Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

CONCIENTIZA TU CLIC

ANATOMÍA DE UN RANSOMWARE

¿QUÉ ES?

- Es un tipo de **malware** que cifra los archivos de un dispositivo, dejándolos inaccesibles.
- Los atacantes exigen un rescate **económico** para devolver el acceso a los datos.
- Afecta tanto a **usuarios individuales** como a organizaciones.

¿CÓMO FUNCIONA?

Infección: Ingresa al sistema a través de un archivo adjunto infectado, un enlace engañoso o una descarga insegura.

Cifrado de archivos: Bloquea el acceso a documentos, imágenes, bases de datos, entre otros, usando algoritmos.

Mensaje de rescate: Aparece una nota pidiendo un pago en criptomonedas, como Bitcoin, a cambio de la clave para descifrar los datos.

Impacto: Si no se paga, los datos pueden quedar inaccesibles permanentemente. Algunas variantes también amenazan con publicar información sensible.

¿SABÍAS QUE?

1. El primer caso documentado fue en **1989**, conocido como "AIDS Trojan".
2. Los ataques de ransomware han aumentado más del **80%** en los últimos años.
3. El **53%** de las organizaciones en Latinoamérica fueron víctimas de estos ataques en el último año.
4. En 2023, el costo promedio por ataque, incluido el rescate y la recuperación, superó los **$4 millones de dólares**.
5. Las **víctimas frecuentes** fueron empresas, hospitales, instituciones educativas y gubernamentales.
6. La forma de **propagación** fue a través de **correos electrónicos** maliciosos, enlaces fraudulentos y descargas inseguras.
7. Aproximadamente el **63%** de los ataques iniciaron con una intrusión en la red hasta 6 meses antes.

¿CÓMO PREVENIRLOS Y PROTEGERNOS?

- Mantener el **software actualizado** para cerrar posibles vulnerabilidades.
- Realizar **copias de seguridad periódicas** y guardarlas en dispositivos externos o en la nube.
- **No abrir archivos ni enlaces sospechosos** de remitentes desconocidos.
- **Usar herramientas de seguridad** como antivirus confiables y firewalls.
- Identificar y evitar amenazas potenciales, **notificar a Seguridad Informática** ante cualquier sospecha.

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

¿Qué es el QUISHING?

Es una técnica de phishing que utiliza **códigos QR** como medio para engañar a las personas y robar información confidencial. En lugar de un enlace directo sospechoso en un correo o mensaje, los ciberdelincuentes usan códigos QR que, al ser escaneados, redirigen a sitios maliciosos.

¿CÓMO FUNCIONA?

1. Creación del código malicioso

Los delincuentes generan un **código QR** que contiene un **enlace malicioso.**

2. Distribución del código QR

Colocan los códigos en **lugares estratégicos** como:

- Carteles físicos o digitales.
- Correos electrónicos disfrazados de comunicaciones legítimas.
- Páginas web o redes sociales.

3. Interacción del usuario

- El usuario escanea el código QR **confiando en que es seguro.**
- Es redirigido a un sitio web falso que **imita una plataforma conocida** o descarga malware en el dispositivo.

4. Robo de información o infección

Los delincuentes **obtienen acceso a datos sensibles** como contraseñas, información bancaria o incluso control del dispositivo.

RIESGOS DEL QUISHING

1. **Robo de datos personales:** Los ciberdelincuentes pueden capturar información como credenciales de inicio de sesión o números de tarjetas de crédito.
2. **Instalación de malware:** El código QR puede llevar a la descarga automática de aplicaciones maliciosas.
3. **Suplantación de identidad:** Los datos robados pueden usarse para suplantar la identidad de la víctima.
4. **Acceso no autorizado:** En las organizaciones, el Quishing puede dar acceso a redes internas, comprometiendo la seguridad de toda la empresa.
5. **Confianza afectada:** Puede generar desconfianza en el uso de códigos QR, afectando su implementación legítima para el comercio.

¿CÓMO PREVENIRLOS Y PROTEGERNOS?

Verificar el origen, asegurarse de que el código QR provenga de una fuente confiable.

Inspeccionar el contenido antes de escanear el contenido, validar con herramientas de seguridad digital.

Evitar escanear códigos de los correos electrónicos **que no hayan sido solicitados.**

Usar aplicaciones de seguridad, algunas aplicaciones de escaneo de códigos QR ofrecen análisis de seguridad.

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

¿Qué es el CIBERACOSO?

Es una forma de violencia digital con hostigamiento, amenazas o humillaciones a través de medios electrónicos como redes sociales, mensajería instantánea o correos electrónicos.

CAUSAS FRECUENTES

1. Uso excesivo y sin supervisión de las plataformas digitales.
2. Falta de educación en el uso responsable de la tecnología.
3. Anonimato en línea, lo que facilita las conductas agresivas.
4. Ausencia de límites claros en la interacción digital.

CONSECUENCIAS

1. Estrés, ansiedad y depresión.
2. Aislamiento social y baja autoestima.
3. Disminución del rendimiento académico.
4. En casos graves, pensamientos suicidas.

¿CÓMO PREVENIRLO?

1. Fomenta el diálogo abierto sobre el uso de internet.
2. Establece normas claras para la interacción en línea.
3. Supervisa y educa sobre el uso responsable de la tecnología.
4. Denuncia conductas inapropiadas en las plataformas digitales.

EN COLOMBIA

El **60% de las mujeres** ha sufrido de violencia digital.

7 de cada 10 niños y adolescentes han sido víctimas de ciberacoso.

Colombia ocupa el **puesto número 10** a nivel mundial en casos de ciberbullying.

RECUERDA

El ciberacoso es un problema serio que afecta la salud mental y emocional. Es responsabilidad de todos promover un entorno digital seguro y respetuoso.

Participa y comparte tus resultados de Interland con toda la comunidad Rosarista, usando el **#InterlandURosario** y sé un **#RosaristaDigital**

Universidad del Rosario | DITIC Dirección de Tecnología Informática y Comunicaciones

Juega, diviértete y aprende a no confiarte en el ciberespacio

INTERLAND

Sé genial en Internet.

Es un juego creado por Google donde a la vez que nos divertimos aprendemos sobre las precauciones y comportamientos en el Ciberespacio.

Conoce más de Interland aquí

Tips de seguridad informática aquí

ROSARISTA DIGITAL

NO TE CONFÍES EN EL CIBERESPACIO

*Juega desde cualquier dispositivo Android, iOS, Windows, Linux, o mediante cualquier explorador.

Universidad del Rosario | 370 Años | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

LA SEGURIDAD LA HACEMOS TODOS

¡NO HAGAS CLIC TAN RÁPIDO!

La seguridad la hacemos todos, y al seguir estas simples medidas podemos asegurar que nuestra información esté protegida.

1. El **correo electrónico** es el medio número uno para los ciberdelincuentes, siempre revisa si conoces a la persona que te envía los correos.
2. Si el mensaje del correo parece **sospechoso**, no des clic en ningún link ni descargues archivos adjuntos, ¡Repórtalo!
3. Siempre coloca el cursor sobre el vínculo para **verificar** la verdadera ruta a la que te está dirigiendo, antes de hacer clic en él.

ANTE CUALQUIER SITUACIÓN DE SOSPECHA

Reporta de inmediato a Servicios 2030 al correo electrónico servicios2030@urosario.edu.co

#ROSARISTADIGITAL

Universidad del Rosario | 370 Años Formando proyectos de vida al servicio del país | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

LA SEGURIDAD LA HACEMOS TODOS

Como #RosaristasDigitales contamos con **Microsoft OneDrive**, una herramienta segura que nos permite tener copias de respaldo de todos nuestros archivos y documentos.

Aprovecha todas las ventajas que ofrece esta herramienta:

- Siempre tendrás tus archivos a la mano: podrás acceder a ellos desde cualquier dispositivo con conexión a internet.
- Copias de respaldo: tus archivos estarán seguros en la nube, lo que significa que podrás recuperarlos en caso de pérdida o daño del dispositivo.
- Comparte y colabora: podrás compartir archivos y trabajar en tiempo real con tus compañeros de trabajo o estudio.
- Ahorra espacio en tu dispositivo: al guardar tus archivos en la nube, liberarás espacio en tu dispositivo.
- Mayor seguridad: Microsoft OneDrive cuenta con medidas de seguridad avanzadas para proteger tus archivos y datos personales.

¡No esperes más para proteger tu información y usar **OneDrive**!

LA SEGURIDAD LA HACEMOS TODOS

#ROSARISTADIGITAL

Universidad del Rosario | 370 Años Formando proyectos de vida al servicio del país | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

LA SEGURIDAD LA HACEMOS TODOS

En la URosario estamos comprometidos con la seguridad de tus datos e información.

Por eso, queremos hablarte sobre el phishing o suplantación de identidad, una práctica que busca engañarte para que compartas información confidencial.

¿CÓMO IDENTIFICAR UN CORREO PHISHING?

Si recibes un correo que te pide hacer clic en un enlace o descargar un archivo adjunto y no reconoces al remitente o no tienes cuenta con la compañía que se hace pasar, **podría tratarse de un intento de phishing**.

PARA PROTEGERTE, TE RECOMENDAMOS:

1. Verificar siempre la dirección del remitente antes de abrir cualquier correo electrónico, hacer clic en enlaces o descargar archivos adjuntos.
2. No compartir información personal o financiera a través de correos electrónicos, mensajes y/o redes sociales.
3. Mantener tus dispositivos y programas actualizados con un buen software de seguridad.
4. Usar contraseñas seguras y diferentes para cada cuenta y cambiarlas con regularidad.

Recuerda que todos nuestros **#RosaristasDigitales** cuentan con medidas de seguridad adicionales como el multifactor de autenticación (MFA) para proteger sus datos, pero es importante que tú también tomes precauciones. **¡La seguridad digital la hacemos todos!**

SI TIENES ALGUNA DUDA

O sospechas que has sido víctima de un ataque de phishing, por favor comunícate con nuestro equipo de soporte a través de los canales oficiales **servicios2030@urosario.edu.co** o en la línea **2970200 ext. 2030.**

Universidad del Rosario | 370 Años Formando proyectos de vida al servicio del país | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

LA SEGURIDAD LA HACEMOS TODOS

RECOMENDACIONES DE SEGURIDAD INFORMÁTICA

¡BLOQUEA ANTES DE RETIRARTE DE TU COMPUTADOR!

- Los datos son el nuevo oro
- Tu estación de trabajo puede ser el patio de recreo de un criminal
- Mantén el escritorio limpio y bloquea la pantalla de todos los dispositivos antes de salir

LA SEGURIDAD LA HACEMOS TODOS

#ROSARISTADIGITAL

Universidad del Rosario | 370 Años Formando proyectos de vida al servicio del país | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

LA SEGURIDAD LA HACEMOS TODOS

¡PROTEGE TUS CUENTAS EN REDES SOCIALES!

En estos tiempos digitales, es importante mantener nuestras cuentas de redes sociales seguras y protegidas. Por eso, te comparto algunas buenas prácticas de seguridad para que puedan aplicar en las cuentas de la Universidad que administran:

- Configura el multifactor de autenticación en cada aplicación que utilices para que tengas una capa extra de seguridad.
- Asegúrate de que tus claves de acceso sean robustas, con al menos 10 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
- Si tienes sospechas de que alguien más ha utilizado tus claves de acceso, cámbialas inmediatamente.
- No repitas las claves de acceso que has utilizado anteriormente y cámbialas cada mes.
- Si alguien deja de trabajar en la Universidad y tenía acceso a alguna cuenta, asegúrate de cambiar las claves de acceso correspondientes.
- Evita conectarte a redes wifi públicas o establecimientos públicos para digitar tus claves de acceso.
- Cierra tus sesiones de aplicaciones, sistemas de información, cuentas de correo y otros recursos tecnológicos después de utilizarlos.
- Si notas cualquier incidente de seguridad o sospechas de un evento inusual relacionado con tus claves de acceso, por favor repórtalo oportunamente a Servicios 2030.

SI TIENES ALGUNA DUDA

comunícate con Servicios 2030 al correo **servicios2030@urosario.edu.co** o a la línea 2970200 ext 2030. Estamos para ayudarte de lunes a viernes de 6:30 a.m. a 7:00 p.m. y sábados de 7:00 a.m. a 2:00 p.m.

¡GRACIAS POR HACER TU PARTE Y SER UN #ROSARISTADIGITAL!

Universidad del Rosario | 370 Años Formando aspectos de vida al servicio del país | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

¡LA SEGURIDAD DIGITAL LA HACEMOS TODOS!

¡PROTEGE TUS DATOS!

Tips para prevenir ataques informáticos.

En los últimos años, se ha presentado un aumento significativo de estos ataques a nivel global, nacional y local, dirigidos hacia universidades y otras organizaciones.

Los atacantes buscan suplantar organizaciones y personas para obtener el control de la información y solicitar pagos para su recuperación. Por eso, es importante tomar medidas preventivas para evitar ser víctima de estos ataques.

CAMBIA TU CONTRASEÑA DE PASAPORTE VIRTUAL

Como mínimo cada 30 días o inmediatamente exista indicio de que esta ha sido expuesta y/o utilizada por otra persona.

CONFIGURA TU CONTRASEÑA DE PASAPORTE VIRTUAL

Utiliza al menos diez (10) caracteres combinando mayúsculas, minúsculas, números y caracteres especiales.

NO UTILICES TU USUARIO Y CONTRASEÑA DE PASAPORTE VIRTUAL

para registrarse o autenticarse en plataformas digitales no institucionales.

Nota: recuerda que para gestionar el cambio de contraseña de Pasaporte Virtual, debes ingresar por este link: **https://pasaporte.urosario.edu.co/**

NUNCA RESPONDAS CORREOS ELECTRÓNICOS

de remitentes desconocidos o que soliciten el diligenciamiento de tu usuario y contraseña de tu cuenta institucional.

NO DESCARGUES NI ABRAS ARCHIVOS ADJUNTOS

de correos sospechosos o desconocidos.

HABILITA LA AUTENTICACIÓN MULTIFACTOR

para hacer más segura tu cuenta y el ingreso a tu información.

SI TIENES ALGUNA DUDA

Comunícate con nuestro equipo de Servicios 2030 a través de la línea telefónica 2970200 ext. 2030 o al correo **servicios2030@urosario.edu.co**.

Universidad del Rosario | 370 Años | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

LA SEGURIDAD LA HACEMOS TODOS

En la era digital, nuestras contraseñas son la primera línea de defensa para proteger nuestra información personal y privada.

¿ESTÁS SEGURO DE QUE TUS CONTRASEÑAS SON SEGURAS?

Te dejamos algunos consejos para crear contraseñas:

- Mezcla números, letras y caracteres especiales.
- Evita el uso de palabras comunes o información personal como: nombre de tu mascota, tu fecha de nacimiento, edad y evita repetir contraseñas utilizadas anteriormente.
- No compartas tus contraseñas con nadie.
- Cambia tus contraseñas con frecuencia.

Recuerda, la seguridad digital la hacemos todos.

¡Únete a **#RosaristaDigital** y protege tus cuentas con contraseñas seguras!

SI TIENES ALGUNA DUDA

Comunícate con nuestro equipo de Servicios 2030 a través de la línea telefónica 2970200 ext. 2030 o al correo **servicios2030@urosario.edu.co.**

Universidad del Rosario | 370 Años | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

LA SEGURIDAD LA HACEMOS TODOS

MEDIDAS DE SEGURIDAD INFORMÁTICA EN TU PUESTO DE TRABAJO

En la Universidad del Rosario estamos comprometidos con tu seguridad digital. Queremos recordarte algunos consejos simples pero importantes para proteger tu información y dispositivos:

- No permitas que otras personas manipulen tu estación de trabajo. Bloquea la pantalla de tus dispositivos.
- No compartas tus claves de acceso con nadie y cambia tu contraseña constantemente.
- Recuerda cerrar sesión en tu equipo y aplicaciones antes de salir para proteger la privacidad y seguridad de tus datos.
- Realiza copias de seguridad de tus datos importantes mediante **Microsoft OneDrive**.

Recuerda, **la seguridad digital la hacemos todos**.
Juntos podemos proteger nuestros datos y dispositivos.

Si tienes alguna duda comunícate con nuestro equipo de Servicios 2030 a través de la línea telefónica 2970200 ext. 2030 o al correo servicios2030@urosario.edu.co.

¡GRACIAS POR HACER TU PARTE Y SER UN #ROSARISTADIGITAL!

Universidad del Rosario | 370 Años | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

LA SEGURIDAD LA HACEMOS TODOS

PROTEGE TU INFORMACIÓN EN SOLO 3 PASOS

¡Protege tu información con la autenticación multifactor (MFA) en tu cuenta institucional de correo electrónico!

Con esta nueva funcionalidad podrás evitar accesos no autorizados y suplantación de identidad. Para configurarla, solo necesitas descargar la aplicación **Microsoft Authenticator** en tu dispositivo móvil. Una vez hecho esto, podrás aprobar el acceso a tu cuenta institucional.

¿CÓMO ACTIVARLA?

1. PARA CONTAR CON ESTA NUEVA FUNCIONALIDAD:
   Descarga la aplicación Microsoft Authenticator en tu dispositivo móvil, la cual te permitirá aprobar el acceso a tu cuenta institucional.

2. UNA VEZ CONFIGURADA TU CUENTA INSTITUCIONAL EN LA APLICACIÓN,
   debes considerar que podrás activar la función de huella digital y/o contraseña como un medio adicional para "Aprobar" el ingreso a Microsoft Authenticator y a tu cuenta de URosario.

3. APLICACIÓN MICROSOFT AUTHENTICATOR*
   Recibirás una notificación push a tu dispositivo móvil para "Aprobar" o "Denegar" el acceso a tu cuenta de URosario.

Únete a esta iniciativa, recuerda que la seguridad la hacemos todos.

*Progresivamente, a partir del 31 de julio de 2023, se activará esta configuración sobre tu cuenta.

SI TIENES ALGUNA DUDA

Comunícate con Servicios 2030 al correo **servicios2030@urosario.edu.co** o a la línea 2970200 ext 2030. Estamos para ayudarte de lunes a viernes de 6:30 a.m. a 7:00 p.m. y sábados de 7:00 a.m. a 2:00 p.m.

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

NO TE CONFÍES EN EL CIBERESPACIO

RECOMENDACIONES DE SEGURIDAD INFORMÁTICA

PISTAS PARA IDENTIFICAR UN SMS SMISHING

1. El **Remitente** es de un número celular desconocido.

2. El mensaje es **urgente, importante, llamativo** y lleva a hacer clic en algún vínculo.

3. Contiene un enlace, generalmente acortado, para **hacer clic**.

4. Invita a descargar una supuesta **aplicación -app**.

5. Solicita **datos personales**, credenciales o bancarios.

#ROSARISTADIGITAL

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

NO TE CONFÍES EN EL CIBERESPACIO

VISHING: estafa por llamada telefónica

El **vishing** es un ataque basado en el engaño y la manipulación, donde por medio de una **llamada telefónica** el atacante **suplanta la identidad** de una empresa, organización o persona de confianza para lograr su acto fraudulento.

Te recomendamos tener **precaución al compartir** tus datos personales en correos electrónicos o a personas desconocidas. Los estafadores desarrollan un **ambiente de confianza** incluyendo llamadas telefónicas para llevar a cabo el fraude.

#ROSARISTADIGITAL

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

NO TE CONFÍES EN EL CIBERESPACIO

WHATSAPP

Es una de las mensajerías instantáneas mas usadas en el mundo.

Puedes ser victima de fraude por medio de chats con **ofertas laborales, comerciales, premios** en donde te piden información confidencial.

En varios casos los ciberdelincuentes intentarán acceder y/o tomar control de tu WhatsApp por medio de envió de códigos verídicos de WhatsApp.

Recomendaciones para protegerte de este ataque/fraude:

1. No hacer clic en enlaces sospechosos con ofertas laborales, comerciales o premios.
2. No suministrar información personal o confidencial a contactos o números sospechosos.
3. Bloquear y denunciar / reportar los chats, contactos y/o números sospechosos ante WhatsApp.
4. Verificar constantemente los contactos añadidos y sus números telefónicos celulares para evitar estafas.
5. Verificar el numero de contacto teniendo presente el prefijo del país, por ejemplo, en Colombia el numero telefónico celular debe empezar con +57.
6. No contestar llamadas ni mensajes a números sospechosos o desconocidos, especialmente los prefijos que mas utilizan los ciberdelincuentes son: +95, +91, +212, +225, +231, +233, +234, +355, +387.

#ROSARISTADIGITAL

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

NO TE CONFÍES EN EL CIBERESPACIO

EL MALWARE

Es un programa malicioso que realiza acciones dañinas en el sistema de información, sin el consentimiento del usuario.

El Adware es un programa que automáticamente muestra u ofrece **publicidad** en una pagina web o en una instalación de software.

Muchas veces el Adware puede ser usado por ciberdelincuentes para instalar Malware.

Los términos de uso de diferentes software no confiables no son completamente transparentes y pueden **ocultar** acciones maliciosas.

Se recomienda no hacer clic a los Adware, navegar por paginas seguras e instalar software confiable.

#ROSARISTADIGITAL

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

NO TE CONFÍES EN EL CIBERESPACIO

EL CARDING

"Carding" -card es tarjeta en inglés-.

es un tipo de fraude que utiliza información de tarjetas robadas para utilizarlas de manera fraudulenta.

RECOMENDACIONES PARA PROTEGERTE DE ESTE ATAQUE/FRAUDE:

1. No hacer caso a mensajes spam o correos electrónicos con remitentes desconocidos.

2. Llevar un periódico control de tus operaciones y transacciones bancarias. En especial en fechas de alta demanda como: rebajas, vacaciones, navidad, Black Friday, etc.

3. Desactivar el sistema NFC Near field communication o comunicación de campo cercano de tu celular o utiliza un protector antirrobo de tarjetas para guardarlas en tu bolsillo.

4. Realizar compras online que usen pasarela de pago o métodos de pago seguro.

5. No proporcionar información en páginas de dudosa reputación.

6. Usar tarjetas monedero o virtuales que te ofrezca el banco para pagos online.

7, Habilitar la confirmación con PIN cuando uses el sistema NFC Near Field Communication o comunicación de campo cercano.

8.Nunca proporcionar los datos bancarios por teléfono.

9. No usar ordenadores públicos para hacer compras.

10. Activar el doble factor de autenticación -MFA- para los pagos con tarjeta.

#ROSARISTADIGITAL

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

NO TE CONFÍES EN EL CIBERESPACIO

EL ROBO DE IDENTIDAD DIGITAL

es un ciberdelito donde una persona se hace pasar por otra con el fin de obtener beneficios, generar un fraude u ocasionar un daño.

¿QUÉ HACER ANTE UNA SUPLANTACIÓN O ROBO DE IDENTIDAD?

1. **Actuar de inmediato**. Los problemas asociados pueden ser muy graves, desde un desprestigio social hasta una deuda millonaria en diferentes entidades financieras.

2. Consultar urgente con un **abogado especializado** en suplantación de identidad.

3. **Obtener** toda la información relacionada como mensajes, capturas de pantalla, correos electrónicos, etc.

4. **Denunciar** la red social que corresponda para que se elimine la cuenta falsa.

5. Presentar la **denuncia** ante la Fiscalía General y la Policía Nacional de Colombia.

6. Informar a la entidad para que **bloquee e impida** cualquier actividad con las cuentas bancarias.

#ROSARISTADIGITAL

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

ANTISPAM

Es un software que permite a los usuarios prevenir o restringir la entrega de spam / correos no deseados.

En la Universidad del Rosario contamos con un mensaje de precaución sobre los correos electrónicos externos. Además, advierte sobre los correos no deseados, sospechosos y los riesgos al descargar archivos adjuntos o dar clic a links.

NO TE CONFÍES
EN EL CIBERESPACIO

#ROSARISTADIGITAL

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

REPORTAR INCIDENTES

Un incidente es un suceso en el cual ocurre o podría haber ocurrir un daño, deterioro o riesgo a otra persona o a la institución.

Ejemplos de incidentes

- Ver personas extrañas usando equipos de computo
- Uso inadecuado de la red de la universidad para enviar información
- Suplantación
- Escaneos
- Usar los recursos de Office de manera ilegal para compartir información confidencial.

Recuerda que debes reportar cualquier incidente de seguridad al correo

servicios2030@urosario.edu.co

NO TE CONFÍES EN EL CIBERESPACIO

#ROSARISTADIGITAL

Universidad del Rosario | DITIC Dirección de Tecnología, Informática y Comunicaciones

ROSARISTA DIGITAL

SEGURIDAD PROTECCIÓN DE LOS NIÑOS PARA FUNCIONARIOS
CONTROL PARENTAL

Padres de familia

- Existen diversos riesgos en internet que afectan a los menores de edad. Desde contenido inapropiado, virus, malware (publicidad engañosa), noticias falsas, fraudes, grooming, ciberacoso, entro otros. Te damos estos tips para que implementes con tus hijos
- Si autorizas que tengan una **red social**, lo recomendable es que creen el perfil juntos, configuren las **opciones de privacidad**, negocien el tipo de contenido que subirán y crear una contraseña segura.
- Si tu hijo **juega en línea**, asegúrate de establecer una relación de confianza contigo y que puedan hablar de los riesgos. Que nunca entregue información personal, datos, ubicación e información financiera.
- **Netflix** cuenta con opciones de control parental donde podrás crear perfiles de con clasificación por edad específica, para evitar contenido inadecuado para los menores.
- **Amazon** ofrece opciones de control parental donde puedes configurar diversos aspectos de Prime Video y prevenir las compras accidentales.

NO TE CONFÍES EN EL CIBERESPACIO

#ROSARISTADIGITAL