Guía de

CIBER SEGU RIDAD

para todos

#UnidosSomosMásSeguros

Universidad de los Andes | Vicerrectoría Administrativa y Financiera | DSIT Dirección de Servicios de Información y Tecnología.

1

PREGUNTAS & RESPUESTAS

SOBRE LA CIBERSEGURIDAD

Aprende

¿Qué es la seguridad de la información?

Buscando asegurar la confidencialidad, integridad y disponibilidad de los datos digitales y físicos, la seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten proteger los datos y mitigar riesgos de robo o fuga de información.

¿Qué es la ciberseguridad?

Son buenas prácticas preventivas y correctivas que se implementan a través de tecnología y permiten defender los equipos de cómputo, las aplicaciones que se encuentran en el datacenter, la red cableada e inalámbrica de la universidad, los computadores y/o portátiles, sitios web y la cuenta Uniandes entre otros, de ataques maliciosos o amenazas digitales.

¿Qué son los ataques cibernéticos?

Los ataques cibernéticos o ciberataques son actos que infringen la ley y se cometen a través de la tecnología, tienen una gran variedad de fines como: chantajear y/o robar información institucional para pedir rescates; también pueden exponer, alterar, inhabilitar, o destruir información confidencial y/o restringida mediante accesos no autorizados con el fin de crear caos en las instituciones y/o utilizar recursos tecnológicos en la nube para financiar sus investigaciones.

¿Quiénes están detrás de ataque cibernéticos?

Delincuentes informáticos, hackers, organizaciones criminales, cuyo propósito es apropiarse de la información y/o de los recursos tecnológicos para extorsionar a las organizaciones o las personas vulneradas.

¿Qué tipo de ciberataques existen?

Los ciberdelincuentes informáticos, cada vez emplean técnicas más complejas, dañinas y difíciles de detectar. Los tipos de ciberataques existentes van en aumento debido al ingenio y creatividad de los ciberdelincuentes; algunas de las técnicas más usadas, son: **(i)malware**, es un software de carácter dañino que se instala en el dispositivo, se propaga por la red causando daño en los dispositivos que encuentre; **(ii)phishing**, es una técnica de ingeniería social que consiste en engañar y ganar la confianza de la víctima para robar las credenciales con el fin de obtener acceso a la información personal, financiera, confidencial y/o restringida.

Protege

¿Qué protegemos y por qué lo hacemos?

Protegemos la **Información institucional** generada en nuestros procesos **y la infraestructura tecnológica** que la soporta. La información institucional la protegemos porque ella contiene datos confidenciales y restringidos, a los cuales debemos cuidar y salvaguardar su privacidad e integridad .

Previene

¿Qué debemos hacer para protegernos?

Adquirir **conocimientos**, desarrollar **habilidades** y generar **cambio de comportamientos** frente a la seguridad, aplicando sentido común; con el fin de no caer en trampas expuestas por los ciberdelincuentes.

4 CLAVES
PARA NAVEGAR SEGURO
EN INTERNET

1 Tus dispositivos

La ciberseguridad se centra en los mecanismos o controles que sirven para proteger tus dispositivos y la información institucional cuando navegamos por la red o internet.

A diferencia de lo que podríamos pensar, para poner en práctica algunas medidas de seguridad sólo necesitamos aplicar algunos conceptos básicos y un poco de sentido común en la utilización de nuestros dispositivos.

Con las siguientes tres (3) recomendaciones de ciberseguridad, podrás mantener más seguros tus dispositivos informáticos y de esta manera salvaguardar la información institucional y personal.

Recuerda que **#UnidosSomosMásSeguros.**

1. Mantener actualizado el sistema operativo de todos tus dispositivos (portátiles, celulares, tablets), permite resolver fallas o vulnerabilidades que puedan ser aprovechadas por los ciberdelincuentes.

2. Tener por lo menos un antivirus activo en tus dispositivos y mantenerlo actualizado, es la principal protección contra las amenazas y el mejor filtro que tenemos para detectar y eliminar cualquier tipo de virus o malware (software malicioso).

3. Si descargas las aplicaciones directamente a tu computador, verifica que provengan de plataformas oficiales como: Microsoft Store, Google Play o App Store. Valida que los proveedores de estas aplicaciones sean confiables y tengan buenas valoraciones. Si descargas las aplicaciones directo a tu portátil, revisa los permisos que solicita para instalarse y analiza el programa descargado con el antivirus, antes de instalarlo en tu dispositivo.

Con estas medidas de protección, minimizamos el riesgo de que ataquen nuestros dispositivos y evitamos que roben nuestra información.

2 Cuenta Uniandes

La Cuenta Uniandes es la herramienta entregada por la Universidad para ingresar a los recursos digitales, por ello **¡Es importante protegerla!**.
Al salvaguardar tu cuenta Uniandes, estamos protegiendo la puerta de entrada a nuestros sistemas informáticos y a nuestra información. Tener buenas prácticas de seguridad con tu cuenta, minimizará ser víctima de robo de identidad y de acceso indebido a sistemas de información; previniendo así, el robo o pérdida de información confidencial o restringida. Aquí te dejamos dos (2) recomendaciones.

1. Usa una contraseña robusta con más de 12 caracteres, procura usar mayúsculas, minúsculas y caracteres especiales. ¡No utilices palabras fáciles de recordar como nombres o fechas de nacimiento! Una buena táctica es utilizar frases sin sentido o palabras que no existan en el diccionario combinando números y letras como: **ElCi3loEsdeColor3s&75#**

2. Activa el **A2P (doble factor de autentificación)**, este control es una medida de seguridad muy importante que adiciona una segunda capa de protección a tu cuenta para verificar el acceso a las cuentas en línea. Esta medida es de **uso obligatorio** para controlar el acceso a las aplicaciones y al correo institucional.

Estas prácticas nos ayudarán a protegernos de ataques de ciberdelincuentes que quieran acceder a los recursos digitales e información de la Universidad a través de la cuenta Uniandes. ¡Es responsabilidad tuya, proteger tu cuenta!

3 Conexión a la red

Hoy en día navegar en internet y conectar nuestros dispositivos electrónicos a la red, se volvió una necesidad. Para poder realizar estas conexiones las hacemos a través de las redes cableadas o inalámbricas (Wifi). Al conectarnos a estas redes debemos asegurarnos que sean redes seguras o que tengamos la certeza de que podemos confiar en ellas. A continuación, veremos algunos tips de protección para conectarnos a internet de manera segura:

1. Ten especial cuidado al conectarte a una red wifi pública. Estas redes pueden ser interceptadas por ciberdelincuentes para detectar cualquier intercambio de información que hagas desde tus dispositivos.

2. Mantén siempre actualizado tu navegador favorito en tus dispositivos. Un navegador desactualizado podría tener brechas de seguridad por las cuales los ciberdelincuentes a través de tu navegación pueden expiarte, robar tu cuenta y/o contraseña de acceso a tus aplicaciones.

3. Elimina las cookies e historial de navegación de manera periódica en tu navegador preferido. Las cookies son archivos que se descargan en tu dispositivo cuando utilizas navegadores y guarda información sobre tus hábitos de navegación en internet.

4. Activa el modo incógnito en tu navegador preferido, esta opción te permitirá usar la red sin que el navegador guarde ningún tipo de información de los sitios que visitas.

4 Evita engaños

Identifica las amenazas cibernéticas y evita engaños derivados del uso de técnicas psicológicas que buscan obtener información confidencial de la Universidad. Este tipo de trampas son llamadas **ingeniería social.**

La ingeniería social es un conjunto de técnicas de manipulación que usan los ciberdelincuentes para engañarnos, haciéndose pasar por otra persona u organización para obtener acceso a nuestros datos.

Técnicas de engaño

1. Phishing: es un ataque en el cual los mensajes que llegan **parecen provenir de una fuente fiable.**

2. Baiting: ocurre cuando un ciberdelincuente deja **olvidada una USB infectada con malware** (software malicioso) en un lugar fácil de hallar; si conectas la USB a tu computadora el delincuente podrá ver la información de tu computador y todo lo que haces.

3. El **vishing** es la práctica de suplantación de un **número telefónico.**

4. El **smishing** funciona por medio de mensajes de texto o SMS, normalmente se pide a la víctima que realice una **acción inmediata a través de un enlace malicioso.**

Si encuentras algún correo electrónico sospechoso, contacta a la DSIT por medio del correo unidossomosmasseguros@uniandes.edu.co y te responderemos de lunes a viernes antes de 12 horas.

Ciber Seguridad

#UnidosSomosMásSeguros

Universidad de los Andes | Vicerrectoría Administrativa y Financiera | DSIT Dirección de Servicios de Información y Tecnología.