LA IMPORTANCIA DE LA CIBERSEGURIDAD Y LA PROTECCIÓN DE DATOS PERSONALES

En la era digital en la que estamos inmersos, la interconexión y el contacto con la tecnología se han convertido en dos factores omnipresentes, razón por la cual, la **ciberseguridad** ha emergido como una preocupación crítica para individuos, empresas y gobiernos por igual.

Nadie puede negar que el vertiginoso avance tecnológico ha traído consigo innumerables beneficios, pero también ha dado lugar a un aumento exponencial de las amenazas cibernéticas. La conectividad global, el almacenamiento masivo de datos y la proliferación de dispositivos conectados han creado un terreno propicio para los ciberdelincuentes, quienes, con ingenio y sofisticación, han encontrado nuevas formas de comprometer la seguridad de la información.

En este contexto, la protección de datos personales y la implementación efectiva de medidas de ciberseguridad no solo se han vuelto imperativas, sino que son esenciales para salvaguardar la integridad de los usuarios y garantizar la confianza en el espacio digital.

La **seguridad informática** o **ciberseguridad** es la suma de procesos, recursos y herramientas que se emplean con el fin de proteger y defender dispositivos, sistemas electrónicos, servidores, redes y programas de posibles ataques digitales. En otras palabras, se centra en asegurar que los recursos digitales y la información electrónica estén protegidos contra posibles riesgos cibernéticos.

Habitualmente, los ciberataques buscan acceder, modificar o eliminar información confidencial o de elevada importancia para paralizar las actividades cotidianas o exigir “rescates” por la información sustraída o manipulada. Aplicar medidas eficaces que contrarresten estos intentos por vulnerar datos privados se vuelve una tarea cada vez más compleja debido a la multitud de dispositivos y a la constante sofisticación que emplean los atacantes.

LA IMPORTANCIA DE LA CIBERSEGURIDAD Y LA PROTECCIÓN DE DATOS PERSONALES

Frente a este panorama, los profesionales de la ciberseguridad trabajan para desarrollar y aplicar medidas preventivas, detectivas y correctivas para mitigar los riesgos y responder eficazmente a incidentes de seguridad cibernética. Esto implica la implementación de protocolos de seguridad, el uso de tecnologías avanzadas, como firewalls y sistemas de detección de intrusiones, y la promoción de buenas prácticas de seguridad entre los usuarios.

Según un estudio de Check Point Research, la división de Inteligencia de Amenazas de la compañía de ciberseguridad Check Point, **los ciberataques globales se incrementaron** en un 8% en el segundo trimestre del 2023. Este reporte resalta la astucia de los atacantes al combinar las tecnologías de Inteligencia Artificial (IA) de última generación con herramientas establecidas desde hace tiempo, como los dispositivos USB, para llevar a cabo ciberataques a gran escala.

Hoy en día es común recibir correos, mensajes o llamadas con el fin de obtener información personal, financiera, académica o laboral. Muchas veces, la persistencia de los atacantes llega a tal punto que, cuando la víctima se da cuenta de lo sucedido, es demasiado tarde.

Actualmente, la legislación en Colombia, contempla la Ley de Protección de Datos Personales o Ley 1581 de 2012 y reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

Los datos personales se deben proporcionar en cualquier tipo de trámite en los que es determinante transparentar la información de cada persona, ya sea para adquirir productos o contratar servicios. Sin embargo, en estas situaciones, las personas deben recibir obligatoriamente el Aviso de Privacidad, que es un documento mediante el cual se da a conocer a los titulares de los datos la información que se recaba y para qué fines será utilizada, además de la responsabilidad de protegerla.

LA IMPORTANCIA DE LA CIBERSEGURIDAD Y LA PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales es de suma importancia por varias razones fundamentales, en esta ocasión se presentarán tres:

- La privacidad es un derecho fundamental que debe ser protegido y todos tenemos la facultad de decidir qué información compartimos y con quién la compartimos. Cuando se recopilan datos personales sin nuestro consentimiento, se viola nuestra privacidad y se pone en riesgo nuestra seguridad.
- Los datos personales son valiosos y pueden ser utilizados con fines malintencionados. La información personal también puede ser utilizada para acosar, amenazar a las personas o incluso cometer fraudes.
- La protección de datos personales es esencial para proteger la seguridad nacional y la estabilidad económica. Esta información puede ser utilizada para concretar actividades ilícitas o para recopilar datos sensibles sobre empresas o gobiernos. Si los datos personales son sustraídos ilegalmente puede generar graves consecuencias como la interrupción de los sistemas de seguridad a nivel nacional o la pérdida de confianza de clientes e inversores.

¿Cómo puede la ciberseguridad custodiar los datos personales a nivel empresarial?

La ciberseguridad se ha convertido en una herramienta que protege los datos de accesos no autorizados, usos indebidos, modificaciones, eliminaciones o robo. En las empresas implica tiempo para capacitar al personal y dinero para invertir en los programas de software correctos y que garanticen la protección, pero se puede actuar a través de tres frentes:

1. **Implementar medidas de seguridad técnicas y organizativas.**
    - Controlar y restringir el acceso a los datos solo a las personas que lo requieren.
    - Asegurar que las redes informáticas sean seguras y se encuentren protegidas contra ataques.
    - Detectar y eliminar software malicioso que pueda poner en riesgo los datos.
    - Realizar copias de seguridad de los datos para que puedan ser restaurados en caso de un incidente de seguridad.

LA IMPORTANCIA DE LA CIBERSEGURIDAD Y LA PROTECCIÓN DE DATOS PERSONALES

2. **Capacitar a los empleados en materia de ciberseguridad.**
    - Concientizarlos sobre la importancia de la protección de datos.
    - Enseñarles a identificar y evitar los riesgos de ciberseguridad.
    - Brindarles las herramientas y conocimientos necesarios para proteger los datos en su trabajo diario.

3. **Establecer un plan de respuesta a incidentes.**
    - Definir los pasos a seguir en caso de un incidente de seguridad.
    - Identificar a las personas responsables de responder al problema.
    - Probar y actualizar el plan de respuesta a incidentes regularmente.

En definitiva, la protección de datos personales es un tema crucial en la era digital. Las leyes y regulaciones garantizan que esta información tan sensible se maneje de manera ética y segura. No obstante, los atacantes siempre se encuentran al acecho y es deber de los ciudadanos informarse sobre cómo hacer respetar sus derechos en relación con sus datos personales y qué medidas deben tomar para proteger su información personal en línea y fuera de ella.

Referencia:

Redacción Tus Datos. (2025) Ciberseguridad y protección de datos: claves para las empresas. Tusdatos.co. Recuperado de: https://www.tusdatos.co/blog/la-importancia-de-la-ciberseguridad-y-la-proteccion-de-datos-personales