SEGURIDAD INFORMÁTICA.

La Seguridad Informática se refiere a las características y condiciones de los sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Considerar aspectos de seguridad significa a) **conocer el peligro**, b) **clasificarlo** y c) **protegerse** de los impactos o daños de la mejor manera posible. Esto significa que solamente cuando estamos consientes de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de nosotros, podemos tomar medidas de protección adecuadas, para que no se pierda o dañe nuestros recursos valiosos.

En este sentido, la Seguridad Informática sirve para la **protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.**

SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

En la Seguridad Informática se debe distinguir dos propósitos de protección:

- **la Seguridad de la Información**
- **la Protección de Datos.**

SEGURIDAD DE LA INFORMACIÓN: Se entiende por seguridad de la información **el** conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.

El objetivo de la protección son los datos mismos y trata de evitar su pérdida y modificación no-autorizada. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el **propio interés de la institución** o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial).

PROTECCIÓN DE DATOS,: En cambio en la protección de datos se entiende, aquellos datos personales que protegen la información de las personas y que se ubica dentro del campo de estudio del Derecho Informático, del derecho de la información, de los derechos humanos y del derecho constitucional.

Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no solo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.

En líneas generales, seguridad de datos se refiere a medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos**,** los cuales pueden encontrarse en ordenadores, bases de datos, sitios web, etc. La seguridad de datos también protege los datos de una posible corrupción.

Seguridad de datos incluye conceptos como encriptación de datos, tokenización y prácticas de gestión de claves que ayudan a proteger los datos en todas las aplicaciones y plataformas de una organización**.**

El objetivo de la protección no son los datos en si mismo, sino el contenido de la información sobre personas**,** para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

Sin embargo hay que destacar que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo o obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, sin embargo el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuadamente o arbitrariamente.

Existen algunas profesiones que, por su carácter profesional, están reconocidos o obligados, por su juramento, de respetar los datos personales como por ejemplo los médicos, abogados, jueces y también los sacerdotes. Pero independientemente, si o no existen normas jurídicas, la responsabilidad de un tratamiento adecuado de datos personales y las consecuencias que puede causar en el caso de no cumplirlo, recae sobre cada persona que maneja o tiene contacto con tal información, y debería tener sus raíces en códigos de conducta y finalmente la ética profesional y humana, de respetar y no perjudicar los derechos humanos y no hacer daño.

En algunos países la protección de datos encuentra reconocimiento constitucional, como derecho humano y en otro simplemente legal. Se protege también a través del derecho a la privacidad y del derecho a la inviolabilidad de las comunicaciones.

El objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

Sin embargo hay que destacar que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo o obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, sin embargo el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuadamente o arbitrariamente.

Existen algunas profesiones que, por su carácter profesional, están reconocidos o obligados, por su juramento, de respetar los datos personales como por ejemplo los médicos, abogados, jueces y también los sacerdotes. Pero independientemente, si o no existen normas jurídicas, la responsabilidad de un tratamiento adecuado de datos personales y las consecuencias que puede causar en el caso de no cumplirlo, recae sobre cada persona que maneja o tiene contacto con tal información, y debería tener sus raíces en códigos de conducta y finalmente la ética profesional y humana, de respetar y no perjudicar los derechos humanos y no hacer daño.
Si revisamos otra vez los resultados del ejercicio *con el banco y en particular los elementos que clasificamos como "Información Confidencial", nos podemos preguntar, ¿de qué Manera nos podría perjudicar un supuesto mal manejo de nuestros datos personales, por parte del banco, con la consecuencia de que terminen en manos ajenas? Pues, no hay una respuesta clara en este momento sin conocer cuál es la amenaza, es decir quién tuviera un interés en esta información y con qué propósito?*

Ejercicio: Seguridad de la Información y Protección de Datos

Este ejercicio sirve para mostrar la diferencia entre la Seguridad de la Información y la Protección de Datos y su importancia para la decisión y justificación, cuáles de los elementos de información requieren una mayor atención en su cuidado.

Suponiendo que todos contamos con una cuenta bancaria, se hace la pregunta a los participantes ***¿Cuáles son los datos, informaciones que maneja el banco sobre mí?*** *y se presenta las respuestas en tarjetas*
A continuación el grupo se pone de acuerdo, ***¿Cuáles de los elementos se considera como Información confidencial?****, las cuales el banco debería tratar de tal manera, que no terminen en manos ajenas.*

Números de cuentas bancarias	Patrimonio	Firma	Hábitos de consumo (restaurantes, tiendas)
Número de identificación	Dirección domicilio	Profesión, Cargo laboral	Contraseñas de cuenta
Transacciones bancarias	Consumo servicio de teléfono, electricidad, etc	Nombre y Apellido	Salario
Números telefónicos	Deudas y créditos	Lugar de estudio de hijos	Capacidad de consumo

(Consejo metodológico: es importante que se aplique una visión crítica, porque a primera vista todos los elementos nos parecen "privados", sin embargo, reflexionando un poco sobre nuestro propio estilo de difusión de la información, nos damos cuenta que muchos de los elementos mencionados, se maneja en un ámbito bastante público).

¿Cuáles de los elementos se considera como Información público?

Números de cuentas bancarias	Patrimonio	Firma	Hábitos de consumo (restaurantes, tiendas)
Número de identificación	Dirección domicilio	Profesión, Cargo laboral	Contraseñas de cuenta
Transacciones bancarias	Consumo servicio de teléfono, electricidad, etc	Nombre y Apellido	Salario
Números telefónicos	Deudas y créditos	Lugar de estudio de hijos	Capacidad de consumo

Como último paso se discute en el grupo ***¿Cuáles de los elementos son de interés propio del banco, para que sea capaz de manejar mi cuenta?***

Números de cuentas bancarias	Patrimonio	Firma	Hábitos de consumo (restaurantes, tiendas)
Número de identificación	Dirección domicilio	Profesión, Cargo laboral	Contraseñas de cuenta
Transacciones bancarias	Consumo servicio de teléfono, electricidad, etc	Nombre y Apellido	Salario
Números telefónicos	Deudas y créditos	Lugar de estudio de hijos	Capacidad de consumo

Conclusiones:

- *Existe una divergencia en la percepción de la gente (en este caso el grupo participante), cuáles de los elementos deben ser calificados como confidencial y por tanto recibir un tratamiento más cuidadoso por parte de la institución que lo maneja (el banco).*
- *Los elementos que se puede considerar como confidenciales, del punto de vista de la persona que aparece en ellos, y por consecuencia merecen un manejo más cuidadoso por parte del banco, no coinciden con los elementos que son críticos para este, para garantizar el buen manejo de mis recursos económicos. Entonces hay una probabilidad que exista una diferencia en la opinión, entre el propietario de la cuenta y el banco, sobre la importancia y atención en el manejo de los diferentes elementos informativos.*
- *Dentro del marco de la Seguridad Informática, los elementos que definimos como confidenciales, requieren una atención especial, porque están ligados al concepto de la Protección de Datos y los que son de interés propio del banco.*
    - *https://www.argentina.gob.ar/aaip/datospersonales*
    - *https://www.powerdata.es/seguridad-de-datos*

ALGUNOS CONCEPTOS QUE DEBES CONOCER

La seguridad de datos es un tema de suma importancia que nos afecta a casi todos nosotros. Cada vez son más los productos tecnológicos que de una u otra forma deben ser tenidos en cuenta para temas de seguridad y que se están introduciendo en nuestra vida cotidiana, desde smartwatches hasta vehículos sin conductor. Todos estos dispositivos conectados crean nuevas "conversaciones" entre dispositivos, interfaces, infraestructuras privadas y la nube, lo que a su vez crea más oportunidades para que los hackers puedan escuchar.

RANSOMWARE

Tendencias recientes han demostrado que los ataques de **ransomware** están aumentando en frecuencia y en gravedad. Se ha convertido en un negocio en auge para ladrones cibernéticos y hackers, que acceden a la red y secuestran datos y sistemas. En los últimos meses, grandes empresas y otras organizaciones, así como también usuarios particulares, han caído víctimas de este tipo de ataques y han tenido que pagar el rescate o correr el riesgo de perder datos importantes.

Entonces, ¿qué conceptos deberíamos conocer que puedan ayudarnos a proteger nuestra red y prevenir esta nueva ola de ataques cibernéticos modernos?

Los ingenieros de seguridad se ocupan de proteger la red de las amenazas, ellos diseñan sistemas que protegen las cosas y los implementa, realizan pruebas hasta hacerlos cada vez más seguros, realizan revisiones regulares de código como así también crean arquitecturas de seguridad para mantener bloqueada y segura la red.

ENCRIPTACIÓN

Si la ingeniería de seguridad de datos protege la red y otros activos físicos como servidores, computadoras y bases de datos, **la encriptación protege los datos y archivos reales almacenados en ellos o que viajan entre ellos a través de Internet.** Las estrategias de encriptación son cruciales para cualquier empresa que utilice la nube y son una excelente manera de proteger los discos duros, los datos y los archivos que se encuentran en tránsito a través de correo electrónico, en navegadores o en camino hacia la nube.

En el caso de que los datos sean interceptados, **la encriptación dificulta que los hackers hagan algo con ellos**. Esto se debe a **que los datos encriptados son ilegibles para usuarios no autorizados sin la clave de encriptación**. Detección de intrusión y respuesta ante una brecha de seguridad

Si en la red ocurren acciones de aspecto sospechoso, como alguien o algo que intenta entrar, la detección de intrusos se activará. Los sistemas de detección de intrusos de red (NIDS) supervisan de forma continua y pasiva el tráfico de la red en busca de un comportamiento que parezca ilícito o anómalo y lo marcan para su revisión. Los NIDS no sólo bloquean ese tráfico, sino que también recopilan información sobre él y alertan a los administradores de red.

TOKENIZACIÓN

Con la multiplicación de los métodos de pago disponibles, es vital añadir una capa de seguridad adicional para proteger datos sensibles de las tarjetas de crédito.

La tokenización es el proceso que permite proteger datos sensibles, sustituyéndolos por equivalentes no-sensibles, conocidos como tokens. Se utiliza para evitar el robo de datos en las transacciones con tarjetas bancarias.

Cuando se activa la tokenización, un algoritmo genera un valor aleatorio y único que sustituye el número de cuenta del comprador (o número PAN). Este valor aleatorio es el token. Estos tokens pasan de forma segura por la red para proceder al pago sin exponer los datos de la tarjeta bancaria. El número de tarjeta se encuentra protegido en una bóveda segura.

Las tarjetas con chip fueron creadas para proteger la información bancaria en los puntos de venta. La tokenización provee el mismo nivel de seguridad en las compras. Ambos sistemas evitan que los datos puedan ser robados.

¿Cuál es la diferencia entre tokenización y encriptación?

Tanto la tokenización como la encriptación de datos sirven para proteger los datos online, pero son dos tecnologías diferentes y no son intercambiables. Siempre se usan ambos sistemas en las transacciones en tiendas de e-commerce, para asegurar el proceso de pago de principio a fin. Los datos se mapean en una base de datos (por ejemplo para comparar bases de datos) a través de tokens, pero a la vez los datos se encriptan a la hora de almacenarlos. Esto es uno de los requerimientos del protocolo PCI DSS.

Tokenización	Encriptación
Genera un token aleatorio y almacena el mapeo en una base de datos	Utiliza un algoritmo de encriptación y una clave para transformar texto llano en texto encriptado
Se puede utilizar para datos estructurados como los de las tarjetas bancarias	Se puede utilizar para datos no estructurados como ficheros enteros, o para datos estructurados
Requiere un acceso directo a una bóveda para mapear el valor de los tokens	Mejor para intercambiar datos con terceros que tengan la clave de encriptación
Preserva el formato sin rebajar el nivel de seguridad	Una encriptación con menor nivel de seguridad permite preservar el formato
Los datos originales no salen de la organización	Los datos originales salen de la organización, de forma encriptada

FIREWALL

¿Cómo mantener a visitantes no deseados y software malicioso fuera de la red? Cuando estás conectado a Internet, una buena manera de asegurarse de que sólo las personas y archivos adecuados están recibiendo nuestros datos es mediante firewalls: **software o hardware diseñado con un conjunto de reglas para bloquear el acceso a la red de usuarios no autorizados**. Son excelentes líneas de defensa para evitar la interceptación de datos y bloquear el malware que intenta entrar en la red, y también evitan que la información importante salga, como contraseñas o datos confidenciales.

CLAVES PARA PROTEGER TUS DATOS PERSONALES

Actualmente, 6 de cada 10 usuarios vuelcan información personal en la nube, aplicaciones y redes sociales, exponiéndose diariamente al robo de sus datos. ¿Instalar un antivirus? ¿Configurar la privacidad en las redes sociales? ¿Crear una contraseña compleja? ¿Qué conviene hacer para evitar el acceso ilegal a nuestros mensajes y contenidos?

A pesar de seguir los requerimientos básicos de seguridad, la mayor parte de los usuarios expone sus datos, bien por desconocimiento o por exceso de confianza, y ponen en constante peligro su seguridad informática.

Actualizarse es clave

Las apps de nuestros dispositivos pueden actualizarse de forma manual o permitir que se actualicen automáticamente. Si mantenemos las apps actualizadas, se podrá acceder a las funciones más recientes con mejoras de estabilidad y seguridad. Esto permite solucionar las fallas y errores de versiones anteriores, como los que registran la protección de datos, por ejemplo.

Recientemente WhatsApp activó la encriptación de extremo a extremo de las comunicaciones de sus usuarios para que sólo quien envía y quien recibe pueda ver el contenido. Si la aplicación no es actualizada, no se podrá contar con ese beneficio.

La privacidad se cuida en casa

Los bares y locutorios ofrecen acceso rápido y barato a redes WIFI o a una PC con internet, pero no sabemos quién puede acceder a ese dispositivo, ni cuáles son las medidas de seguridad que posee. Por lo tanto, nunca se deben ingresar datos privados ni acceder a servicios autenticados, como email, redes sociales y homebanking desde ese tipo de dispositivos.

En el caso de las redes domésticas, se recomienda cambiar la contraseña del WiFi periódicamente, como mínimo, cada dos meses.

No es con todos

Aunque parezca engorroso, es importante leer los términos y condiciones antes de instalar una aplicación o servicio, para saber si estamos dándole permiso para almacenar nuestros datos en la nube. Si esto ocurre, el servidor se convierte en el "dueño de los datos y el usuario pierde el control de su información. Además, es primordial configurar la privacidad de las publicaciones en redes sociales. Actualmente, todas las redes permiten realizar ajustes personalizados para resguardar los contenidos e incluso, algunas como Facebook, dan la opción de establecer permisos específicos para cada actualización de estado.

No todo lo que brilla es oro

¿De dónde proviene el archivo que me enviaron? ¿Es seguro? Una de las principales formas de engaño y robo de datos es enviar a los usuarios archivos, formularios, y solicitudes de contacto a través de perfiles y cuentas falsas. En este sentido, el especialista de Educación IT aconseja que "lo mejor es no abrir archivos de dudosa procedencia ni aceptar en redes sociales a personas desconocidas. Es ideal no responder a mensajes que soliciten información confidencial, aunque digan ser de entidades de confianza, como el banco, por ejemplo.

Utilizar aplicaciones seguras

Para asegurarse de que una aplicación está libre de virus y malware (software malicioso), lo mejor es chequear si tiene buena reputación, si fue desarrollada por empresas de confianza, y si además, es utilizado por muchos otros usuarios. Existen sitios web de descarga gratuita de programas que engañan a los usuarios y al descargar la aplicación se ejecutan de forma oculta contenidos maliciosos que destruyen o que se apropian de los datos almacenados

¿Cómo crear una buena contraseña?

"Las contraseñas más robustas y complejas son aquellas que combinan mayúsculas, minúsculas, símbolos y números, sostuvo Portantier y agregó: "No se recomienda utilizar la misma contraseña en todos los servicios ni incluir fechas de nacimiento, aniversarios, números de teléfono o fragmentos del DNI . En el caso de sospechar que una contraseña haya sido comprometida, lo ideal es cambiarla al instante.

¡Bendito seas back up!

Un virus, un error humano, una falla en el dispositivo podrían borrar nuestros datos. Por eso es importante que siempre se realicen copias de seguridad de la información en medios de almacenamiento extraíbles, como DVD regrabables, discos externos o Pendrives USB. A la vez, podemos contar con programas que realicen backups automáticos sin que sea necesaria ninguna intervención por parte del usuario para su ejecución.

https://www.argentina.gob.ar/aaip/datospersonales