e implementar métodos de recuperación