Plataforma de
Aprendizaje Virtual

Conceptos Fundamentales sobre Ciberseguridad

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Unidad 1

Conceptos Fundamentales sobre Ciberseguridad

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Unidad 1

Concepto fundamentales sobre ciberseguridad

Este manual se realizó con la colaboración de la Dirección Nacional de Ciberseguridad, perteneciente a la Subsecretaría de Tecnologías de la Información de la Nación.

Un poco de Historia

Hoy en día, la idea de llevar en el bolsillo dispositivos pequeños y portátiles, conectados permanentemente a Internet, no nos resulta sorprendente. Los smartphones, computadoras portátiles, tablets y otros dispositivos forman parte de nuestra vida cotidiana, y cada vez más servicios, actividades y pasatiempos se realizan por medio de entornos digitales.

Sin embargo, para llegar a la "naturalización" de Internet, pasaron décadas de investigaciones, pruebas, errores y descubrimientos tecnológicos.

Los inicios de Internet se remontan a mediados del siglo XX. En un contexto de Guerra Fría, en el que Estados Unidos y la Unión Soviética se disputaban la hegemonía luego de la Segunda Guerra Mundial, la competencia tecnológica y científica entre ambos bloques era uno de los principales frentes de batalla. A fines de la década del '60, el Departamento de Defensa de los Estados Unidos creó ARPANET, una red de computadoras que permitía tener acceso a información militar desde cualquier punto del país. Quizás sin saberlo, estaban dando inicio a una revolución tecnológica sin precedentes.

Este primer sistema de comunicación descentralizada entre computadoras, lo que hoy conocemos como red de Internet, nació entonces con fines militares. Sin embargo, debido al fuerte potencial del sistema y al desarrollo de la PC (la computadora personal) durante los años '80, la red de Internet comenzó a expandirse y utilizarse en ámbitos laborales y domésticos. Poco a poco, gracias al avance en los desarrollos tecnológicos, el acceso a los dispositivos electrónicos se fue popularizando**.**

convirtiéndose, al cabo de unos años, en el medio de comunicación por excelencia a nivel mundial.

Importancia de la seguridad de la información

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 sí misma, pero puestos en relación y analizados en su conjunto, pueden brindar conocimientos de distinta índole.

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 físicas o jurídicas pueden solicitar información pública sin necesidad de explicar el motivo de su pedido. También puede interpretarse como aquella información que no tiene restricciones en cuanto a quiénes pueden accederla, es decir que cualquiera puede acceder a ella.

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

3. Información confidencial o clasificada: es la información a la que sólo puede acceder un grupo reducido de personas con la debida autorización, debido a la naturaleza secreta, importante, 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, existe otro tipo de información cuya circulación sin consentimiento puede implicar un riesgo para las

personas u organizaciones implicadas. Esta información puede alojarse ya sea en soportes digitales (computadoras, celulares, tablets, pen drives, 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 : se trata de un concepto más reciente, que surge a partir de la expansión del uso de Internet y de los dispositivos electrónicos interconectados. 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 específicamente en el entorno virtual o ciberespacio. 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. Esta última definición se encuentra contenida en una de las normas que componen la serie ISO/IEC 27000.

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 seguridad de la información se articula sobre tres dimensiones o propiedades que son los pilares sobre los que se aplican medidas de protección para proteger los datos. Veamos cuáles son las características de esta tríada:

1. Confidencialidad: la confidencialidad hace referencia a que la información es accesible únicamente

por el personal autorizado. En otras palabras, se busca que la información sea vista por quienes lo necesiten por cuestiones laborales o personales. 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, algunas técnicas de cifrado 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 así como el acceso a Internet funcionen correctamente, en el momento en que son requeridos.

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, es decir quien origina o transmite la información.
- Auditabilidad: poder reconstruir su proceso 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.

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 dispositivos electrónicos interconectados. Los y las especialistas en esta materia buscan proteger las computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos, de posibles ataques maliciosos.

¿Lo sabías?
El 30 de noviembre se celebra el Día Mundial de la Ciberseguridad. La efeméride comenzó a celebrarse en 1988, a partir de una iniciativa de la organización Association for Computing Machinery (ACM), con el objetivo de concientizar sobre los riesgos y prevenciones en el mundo digital.

Las amenazas a la información pueden provenir de diversas causas. Muchas de ellas son provocadas por softwares o programas maliciosos (conocidos como *malware* , concepto que profundizaremos en la Unidad 3), 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. En las próximas unidades veremos con mayor detalle algunas de las principales amenazas informáticas, y cómo protegernos de ellas.

Otra manera de clasificar los tipos de amenazas es según su origen, que puede ser interno o externo:

- **Amenazas externas:** son aquellos ataques que se ejecutan de forma remota, por fuera de la red que puede resultar afectada. Para poder llevar adelante este tipo de ataques, el ciberdelincuente debe seguir 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.

¿Lo sabías?
Aunque comúnmente utilizamos la palabra hacker como sinónimo de “pirata informático”, los expertos informáticos aclaran que esa definición se ajusta más al término cracker. ¿Cuál es la diferencia? Mientras que un hacker es una persona que usa sus conocimientos para descubrir vulnerabilidades y fallos en sistemas informáticos (y, eventualmente, mejorarlos), un cracker es quien se dedica a vulnerar dichos sistemas informáticos para cometer operaciones ilícitas.

¡Esperamos que hayas disfrutado esta primera unidad! En la próxima unidad trabajaremos sobre el concepto de Ingeniería Social, sus principales técnicas y algunos consejos de seguridad para prevenirse de ese tipo de ataques.

Plataforma de
Aprendizaje Virtual

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología