Seguridad Informatica

Trabajo Práctico N°3

Seguridad de la Información y Ciberseguridad

En las últimas décadas, como consecuencia de la popularización del uso de Internet, la noción de "información adquirió un lugar central en distintos ámbitos de la vida social. Con el proceso de digitalización a nivel global, la cantidad y velocidad de producción y circulación de los "datos" tuvo un crecimiento exponencial, poniendo de relevancia la importancia de la protección y seguridad de dicha información. Ahora bien, existen distintos tipos de información, que a su vez requieren distintos niveles de protección.

Veamos con mayor profundidad algunas de estas distinciones.

LA INFORMACIÓN: algunas clasificaciones

A grandes rasgos, podríamos definir a la información como un conjunto organizado y procesado de datos, de los cuales se puede extraer algún tipo de conocimiento. Aisladamente, los datos no constituyen necesariamente una información en si misma, pero puestos en relación y analizados en su conjunto, pueden brindar conocimientos de distinta indole

Si bien existen diversos criterios para clasificar los tipos de información, podemos distinguir algunas categorías:

1. Información pública: es todo tipo de información, en cualquier formato (texto, imagen, etc.) en poder del Estado o generado, obtenido o financiado con fondos públicos. Todas las personas fisicas o juridicas pueden solicitar información pública sin necesidad de explicar el motivo de su pedido.

2. Información personal es toda la información que se relaciona con las personas fisicas y que puede identificarias, como por ejemplo: nombre, apellido, número de DNI, dirección, teléfono, situación crediticia, imagen, etc.

3. Información confidencial o clasificada es la información a la que sólo puede acceder un grupo reducido de personas, debido a la naturaleza secreta, peligrosa, delicada o privada de los datos que contiene.

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Como acabamos de ver, si bien hay información que es pública, a la que cualquiera tiene derecho a acceder, existen otro tipo de informaciones cuya circulación sin consentimiento puede implicar un nesgo para las personas u organizaciones implicadas. Esta información puede alojarse ya sea en soportes digitales (computadoras, celulares, tablets, pendrives, etc.), como así también en soportes no digitales (por ejemplo, papeles, documentos o conversaciones privadas). Podemos entonces distinguir tres conceptos

1 Seguridad informática: protección de las infraestructuras tecnológicas que soportan el conjunto de actividades que lleva adelante una organización para gestionar su información.

2. Seguridad de la información: conjunto de acciones que buscan preservar la confidencialidad, integridad y disponibilidad de la información, más allá del soporte en el que esta se aloje (es decir, sea o no digital).

3. Ciberseguridad o seguridad informática: se trata de un concepto más reciente, que surge a partir de la expansión del uso de Internet y de los dispositivos electrónicos. A diferencia de la seguridad de la información, que es una noción más general, la ciberseguridad comprende al conjunto de acciones que buscan preservar la confidencialidad, integridad y disponibilidad de la información alojada especificamente en soportes digitales. Implica la "salvaguarda de las personas, las organizaciones, la sociedad y las naciones de los riesgos cibernéticos, entendiéndose por 'salvaguarda la mantención de los riesgos cibernéticos en un nivel tolerable

Seguridad de la información

La seguridad de la información es, entonces, el conjunto de acciones y medidas que permiten resguardar y proteger la información, ya sea de una persona, organización o sistema, en los distintos soportes en los que esta pueda encontrarse. La triada CID (Confidencialidad, Integridad y Disponibilidad) es un modelo que nos permite alender a algunos aspectos claves a la hora de tomar medidas para la seguridad de la información.

Veamos cuáles son las características de esta triada:

1. Confidencialidad: busca que la información pueda ser vista y obtenida sólo por quienes deben hacerlo en razón de su derecho personal o actividad en una organización, evitando que personas no autorizadas puedan acceder a ellas. El cifrado de datos, las contraseñas, los tokens de seguridad y la verificación biométrica son algunos de los métodos más utilizados para garantizar la confidencialidad.

2. Integridad: implica que la información no sea modificada, eliminada o generada por personas no autorizadas. El control de versiones y las copias de seguridad son herramientas útiles para asegurarse que la información no se vea alterada indeseadamente.

3. Disponibilidad: garantiza que el acceso a la información pueda realizarse cuando y desde donde sea requerida por las personas autorizadas. Para ello, es fundamental que, en caso de tratarse de dispositivos electrónicos, el hardware y el software funcionen correctamente, así como el acceso a Internet en caso de ser necesario.

Confidencialidad

Seguridad de la Información

Integridad

Disponibilidad

Existen también otras características que debe poseer la información para conservar su valor Sin entrar en tecnicismos, mencionamos algunas brevemente:

Legalidad: que cumpla con leyes y normas

Autoría: tener certeza de dónde proviene

Auditabilidad: poder reconstruir su generación.

No repudio que la otra parte no pueda negar que la originó o recibió

Autenticidad: asegurar la validez de la información en tiempo, forma y distribución,

así como su origen y demás requisitos que le apliquen.

Confiabilidad: que se garantice su fiabilidad. Seguridad de la información

Ciberseguridad

Como se mencionó anteriormente, la ciberseguridad es un concepto más reciente, que hace referencia a la protección de la información que se genera y procesa en los dispositivos electrónicos. Los y las especialistas en esta materia buscan proteger las computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de posibles ataques maliciosos

Las amenazas a la información pueden provenir de diversas causas. Si bien en la gran mayoría de los casos son provocadas por softwares o programas maliciosos, también pueden provenir de intrusos (personas que consiguen acceder a datos sin autorización, como los crackers), por fallos en los sistemas informáticos (que provoquen una pérdida total o parcial de la información), siniestros (tales como robos, incendios, inundaciones u otro tipo de catástrofes), etc.

Otra manera de clasificar los tipos de amenazas es según si su origen es interno o externo:

Amenazas extemas son aquellos ataques que se ejecutan de forma remota, por fuera de la red. Para poder llevar adelante este tipo de ataques, el ciberdelincuente debe llevar adelante una serie de pasos con la finalidad de vulnerar la red.

Amenazas internas: son aquellos ataques que se producen de forma interna, sin la necesidad de acceder remotamente a los dispositivos. Este tipo de acciones suelen darse en ámbitos de mayor confianza, en los que el atacante logra acceder a la información a partir de conseguir algunos datos simples como contraseñas.

Características	Seguridad informática	Seguridad de la información	Ciberseguridad
Definición	Protección de las infraestructuras tecnológicas que soportan el conjunto de actividades que lleva adelante una organización para gestionar su información	Conjunto de acciones que buscan preservar la confidencialidad, integridad y disponibilidad de la información, más allá del soporte en el que este se aloje(es decir, sea o no digital)	Conjunto de acciones que buscan preservar la confidencialidad, integridad y disponibilidad de la información alojada específicamente en soportes digitales
Ámbito de aplicación	Infraestructuras tecnológicas de una organización	Información en cualquier soporte	Información en soportes digitales
Enfoque	Protección de daños al software o hardware y robo de datos.	Protección de la información	Protección de la información digital
Tipo de información	Personal	Confidencial	Publica, personal o confidencial
Soporte	Digital	Digital y no digital	Digital