Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín Informativo

Dieciocho

Agosto: Privacidad Digital y la Protección de Datos

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Dieciocho
Agosto de 2023

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director
CSIRT Académico UNAD

Responsable de la Edición
Ing. Yenny Stella Núñez Álvarez

Revisó
Ing. Diego Fernando Medina Soto
Director CCAV Facatativá

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Boletín informativo Número 18

Agosto 2023

Privacidad Digital y la Protección de Datos

Autores:

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Yenny Stella Núñez Álvarez
CSIRT Académico UNAD
https://orcid.org/0000-0003-0128-1214

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

La digitalización de nuestro entorno es una tendencia creciente que afecta diversos aspectos de nuestra vida, como el trabajo, el estudio, el hogar y el entretenimiento, entre otros. Estos ámbitos cada vez dependen más de dispositivos móviles, equipos informáticos, sitios web, software en la nube, big data, aplicaciones, inteligencia artificial y electrodomésticos conectados a través de IoT, junto con otras tecnologías emergentes. Sin embargo, todas estas innovaciones comparten un denominador común: para aprovechar sus ventajas, es necesario compartir información privada que resulta esencial para el registro, el funcionamiento y la sincronización de servicios, entre otros aspectos. Debido a esto, surge la necesidad de regular y asegurar el tratamiento adecuado de los datos y la privacidad digital de la información.

Fuente: https://www.freepik.es/foto-gratis/manos-trabajando-superposicion-grafica-red-dispositivos-

Desarrollo

Riesgos de seguridad y privacidad de los datos

Fuente: https://www.freepik.es/foto-gratis/tecnologia-sistema-red-seguridad-desarrollo-grafico

En la vida cotidiana, compartimos información personal en muchos procesos y plataformas, como solicitar una cita médica, crear cuentas, instalar aplicaciones, responder encuestas inscribirse en eventos o adquirir servicios o productos entre otros. También lo hacemos en las redes sociales, donde compartimos información sobre nuestro círculo social, pasatiempos, orientaciones políticas y otros detalles personales.

A menudo, no nos detenemos a pensar dónde se almacenan estos datos ni a los peligros a que pueden estar expuestos a causa de un ciberataque si no se les da un tratamiento adecuado. Estos riesgos pueden incluir:

- **Violaciones de datos:** ocurren cuando un adversario accede de manera no autorizada a sistemas o bases de datos que contienen información personal. Esto puede incluir datos como nombres, direcciones, números de tarjeta de crédito o datos que pueden ser públicos, privados o reservados.
- **Phishing:** es una técnica en la que los atacantes envían mensajes de correo electrónico falsos que parecen ser de fuentes legítimas para engañar a las personas y obtener información confidencial, como contraseñas o números de cuenta bancaria[1].
- **Ransomware:** es un tipo de malware que cifra los datos de una víctima y luego exige un rescate a cambio de la clave descifrada. Esto puede resultar en la pérdida de datos personales si la víctima decide no pagar el rescate[2].
- **Ataques a la nube:** A medida que más datos se almacenan en la nube, los ciberdelincuentes han dirigido sus esfuerzos hacia la nube. Los ataques a servicios de almacenamiento en la nube pueden exponer datos personales si no se toman medidas de seguridad adecuadas.
- **Vulnerabilidades[3] en aplicaciones y software:** Las aplicaciones y el software con vulnerabilidades de seguridad pueden ser explotados por los atacantes para acceder a datos personales. Es importante mantener el software actualizado y aplicar parches de seguridad.

[1] https://latam.kaspersky.com/resource-center/threats/data-theft
[2] https://www.powerdata.es/seguridad-de-datos

[3] https://www.bancosantander.es/glosario/vulnerabilidad-informatica

- **Fugas de datos internas:** No todos los riesgos cibernéticos provienen de fuentes externas. Las fugas de datos internos pueden ocurrir cuando los empleados acceden, comparten o roban información confidencial[4].
- **IoT y dispositivos conectados:** Los dispositivos de Internet de las cosas (IoT) a menudo recopilan y transmiten datos personales. La falta de seguridad en estos dispositivos puede dar lugar a la exposición de datos privados.
- **Ingeniería social:** Los atacantes pueden aprovechar la ingeniería social para obtener acceso a datos personales. Esto implica manipular a las personas para que divulguen información confidencial.
- **Regulaciones y cumplimiento:** Los riesgos cibernéticos también incluyen el incumplimiento de regulaciones de privacidad, como el Reglamento General de Protección de Datos (GDPR) en Europa o leyes de privacidad en otros países. Las organizaciones pueden enfrentar multas y sanciones si no protegen adecuadamente los datos personales. Le inviramos a conocer las sanciones aplicadas por las SIC para el año 2022[5]
- **Errores humanos:** Los errores humanos también pueden dar lugar a violaciones de datos. Como perdidas de tarjetas de crédito con información personal o la publicación accidental de información confidencial en un sitio web público.
- **Prácticas de recopilación de datos inapropiadas:** Algunas empresas recopilan datos personales de forma inapropiada. Como la recopilación de datos personales sin el consentimiento de los usuarios o puede recopilar datos personales que no son necesarios para la prestación de sus servicios.
- **Cumplimiento inadecuado de la ley:** Las empresas que no cumplen con las leyes de protección de datos pueden poner en riesgo la privacidad de los datos de sus clientes, omitiendo la implementación de medidas de seguridad adecuadas para proteger los datos personales de sus bases de datos o registros.

Protección, seguridad y privacidad de los datos

Debido a que la información y los datos tienen una importancia fundamental en todos los niveles y sectores, hace que su masificación digital este regulada con medidas y normas que garanticen su integridad[6], confidencialidad[7] y disponibilidad[8], a partir de esta premisa surgen tres conceptos:

- **La privacidad de datos** se enfoca en prevenir el uso no autorizado y la divulgación de datos personales y confidenciales. Como resultado, las empresas pueden proteger los derechos de privacidad de las personas y mantener la confidencialidad de la información al garantizar que los datos estén protegidos.
- **La protección de datos** es el proceso que previene el acceso, uso y divulgación no autorizada de los datos. Consiste en implementar políticas[9], procedimientos y tecnologías para garantizar la confidencialidad, integridad y disponibilidad de los datos.

[4] https://csirt.unad.edu.co/difusion-y-divulgacion/documentos-y-guias
[5] https://www.sic.gov.co/sanciones-proteccion-datos-personales-2022
[6] *"La integridad de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores. La información ha podido ser alterada intencionadamente o ser incorrecta y nosotros podemos basar nuestras decisiones en ella". (INCIBE)*
[7] *"La confidencialidad implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso" (INCIBE)*
[8] *"La disponibilidad de la información hace referencia a que la información esté accesible cuando la necesitemos. Algunos ejemplos de falta de disponibilidad de la información son: cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de denegación de servicio, en el que el sistema «cae» impidiendo accesos legítimos" (INCIBE)*
[9] https://selloeditorial.unad.edu.co/images/2022/boletines-cip-csirt/boletin_8.pdf

- **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, entre otros activos de información[10]. La seguridad de datos también protege los datos de una posible corrupción.

Basado en estos conceptos se puede señalar que la privacidad digital y la protección de datos son piezas clave en un mundo digital caracterizado por miles las transacciones en línea y de procesamientos innumerables de datos de todo tipo, porque proporcionan las directrices, marcos de trabajo, estándares y normativas para el tratamiento adecuado de los datos a partir de políticas, procedimientos, tecnologías y buenas prácticas para el acceso, uso y divulgación de estos[11].

Medidas de protección y prevención de la privacidad de los datos

Se requiere para minimizar los riesgos que las organizaciones implementen medidas de seguridad efectivas, capaciten periódicamente al talento humano sobre la seguridad y la privacidad de los datos, conozcan las regulaciones de privacidad vigentes sobre recopilación y autorización de datos, tomar precauciones, como utilizar contraseñas seguras y ser conscientes de las amenazas de phishing, para proteger su privacidad en línea.

Es importante tener presente que la seguridad y la privacidad de los datos son responsabilidad de todos. Las personas, las empresas y las organizaciones deben trabajar juntas para proteger los datos personales[12].

Otras medidas orientadas a proteger los sistemas de información en donde se realizan las transacciones y procesamiento de datos son las siguientes:

- **Encriptación:** Es un proceso que convierte los datos en un formato ilegible para usuarios no autorizados. Esto ayuda a proteger los datos almacenados en dispositivos, en tránsito por Internet o almacenados en la nube.
- **Detección de intrusión y respuesta ante una brecha de seguridad:** Los sistemas de detección de intrusos de red lo hacen de forma pasiva, es decir, sin interferir con el tráfico. Cuando detectan actividad sospechosa, la marcan para su revisión y alertan a los administradores de red.
- **Firewall:** Los cortafuegos bloquean el acceso a la red de usuarios no autorizados. Son una línea de defensa importante contra las violaciones de seguridad.
- **Análisis de vulnerabilidades:** Se trata de aplicar una variedad de técnicas para escanear el sistema en busca de vulnerabilidades, como análisis de código, pruebas de penetración y análisis de vulnerabilidades conocidas[13].
- **Pruebas de intrusión:** Los adversarios pueden utilizar un conjunto de técnicas para penetrar en un sistema, como la explotación de vulnerabilidades conocidas, el phishing o el malware. Las pruebas de penetración utilizan estas mismas técnicas para identificar las vulnerabilidades que podrían ser explotadas por un atacante real[14].

[10] https://selloeditorial.unad.edu.co/images/2022/boletines-cip-csirt/Boletin_13.pdf
[11] https://www.powerdata.es/seguridad-de-datos
[12] https://www.powerdata.es/servicios-de-consultoria

[13] https://www.deltaprotect.com/blog/que-es-pentesting
[14] https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/

- **Información de seguridad y gestión de eventos - SIEM:** El SIEM analiza los datos en tiempo real para identificar amenazas potenciales. Este tipo de sistemas pueden ayudar a las organizaciones a detectar ciberataques antes de que causen daños.
- **Protocolo HTTPS:** Las conexiones HTTPS cifran los datos enviados y recibidos entre un navegador y un servidor web. Esto ayuda a proteger los datos de la interceptación y el robo.
- **El software anti malware y anti spyware:** El software orientado a la ciberseguridad también es importante para proteger los datos y los sistemas ante un ataque cibernético, está diseñado para supervisar el tráfico de Internet entrante y saliente de los dispositivos de los usuarios finales, también contribuye a detectar y bloquear malware, como spyware, adware y virus troyanos.
- **Prevención de pérdida de datos (DLP):** Puede implementarse mediante software o hardware para supervisar el tráfico de red y detectar la transferencia de datos confidenciales. Asimismo, ayuda a las empresas a cumplir con las normativas de seguridad y proteger la privacidad de los datos de los clientes.

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:


Correo: csirt@unad.edu.co


Twitter: @csirtunad


Página web: https://csirt.unad.edu.co

Referentes Bibliográficos

[1] https://latam.kaspersky.com/resource-center/threats/data-theft

[2] https://www.powerdata.es/seguridad-de-datos

[3] https://csirt.unad.edu.co/difusion-y-divulgacion/documentos-y-guias

[4] https://www.powerdata.es/seguridad-de-datos

[5] https://www.powerdata.es/servicios-de-consultoria

[6] https://www.deltaprotect.com/blog/que-es-pentesting

[7] https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/