


Introducción a la Ciberseguridad


Módulo 1

La información como un bien y la necesidad de protegerla

La información como un bien y la necesidad de protegerla

Información y **datos** son conceptos básicos dentro de la informática y, si bien en el lenguaje cotidiano podrían entenderse como lo mismo, cuentan con diferentes significados. A continuación descubriremos cuál es la diferencia.



- **Dato:** un dato es un símbolo que describe un hecho, una condición, un valor o una situación. Un dato puede ser una letra, un número, un signo ortográfico o cualquier símbolo y que representa una cantidad, una medida, una palabra o una descripción.
 - **Información:** se refiere al conjunto de datos que están procesados y analizados de modo que podemos predecir o entender la realidad por medio de ellos.
- 

Veamos un ejemplo

80%, alfabetismo y 2000 son tres datos que por sí solos no tienen sentido. Estos datos se podrían convertir en información de la siguiente forma:

Durante el año 2000 se ha detectado en el país una tasa del 80% de alfabetismo.



Determinar qué información debemos proteger

Cuando uno se encuentra en la posición de llevar adelante una estrategia que defina qué activos serán los que tiene que proteger, deberá tener en cuenta principalmente aquellos que son de vital necesidad para la organización. En la actualidad, es necesario prestar muchísima atención a aquellos bienes/activos intangibles, en especial la **información necesaria para que se puedan realizar las actividades diarias**.

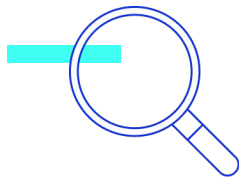
Para determinar qué es lo que debemos proteger es casi obligatorio entender **cómo funciona una empresa, qué procesos/actividades realiza, por medio de qué *software* lo hace y en qué *hardware* se sustentan dichos programas**.

Por ello, tendremos que evaluar, en conjunto con el resto de las áreas de la organización, qué información es importante resguardar y cuál no. Tengamos en cuenta que no se puede proteger el ciento por ciento de todo porque es costoso. Es muy difícil comprender qué proteger si no se conoce cómo opera una organización. De ahí la importancia de hacer un buen **relevamiento inicial del estado de una empresa**, comprender sus formas, sus necesidades, los riesgos propios de cada industria y, con ello, poder **diseñar una estrategia de seguridad** para minimizar la probabilidad de eventos negativos, que dañan de forma parcial o total las actividades que se realizan.

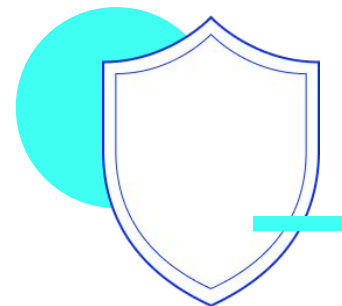
¿Qué proteger?

Son muchas las tareas tendientes a garantizar seguridad en un espacio de trabajo, entre las principales:

1. Mantener actualizada toda la infraestructura tecnológica para evitar que sea vulnerable.
2. Respalidar la información y servicios críticos con copias de seguridad y redundancia de equipos.
3. Gestionar las cuentas de usuario en los distintos sistemas y minimizar los privilegios que tienen para realizar acciones.
4. Controlar el acceso de los usuarios mediante mecanismos de autenticación.
5. Proteger los dispositivos de infecciones de programas maliciosos.
6. Asegurar los equipos y sistemas que se usan para evitar funcionamiento por defecto o de fábrica que son altamente vulnerables.



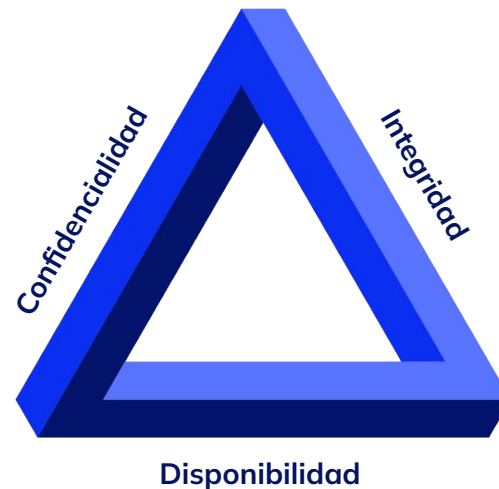
Toda estrategia de seguridad incluirá una serie de actividades para proteger la organización y, dependiendo de cada empresa, podrá ser distinto el plan que se elabore. No obstante, siempre tendrán en común los **pilares de la seguridad**, la famosa **tríada CIA: Confidencialidad, Integridad y Disponibilidad (en inglés, Availability)**.



Tríada CIA: Los pilares de la Seguridad

La correcta **Gestión de la Seguridad de la Información** busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la **confidencialidad, integridad y disponibilidad de la información**.

Es preciso anotar que la seguridad no es ningún hito, es más bien un **proceso continuo** que hay que gestionar, conociendo las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, al tener en cuenta a su vez, **las causas de riesgo y la probabilidad de que ocurran**, así como **el impacto que pueden tener**.



Confidencialidad

La confidencialidad es la propiedad que **impide la divulgación de información a personas o sistemas no autorizados**. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la autorización.

Por ejemplo, una transacción de tarjeta de crédito en Internet, requiere que el número de tarjeta de crédito sea transmitida desde el comprador al comerciante y del comerciante a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que

contiene la banda magnética durante la transmisión de estos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.



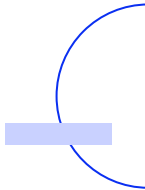
Integridad

Es la propiedad que busca **mantener los datos libres de modificaciones no autorizadas**. No es igual a integridad referencial en bases de datos. A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por

personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.

La integridad de un mensaje se obtiene al adjuntar otro conjunto de datos de comprobación de la integridad: la firma digital, esta es uno de los pilares vitales de la seguridad de la información.



Disponibilidad

La disponibilidad es la **condición de la información de encontrarse a disposición de quienes deben acceder a ella**, ya sean personas, procesos o aplicaciones. A grandes rasgos, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. El objetivo de los sistemas

de alta disponibilidad es que deben estar disponibles en todo momento, para evitar interrupciones del servicio debido a cortes de energía, fallos de *hardware*, y actualizaciones del sistema.





**¡Sigamos
trabajando!**

