Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo

Número **Trece**

Marzo: ¿Cómo aportar a la mejora de la Ciberseguridad UNADISTA?

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

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 Trece
Marzo 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. Luis Fernando Zambrano Hernández

Revisó
Ing. Hernando José Peña Hidalgo
Docente Esp. Seguridad Informática UNAD

Estado legal:
Periodicidad: Quincenal
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 13

Marzo 27 de 2023

¿Cómo aportar a la mejora de la Ciberseguridad UNADISTA?

Autores:

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

John Fredy Quintero Tamayo
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

En la era digital que vivimos, la ciberseguridad es fundamental para reducir el riesgo en nuestro entorno digital. Proteger la información académica, administrativa y financiera, así como la propiedad intelectual generada en procesos de I+D+i y la imagen reputacional; los espacios de educación relacionados con la seguridad de la información es una prioridad. Teniendo presente lo anterior, es crucial el trabajo que viene desarrollando la UNAD estableciendo medidas de ciberseguridad adecuadas para protegerse contra ciberataques y es crucial el que toda la plataforma humana UNADISTA conozca la importancia de hablar de ciberseguridad.

El presente boletín tiene como propósito recordar algunos conceptos que permitan conocer cada vez más sobre la disciplina de la ciberseguridad y la importancia de su implementación y familiarización con técnicas de ataques y como poder reportarlas.

Nota.1: [Fotografía] Recuperado de https://www.freepik.es/

Desarrollo

Algunos conceptos claves:

¿Qué es un activo de información?

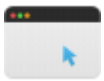
Es un dispositivo tecnológico digital o físico que adquiere o es entregado a una persona para desarrollar sus actividades cotidianas personales o laborales[1]. La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT[2] propuesta por el gobierno de España, cataloga a los activos de información así:

[D] Dato / Información

[K] Claves criptográficas

[Servicios]

[S] Software – Aplicaciones Informáticas



[HW] Equipamiento informático (hardware)

[COM] Redes de comunicaciones

[Media] Soportes de información

[AUX] Equipamiento auxiliar

[L] Instalaciones

[P] personas

¿Qué es una vulnerabilidad de ciberseguridad?:

Se considera como: un fallo o una debilidad que puede presentar un activo de información, lo cual puede permitir que un adversario o ciber atacante comprometa la integridad[3] confidencialidad[4] o disponibilidad[5] de la información.[6]

¿Qué es una amenaza de ciberseguridad?

El Instituto de Ciberseguridad de España – INCIBE[7], plantea el concepto de amenaza como: "*toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un activo de información.*" Es preciso indicar que, al ser materializada una amenaza, se presenta un impacto negativo en el activo de comprometido por la amenaza. En este sentido las amenazas pueden ser intencionadas o no intencionadas y pueden tener como origen:

[1] https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Transparencia_y_acceso_a_la_informacion_publica/SC05-I03%20ACTIVOS%20DE%20INFORMACION%20(1)%20(1).doc
[2] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
[3] Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[4] Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[5] Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[6] https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
[7] https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Desastres naturales

Ataques informáticos intencionados

Insuficiencia en procesos de educación

Errores o fallos no intencionados

De origen industrial

¿Qué es un riesgo de ciberseguridad?

Se considera como la probabilidad de que se genere un incidente en activo de información donde la amenaza se materializa y por consecuencia genera pérdidas o daños en la Disponibilidad, Integridad o Confidencialidad de la información. El riesgo depende los siguientes factores*: "Probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad, produciendo un daño o impacto"*[8].

¿Qué es un evento de ciberseguridad?

Es una acción que puede comprometer la seguridad de un activo de información. Estos deben ser analizados para descartar intentos de ataques o daños en los activos de información.
Eje. Infección de un equipo de cómputo a través de una USB infectada por malware

¿Qué es un incidente de ciberseguridad?

Acción provocada por un evento que afecta la disponibilidad, integridad o confidencialidad del activo de información comprometido de forma negativa
Eje. Daño o borrado de la información a causa del malware ejecutado a través de la USB
A continuación, se presentan algunos tipos de eventos o incidentes: [Imágenes recuperadas de https://www.freepik.es/]

Correo sospechoso

Alerta de virus o malware

Suplantación de identidad

Alteración de información

Indisponibilidad de servicio

Mensajes extorsivos

[8] https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

¿Cómo puedo identificar un evento o incidente de ciberseguridad?

Los eventos o incidentes de ciberseguridad pueden manifestarse de diferentes formas y pueden ser bastante complejos de identificar. Sin embargo, a continuación, se relacionan algunos comportamientos que pueden indicar la posible ejecución de una acción que provocarían un evento o un incidente de ciberseguridad:

Actividades sospechosas en la red de datos corporativa o del hogar: si se nota lentitud inusual en la navegación a través de la red de datos, puede ser que la red está siendo afectada por un tráfico sospechoso o usada por personas no autorizadas. Si presenta este tipo de comportamiento, comuníquese con su proveedor de servicio, o para el caso organizacional con la dependencia encargada para el caso de la UNAD es la Gerencia de Plataformas e Infraestructura Tecnológica - GPIT

En caso de una red corporativa, la técnica de ataque se puede usar un adversario o ciber delincuente es la de reconocimiento de la infraestructura tecnológica.

Comportamiento extraño: si varios usuarios reportan problemas al acceder a ciertas aplicaciones o experimentan lentitud, se podría estar presentando problemas de indisponibilidad de servicios debido a errores en la infraestructura tecnológica o a la ejecución de un ataque informático. En este caso puede ponerse en contacto con la GPIT o con el CSIRT Académico UNAD, reportándolo a través de los siguientes canales:

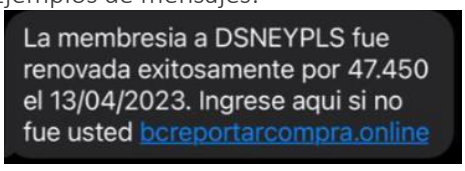
Correo: csirt@unad.edu.co

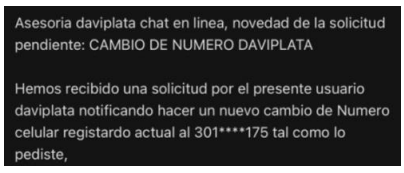
Página web: https://csirt.unad.edu.co/reporte-de-incidente

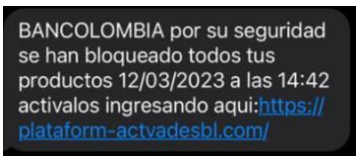
Este comportamiento se puede relacionar además con la técnica de ataque denominada: Colección, que tiene como propósito recolectar información de la víctima para posteriormente vender su información o hacer uso de esta en un acto delictivo.

Mensajes sospechosos: los correos electrónicos o mensajes provienen de remitentes desconocidos y que contienen enlaces o archivos adjuntos sospechosos pueden ser señales de un intento de phishing o smishing. En este caso, repórtelo a través de los enlaces anteriores. Como recomendación, antes de hacer clic procure confirmar con la persona o entidad si el mensaje es auténtico. **"Los ciberdelincuentes aprovechan que usted todavía cree en papá Noel"**

Ejemplos de mensajes:

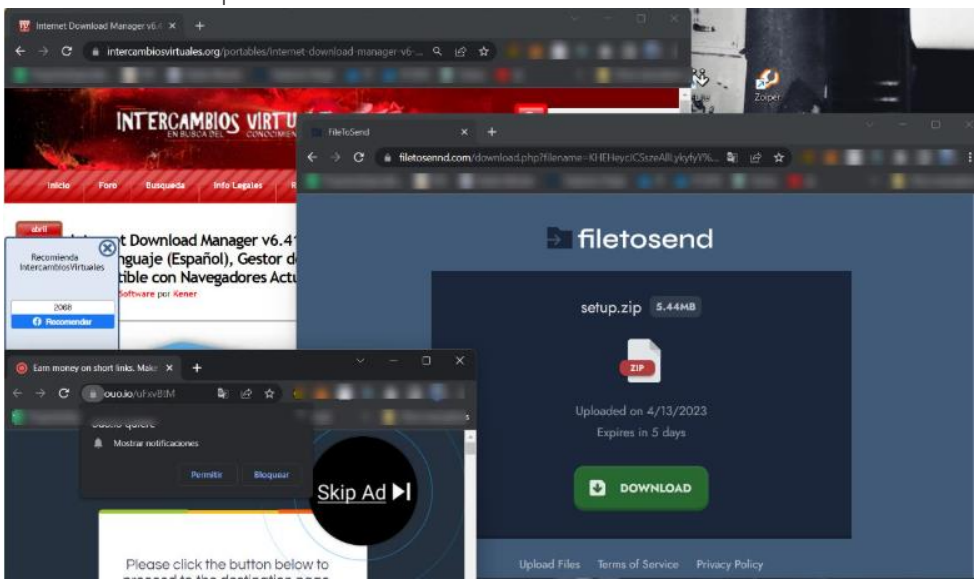






Cambios en la configuración del sistema: Respecto a administradores de servicios informáticos, dado el caso de notar cambios en la configuración del sistema o en los permisos de los usuarios que no deben ser autorizador para ciertas tareas, es señal de un ataque de suplantación, elevación de privilegios o Sql INJECTION. En este caso le invitamos a reportar este evento a través de los enlaces relacionados de forma anterior

Errores inesperados: si recibe errores inesperados del sistema o aplicación, podría ser un signo de un incidente de ciberseguridad generado por un malware, la instalación indebida o no autorizada de software, la navegación en sitios desconocidos, de baja reputación o por desconocimiento de las acciones que un usuario ejecuta en el activo de información, desconociendo el impacto que este puede tener. La siguiente ilustración relacionada con el sitio intercambios virtuales, presenta como al acceder a este sitio de forma automática da apertura a varios sitios que pueden contener archivos con malware incorporado.



Problemas de seguridad conocidos: si has recibido alertas o actualizaciones de seguridad de un proveedor de software o sistema, o hay noticias sobre vulnerabilidades recientes, es importante que estés alerta a posibles ataques.

Si sospecha que un evento o incidente de ciberseguridad está en desarrollo, establezca comunicación con el CSIRT Académico UNAD, esto con el fin de poder investigar y tomar las medidas necesarias para contener y proteger los activos de información.

¿Cómo puedo notificar o reportar un evento o incidente de ciberseguridad?

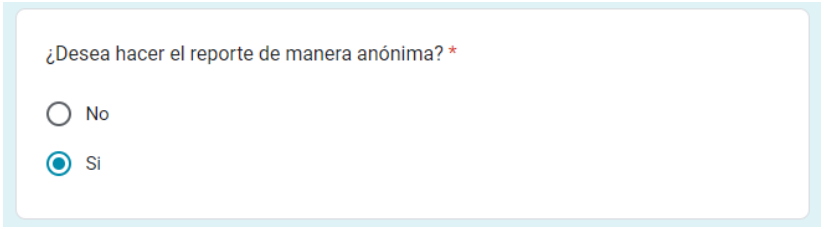
El CSIRT Académico UNAD en conjunto con la Gerencia de Plataformas e Infraestructura Tecnológica - GPIT ha dispuesto los siguientes canales de comunicación:

Correo: csirt@unad.edu.co | seguridad.informacion@unad.edu.co

Página web: https://csirt.unad.edu.co/reporte-de-incidente

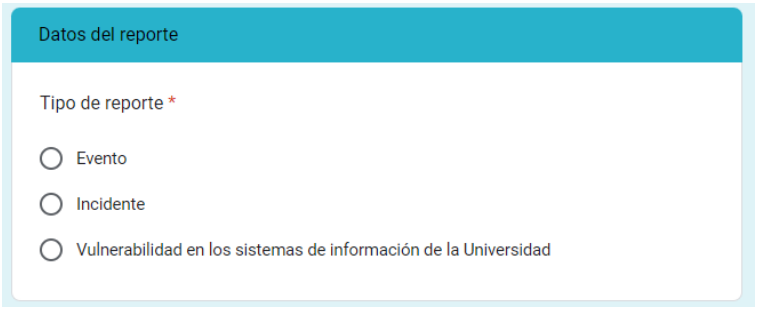
A través de la página del CSIRT https://csirt.unad.edu.co/reporte-de-incidente, encontrará un botón el cual lo dirigirá al formulario donde podrá realizar la notificación. Las siguientes ilustraciones presenta los pasos a dar para generar la notificación:

1. Indicar si se va a realizar el reporte de forma anónima o a nombre propio. En el caso de la segunda opción solo pedirá correo electrónico y nombres. Este insumo sirve para establecer comunicación con la persona que realiza la notificación y así ampliar la información reportada, si así lo estipula en el último paso del reporte.

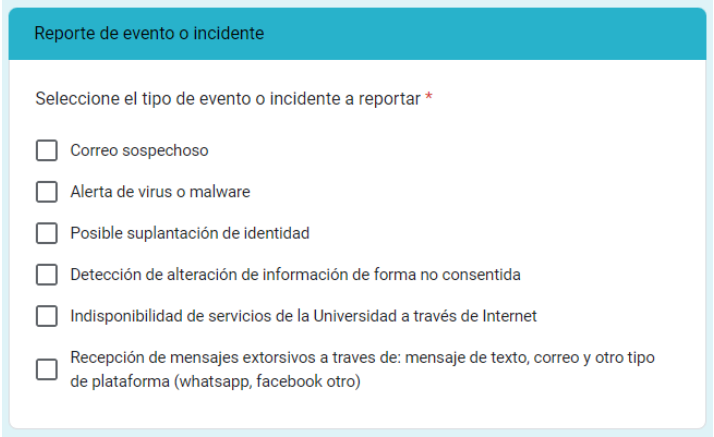


2. Seleccione el tipo de reporte si es un evento o un incidente (tenga presente lo socializado en este boletín).

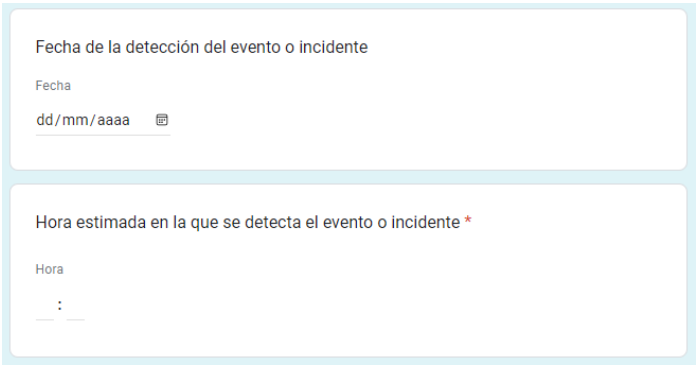
   Respecto a la tercera opción: "**Vulnerabilidad**", no se socializa en este documento ya que para realizar este reporte se requiere de conocimientos básicos de ciberseguridad. Dado el caso de conocer alguna vulnerabilidad en alguno de nuestros sistemas, le invitamos a generar el reporte o ponerse en contacto con el CSIRT; esta información es un insumo importante para seguir mejorando la ciberseguridad de nuestro entorno digital.



3. Seleccione el posible tipo de evento o incidente (puede ser uno o varios)



4. Indique la fecha y hora en la cual se dio cuenta o sospechó que estaba ocurriendo el evento

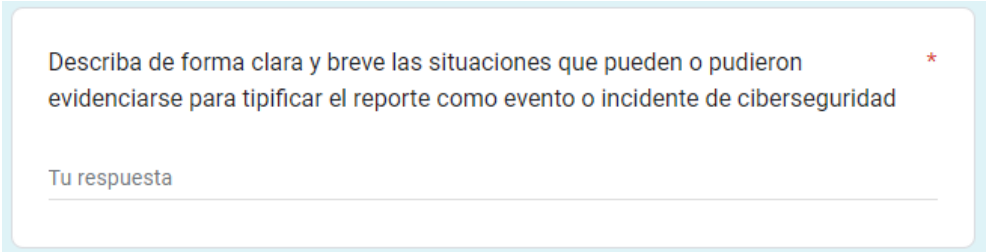


5. Para este punto, procure se los más claro posible relacionando aspectos que considere pudieron ocasionar el evento o incidente. Puede relacionar información como:

    - Software que pudo instalar y generar alguna acción de daño

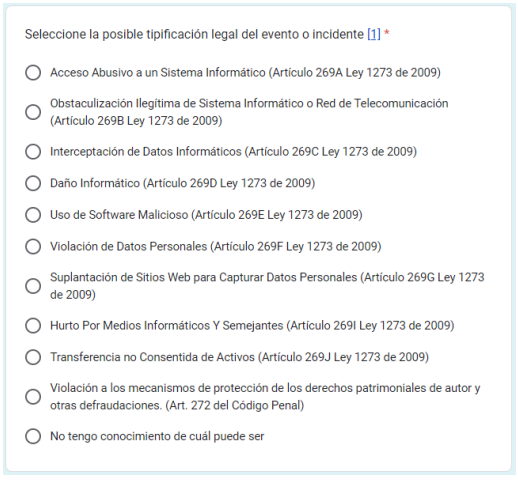
- Correos sospechosos que pudo recibir
- Mensajes extraños del sistema de información
- Desde cuando se está presentando el evento

Describa los comportamientos que lo lleve a pensar que está sucediendo algún evento. (recuerde lo socializado en este boletín)



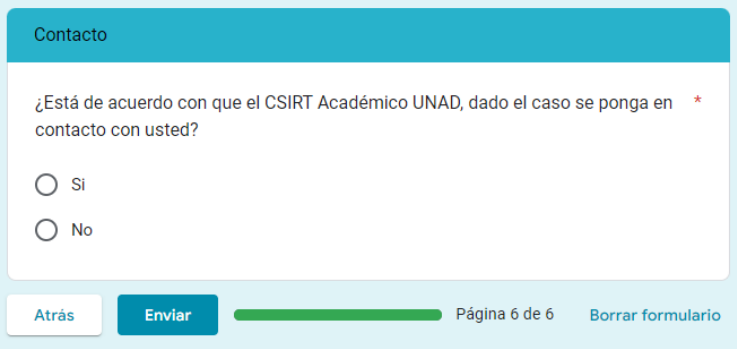
*Para ayudar a identificar lo sucedido, se recomienda adjuntar una imagen o video que permita al Equipo investigador del CSIRT construir el informe correspondiente y recomendar posibles controles para reducir la amenaza o el impacto del incidente. Puede enviar esta información también al correo csirt@unad.edu.co

Si está familiarizado con la ley 1273 de 2009[9], tipifique el evento o incidente informático. De lo contrario seleccione la última opción.



6. Si realizo el reporte a nombre propio, indique si está de acuerdo con que el CSIRT Académico UNAD se ponga en contacto para ampliar la información.

[9] https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf



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