educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Módulo 1

Introducción

La Seguridad

Desde los primeros días de la informática, siempre ha existido la necesidad de establecer algún tipo de **control o protección** sobre el equipamiento y eventualmente, la información generada. Dichos controles y niveles de protección han evolucionado acompañando el avance en el campo de la informática y las comunicaciones.

Así como inicialmente los únicos mecanismos de protección pasaban, por ejemplo, por proteger físicamente el acceso al cuarto donde se albergaban las grandes computadoras con guardias de seguridad; conforme la computación fue evolucionando hacia equipos más pequeños y al alcance de más usuarios, este modelo dejó de ser eficiente. Se tuvo, entonces, que complementar este tipo de controles físicos, con aquellos relacionados con aspectos de ***seguridad lógica***, en donde el principal foco de atención está dado a la **protección de los datos o información que estos dispositivos crean y manipulan**.

Hoy en día es más importante la información que estos equipos almacenan que el hardware que se utiliza para manipularla.

Del mismo modo, la proliferación de las redes de datos, requirió de nuevos cambios en los modelos de seguridad a aplicar por parte de las diferentes organizaciones, que preocupadas por la seguridad de la información relacionada con su actividad, requerían establecer ya no solo **controles** sobre los equipos, sino también sobre el **transporte de datos**. En tal sentido, el mayor impacto sin dudas, respecto de la seguridad relacionada con computadoras hasta ahora, lo haya provocado la llegada de **Internet**.

La nueva tendencia sobre uso de una gran cantidad de **dispositivos móviles y redes inalámbricas** como parte de la infraestructura tecnológica, ha requerido asimismo, que los profesionales en seguridad ajusten de nuevo sus procedimientos y desarrollen un conjunto de técnicas y controles, capaces de velar por la seguridad de la información relacionada con ellos.

Conclusión

La implementación de nuevas tecnologías trae aparejado el advenimiento de nuevas oportunidades de negocio, así como también riesgos, amenazas y nuevos vectores de ataque. Por eso, son requeridas como parte de un proceso continuo, la **revisión constante de los modelos de seguridad y la adecuación de controles,** de modo que se mantenga su vigencia.

Seguridad de la Información vs. Seguridad Informática vs. Ciberseguridad

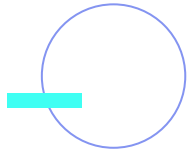
Seguridad de la Información vs. Seguridad Informática vs. Ciberseguridad

Actualmente se utiliza el término ***Seguridad Informática*** para entender todas aquellas actividades que realizan un particular u organización tendiente a proteger su respectiva información y equipos.

No obstante, con los años se han generado avances en materia de tecnología que obligaron a que existan diferentes disciplinas que trabajen la seguridad desde diferentes enfoques.

Podremos entender entonces, en las siguientes pantallas, las diferencias entre los conceptos:

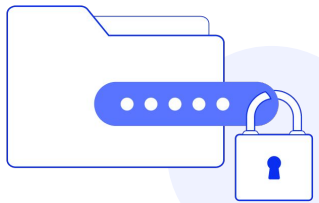
- **Seguridad de la Información.**
- **Seguridad Informática.**
- **Ciberseguridad.**



Seguridad de la Información

Es aquella disciplina que se encarga de velar por **la protección de los activos de información**, entendiendo éstos como aquellos datos o información importante para una organización, independientemente del formato que tengan, ya sea digital o físico, **a través de la reducción de los riesgos** propios que los puedan comprometer.

Se desarrollan normas y procedimientos que tienden a establecer **qué información se debe proteger,** pero no hacen hincapié en el cómo. Tiene una **mirada gerencial** de largo plazo.



Seguridad Informática

Es aquella disciplina que se encarga de **cómo proteger los datos o información que fueron definidos como importantes para la organización**. Centra su trabajo en gestionar qué herramientas utilizar para dar la seguridad necesaria a la información, como a los dispositivos que se utilicen en la organización.

Posee una **mirada más táctica que estratégica**, porque sus funciones son de corto y mediano plazo, a la vez que es **altamente técnica**, porque es aquí donde se desarrollarán todas las tareas propias de seguridad que fueron definidas por la normativa y procedimientos creados por *Seguridad de la Información*.

Ciberseguridad

Es la seguridad informática aplicada al entorno de Internet.

Hoy el paradigma de trabajo está puesto en los **servicios *cloud***, donde ya no es necesario que las empresas cuenten con infraestructura propia. Ahora todo está en un servidor de una empresa y solamente se debe gestionar.

Resumen

Seguridad de la Información define qué es lo que hay que proteger (**datos + información**) en una organización y ***Seguridad Informática*** establece **cómo asegurará** esos activos, con qué herramientas, etc. La ***ciberseguridad*** hará lo mismo, pero centrándose en **Internet**.

Según la envergadura de la organización, encontraremos distintas áreas que desarrollen tareas de seguridad. Por lo general, las grandes empresas, como bancos y financieras, tendrán un área de Seguridad de la Información, desde la que se determinará qué información/datos se deberán proteger, y después desplegarán las distintas subáreas para cumplir todas las tareas necesarias de seguridad, desde el punto de vista técnico.

En otros tipos de organizaciones, por ejemplo las Pymes, quizá no cuenten con un área específica de seguridad, sino con una de *Sistemas* o *Tecnología*, cuyo personal realizará tareas de seguridad. En estos casos, el nivel y profundidad de tareas, por lo general, no suele ser muy amplio, sino más bien tendiente a ser funcional. Dicho en otras palabras, acompañan las tareas del área de *Tecnología* pero no se desarrolla realmente la seguridad como disciplina.

La Seguridad de la Información como una inversión

Es un error ver a la Seguridad de la Información como un gasto y no como una inversión

Un factor clave de entender es que, aún hoy en día, en muchas organizaciones (e inclusive personas) se considera a la Seguridad de la información como un gasto y no como una inversión. Es decir, no pueden ver que su negocio o datos personales, de ser violados, pueden afectar gravemente la continuidad de sus actividades. Por ejemplo, si una empresa el lunes cuando tiene que comenzar sus actividades se alerta que toda la información que tenía guardada en las computadoras de sus usuarios y en los servidores ha sido eliminada, se dará cuenta que no podrá realizar ninguna actividad dado que no sabe qué datos venía manejando y recién allí percibirán el valor que tenía esa información para trabajar.

En ocasiones, las pequeñas empresas prefieren evitar el gasto de una solución como un antivirus, un firewall, etc. porque resulta costoso, pero no se dan cuenta que **el costo final, si su información se pierde, será mucho mayor**.

Ramas dentro de la Seguridad

Ramas dentro de la Seguridad

Habitualmente, las personas cuando deciden estudiar o trabajar en el área de Sistemas o Informática, piensan en perfiles como programador o reparador de PC. Si bien estos perfiles son requeridos en el mercado, existen muchos más que se pasan por alto, y que son también muy demandados y bien remunerados.

Cuando analizamos las tareas que se realizan en el área de seguridad, podemos encontrar que son varias y de diferente complejidad. Si bien cuando uno estudia abarca todos los campos que integran esta disciplina, una vez dentro de un trabajo podrá especializarse en un campo u otro.

Podemos encontrar ramas como:

- **Seguridad de Aplicaciones:** Implica analizar la seguridad en aplicaciones (Web, Mobile, API) para ver si existen vulnerabilidades que puedan permitir que un tercero tome control sobre el software y lo manipule a su provecho.
- **Seguridad en Redes:** supone analizar el estado de la red de la organización, a fin de evitar que existan atacantes tanto desde afuera hacia adentro y lo contrario, como así también la transferencia de archivos entre redes.
- **Ethical Hacking:** Implica poner a prueba una organización ocupando el rol de ser *atacante* con las debidas autorizaciones, con el objetivo de encontrar fallas, explotarlas y reportar cómo se logró comprometer la seguridad, para que luego sean corregidas.
- **DevSecOps:** Implica incluir la seguridad en todo proyecto de desarrollo desde el inicio y en el resto de las etapas, hasta su puesta en producción y post control, cuando esté activo.
- **OSINT:** Implica la búsqueda de información en fuentes abiertas en Internet, para encontrar determinados datos; los cuales, luego serán utilizados en distintos fines: fraudes, estafas, análisis de mercado, etc.

Como podemos notar, al trabajar con seguridad hay que pensar en más de un área dentro de una organización, ya que la información se encuentra repartida por varios lugares y está en constante movimiento. Con lo cual, tendremos que saber de otras disciplinas para poder encontrar la mejor forma de asegurar nuestros sistemas. Por dicha razón, **estudiar seguridad nos dará conocimiento general de otras áreas y disciplinas.**

educación IT
CODE YOUR FUTURE

¡Sigamos trabajando!