[Curso de Hacking Ético](https://platzi.com/clases/ethical-hacking/)

**ArtículoCopias de seguridad. Defensa en lo profundo**

[**Alan Joaquín Baeza Meza**](https://platzi.com/%40ajbaeza)

26 de Abril de 2019

La información que tratamos en nuestros procesos productivos es el activo más importante de nuestros despachos y el de nuestros clientes. Y, como tal, debe protegerse adecuadamente. Esto es lo que conocemos como seguridad de la información.
Debemos garantizar la disponibilidad, integridad y confidencialidad de la información del despacho y de la que es custodio, tanto la que se encuentra en soporte digital, como la que se gestiona en papel.

Las copias de seguridad son la salvaguarda básica para proteger la información. Dependiendo del tamaño y necesidades del despacho, los soportes, la frecuencia y los procedimientos para realizar las copias de seguridad pueden ser distintos.

El soporte escogido dependerá del sistema de copia seleccionado, de la fiabilidad que sea necesaria y de la inversión que deseemos realizar. Estas tres variables van estrechamente unidas y deben estar en consonancia con la estrategia de nuestra organización.

En la implantación de un sistema de copias debemos tener en cuenta al menos las siguientes consideraciones:

1. Analizar la información de la que se va a realizar la copia, así como los sistemas y repositorios donde se encuentra.
2. Debemos tener en cuenta las configuraciones de dispositivos de red, los equipos de los usuarios o incluso información en smartphones. Este paso debe permitirnos descartar información sin relación directa con el negocio o ficheros históricos de los que ya existen copias.
3. Debemos definir formalmente el número de versiones que vamos a almacenar de cada elemento guardado y su periodo de conservación. Esto es lo que se conoce como política de copias de seguridad. En esta decisión influyen las necesidades del negocio y la capacidad de almacenamiento disponible. En cualquier caso, dependerá de la complejidad de la organización y el volumen de los datos. Si el volumen de información es bajo, puede ser factible realizar una copia total diaria.

**Existen 3 tipos de copias principalmente:**

* **Total:** Se realiza una copia completa y exacta de la información original, independientemente de las copias realizadas anteriormente.
* **Incremental:** Únicamente se copian los archivos que se hayan añadido o modificado desde la última copia realizada, sea total o incremental.
* **Diferenciales:** cada vez que se realiza una copia de seguridad, se copian todos los archivos que hayan sido modificados desde la última copia completa.
Hay que llevar un control de los soportes de copia, mediante un etiquetado y un registro de la ubicación de los soportes. Las copias de seguridad tienen que estar en un lugar protegido, por ejemplo, en una caja de seguridad bajo llave.
Esto implica también llevar el control de la vida útil de los mismos, para evitar que el deterioro físico afecte a la integridad de los datos. Si la información almacenada en las copias es confidencial, debemos valorar la posibilidad de cifrarlas, para evitar que, ante una pérdida o sustracción de un soporte, sea posible acceder a ésta. Esta medida debe abordarse con especial cuidado para evitar la pérdida de información en caso de pérdida de las claves.
Debemos disponer de una copia de seguridad fuera de la organización, para evitar la pérdida de la información en caso de incendio, inundación, robo o ser víctima de un malware que rastree nuestra red buscando estas copias de seguridad. Es necesaria una selección adecuada de la localización de dichas copias.

**Defensa en profundidad.**
En el área militar se utiliza el término defensa en profundidad para denotar el uso de varias líneas de defensa consecutivas, cada una de ellas con un nivel de protección creciente, en vez de una única barrera muy fuerte. Las ideas de su implementación teórica se basan en que un potencial enemigo perderá fuerzas al superar cada barrera y, además, dispersará sus recursos y potencia, con lo cual se debilitará.
Así, quien se defiende puede centrar sus esfuerzos en la reorganización y la acción estratégica. En nuestra área, tomamos prestado este concepto para aplicarlo a los sistemas informáticos.



Este concepto cobra vital importancia, no solamente desde la óptica del responsable de seguridad de la información de las organizaciones –encargado de velar por que todos los controles funcionen de manera adecuada–, sino también desde la del atacante, quien es, en definitiva, el que deberá saltear estos controles para cumplir su objetivo.