Universidad Nacional Abierta y a Distancia
ACREDITADA EN ALTA CALIDAD

Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo - Técnico

Número **Diez**

Octubre: mes de la Ciberseguridad

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: CIP – CSIRT Académico UNAD

E-boletín Informativo CIP- CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

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

Número Diez
Octubre de 2022

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

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (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
CIP – CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director CIP CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

Revisó
Ing. Edgar Roberto Dulce
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 10 4
Introducción 4
Desarrollo 5
Recomendaciones para la protección de datos y dispositivos conectados a internet: 5
Recomendaciones para la protección de suplantación de identidad (Phishing) 6
Recomendaciones para el inicio de sesión en nuestros equipos de computo 6
Canales de comunicación 8
Recursos Bibliográficos Consultados 8

Boletín informativo Número 10

Octubre 31 de 2022

Octubre: Mes de la Ciberseguridad

Autores:

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

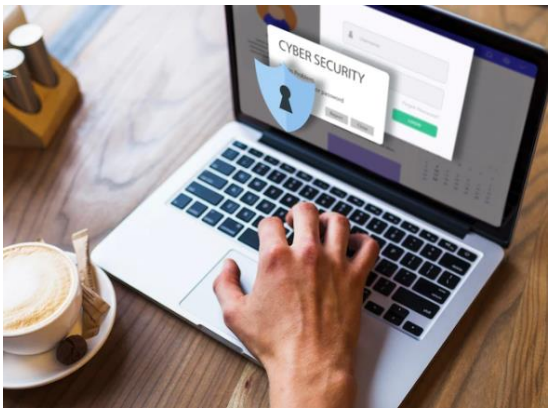
Néstor Raúl Cárdenas Corral
CIP – CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

John Fredy Quintero Tamayo
CIP – CSIRT Académico UNAD
https://orcid.org/0000-0003-0128-1214

Introducción

Este mes se celebra en todo el mundo, el mes de la Ciberseguridad. Es por esto, que el CSIRT Académico UNAD quiere compartir con toda la comunidad UNADISTA, algunas recomendaciones las cuales contribuyen en seguir mejorando la seguridad de nuestro entorno digital.

La información que compartimos en este boletín es *extraída de una serie de boletines publicados por Microsoft denominado "Kit "Be Cyber Smart" (Sea ciberinteligente)"*[1].



Recuperado de: https://www.freepik.es/

[1] https://www.microsoft.com/en-us/security/blog/?p=122149?ocid=eml_pg362740_gdc_comm_mw&mkt_tok=MTU3LUdRRS0zODIAAAGHqjGKSqLeTKgC2cF57fKc4xdy_1UNFjCFmK-Tbzr-zLgiSjswheox-7asHBNHwrdmiJD5FX6GKlTiNdiqGBWnZyfqFWMltDwv5P1XmcIaKHbC0e6hBNCM

Desarrollo

Recomendaciones para la protección de datos y dispositivos conectados a internet:

En el ejercicio de nuestras actividades de la cotidianidad, por lo general nuestros dispositivos están conectados a internet. Esto, sin duda alguna hace que nuestros datos puedan estar expuestos a internet, por tal motivo:

Recuperado de: https://securityintelligence.com/

- **Llegado el caso de recibir un mensaje o correo donde soliciten información personal, desconfie de este**. Tenga presente que los enalces o los sitios web falsos, puende atraer su atención y generar la confianza para que usted acceda a entregar la información que el ciberdelicuente quiere de usted. Para corroborar la información del remitente de la información, busque el sitio oficial y pongase deforma diecta en contacto con este.

- **Tenga cuidado con los archivos aduntos que vienen en los mensajes que ha recibido, los cuales no le generan confianza**. Procure no abrirlos o antes de dar doble clic sobre ellos, procure escanearlos a traves de una herramienta antivirus o sitio que realice esta funcion para reducir el riesgo de poder ser infectado con algun archivo malicioso. El CSIRT Academico UNAD, recomienda hacer uso de sitios como www.virtustotal.com para realizar escaneos a archvios, URLs o software que vaya a instalar.

- **Busque compartir información personal en tiempo real**. Es decir, estableciendo contacto persona a persona o persona a institución. Dado el caso de tener que compartir información por correo electrónico, haga uso de herramientas para cifrado de información[2].

- **Haga uso de aplicaciones de autenticación para mejorar su cibresguridad, sin necesidad de usar cotnraseña**. Para el caso de microsoft, le invitamos a dar una mirada a este enlace.

- **Haga uso de contraseñas fuertes haciendo uso de letras mayúsculas y minúsculas, números y caracteres especiales como: $, %, &, /.** Para facilitar un poco la gestión de estas, puede usar un adminstrador de contraseñas. Google cuenta con un administrador de contraseñas, al cual le invitamos a dar una mirada[3].

[2] https://support.microsoft.com/es-es/office/cifrar-mensajes-de-correo-373339cb-bf1a-4509-b296-802a39d801dc#:~:text=Cifrar%20un%20solo%20mensaje,continuaci%C3%B3n%2C%20haga%20clic%20en%20Enviar.
[3] https://support.google.com/accounts/answer/6208650?hl=es-419

Recomendaciones para la protección de suplantación de identidad (Phishing)

Esta técnica de ataque es una de las más reportadas por usuarios de la Universidad a este equipo de respuestas. Esto indica que toda la comunidad UNADISTA puede estar en riesgo de poder ser vulnerada por este tipo de acción delictiva. El CSIRT Académico Recomienda:

- De una mirada a las direcciones de correo del remitente. Tenga presente que el cambio de un carácter puede pasar desapercibido ante nuestros ojos.

- Verifique los correos electrónicos que contienen saludos genéricos y que soliciten actualización de forma urgente. Ejemplo. "Estimado cliente: se requiere la actualización de datos o su cuenta será inactivada".

- Si le genera duda algún correo, busque información de contacto de la empresa que aparece como remitente y póngase en contacto. Para este caso, no responda el correo ni abra los archivos adjuntos.

- Si debe transmitir información privada, preferiblemente haga uso de otro medio de comunicación. Puede ser línea telefónica, confirmando que la línea sea confiable o hágalo de forma presencial.

- Antes de hacer clic en algún enlace, verifique la procedencia del correo. Por lo general los ciberdelincuentes hacen uso de técnicas de redireccionamiento para robar sus datos mostrando formularios para iniciar sesión o para actualizar datos.

Recomendaciones para el inicio de sesión en nuestros equipos de computo

En el momento de apartarse o ausentarse de su sitio de trabajo o del lugar donde se encuentra su equipo de cómputo, apague el equipo si no requiere trabajar más con este o de cierre la sesión si tiene pensado trabajar en otro momento. Para esto, haga uso de cerrar sesión en el menú de inicio de Windows o de oprimir las teclas **Windows + L** al tiempo.

Así mismo, recuerde usar algún tipo de seguridad para poder acceder a su información, puede ser una contraseña con estructura segura que contenga las siguientes características:

- Por lo menos 12 caracteres de largo (pero 14 o más es mejor).
- Una combinación de letras mayúsculas, letras minúsculas, números y símbolos.
- Ninguna palabra que se pueda encontrar en un diccionario o el nombre de una persona, personaje, producto u organización.
- Significativamente diferente de sus contraseñas anteriores.

- Fácil de recordar, pero difícil de adivinar para otros.

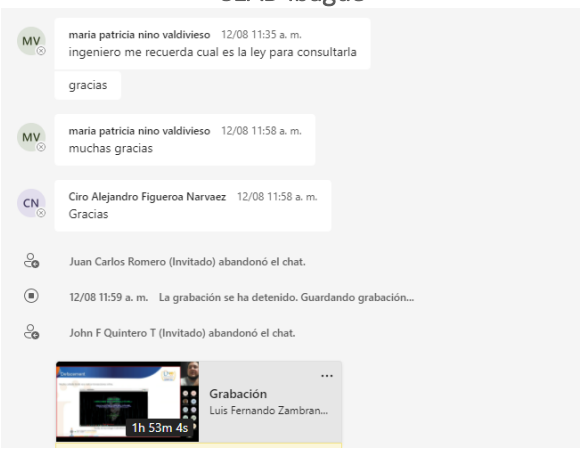
El CSIRT Académico UNAD, viene adelantando en los nodos centrales del país, con personal docente y administrativo, procesos de educación y cultura en ciberseguridad. Le invitamos a ser parte de esta estrategia de Ciberseguridad que sin duda alguna contribuye en el mejoramiento de nuestro entorno Digital.

Agradecemos de forma especial a los centros de **Ibagué** y **Palmira,** y a los docentes que se conectaron de forma virtual en estos espacios, a las Gerencias de **Talento Humano**, **Planeación,** a los **lideres de la ZCBC** y al equipo **PTI** por construir con nosotros una comunidad UNADISTA CIBERSEGURA.

CEAD Palmira

CEAD Ibagué

Lideres ZCBC



PTI

Canales de comunicación

El CIP 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

Recursos Bibliográficos Consultados

[1] Cybersecurity awareness tips from Microsoft to empower your team to #BeCyberSmart. [En línea] Microsoft. Recuperado: https://www.microsoft.com/en-us/security/blog/?p=122149?ocid=eml_pg362740_gdc_comm_mw&mkt_tok=MTU3LUdRRS0zODIAAAGHqjGKSqLeTKgC2cF57fKc4xdy_1UNFjCFmK-Tbzr-zLgiSjswheox-7asHBNHwrdmiJD5FX6GKlTiNdiqGBWnZyfqFWMltDwv5P1XmcIaKHbC0e6hBNCM [Último acceso: 28 10 2022]

[2] Cifrar mensajes de correo. [En línea] Microsoft. Recuperado: https://support.microsoft.com/es-es/office/cifrar-mensajes-de-correo-373339cb-bf1a-4509-b296-802a39d801dc#:~:text=Cifrar%20un%20solo%20mensaje,continuaci%C3%B3n%2C%20haga%20clic%20en%20Enviar [Último acceso: 28 10 2022].

[3] Cómo guardar, administrar y proteger tus contraseñas. [En línea] Google. Recuperado: https://support.google.com/accounts/answer/6208650?hl=es-419 [Último acceso: 28 10 2022]

[4] Cómo guardar, administrar y proteger tus contraseñas. [En línea] Google. Recuperado: https://support.google.com/accounts/answer/6208650?hl=es-419 [Último acceso: 28 10 2022]