Rur@link
Conectamos el campo con el mundo

INFORMACION SOBRE SEGURIDAD

Internet y sus herramientas asociadas son mecanismos ágiles que proveen una alta gama de posibilidades de comunicación, interacción y entretenimiento, tales como elementos de multimedia, foros, chat, correo, comunidades, bibliotecas virtuales entre otros que pueden ser accedidos por todo tipo de público. Sin embargo, estos elementos deben contener mecanismos que protejan y reduzcan los riesgos de seguridad alojados, distribuidos y potencializados a través del mismo servicio de Internet.

Las empresas, instituciones, los gobiernos y las personas utilizan cada vez la World Wide Web para distribuir información importante y realizar transacciones comerciales.

"RURALINK SAS" como proveedor del servicio de conectividad sabe que las relaciones con nuestros clientes se deben fortalecer desde una comunicación asertiva, sana y orientada a proporcionar las herramientas y concejos prácticos necesarios para la protección adecuada de los elementos de cómputo y los servicios asociados a la Internet. Por ello ponemos a disposición de todos, conceptos que pueden evitar o reducir los riesgos a que se está expuesto cuando se interactúa con la Internet y sus elementos asociados.

Conceptos Generales de Seguridad

Son aquellas acciones que están encaminadas al establecimiento de directrices que permitan alcanzar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones ante un evento que las interrumpa.

Integridad: La información producida es de calidad porque no puede ser modificada por quien no está autorizado.

Confidencialidad: La información solo debe ser legible para los autorizados, la misma debe llegar a destino con la cantidad y calidad con que fue prevista.

Disponibilidad: la información debe estar disponible cuando se la necesita. Irrefutabilidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría de quien provee de dicha información.

Activo: Recursos con los que cuenta la empresa y que tiene valor, pueden ser tangibles (servidores, desktop, equipos de comunicación) o intangibles (Información, políticas, normas, procedimientos)

Vulnerabilidad: Exposición a un riesgo, fallo o hueco de seguridad detectado en algún programa o sistema informático.

Amenaza: Cualquier situación o evento posible con potencial de daño, que pueda presentarse en un sistema.

Riesgo: Es un hecho potencial, que en el evento de ocurrir puede impactar negativamente la seguridad, los costos, la programación o el alcance de un proceso de negocio o de un proyecto. Correo electrónico: El correo electrónico es un servicio de red que permite que los usuarios envíen y reciban mensajes incluyendo textos, imágenes, videos, audio, programas, etc., mediante sistemas de comunicación electrónicos.

Elementos de protección

Firewall: Elemento de protección que sirve para filtrar paquetes (entrada o salida) de un sistema conectado a una red, que puede ser Internet o una Intranet. Existen firewall de software o hardware. Este filtrado se hace a través de reglas, donde es posible bloquear direcciones (URL), puertos, protocolos, entre otros.

Anti-virus: Programa capaz de detectar, controlar y eliminar virus informáticos y algunos códigos maliciosos (Troyanos, Works, Rootkits, Adware, Backdoor, entre otros). Estos contienen distintos módulos que nos ayudan a mantener seguro nuestros equipos, entre estos módulos podemos encontrar:

- Anti-phishing
- Control parental
- Anti-malware
- Anti-Ransomware
- VPN

Anti-spam: Programas capaz de detectar, controlar y eliminar correos spam. Criptografía: Es el arte cifrar y descifrar información con claves secretas, donde los mensajes o archivos sólo puedan ser leídos por las personas a quienes van dirigidos, evitando la interceptación de éstos.

Medios de almacenamiento externo

Se conoce como medio de almacenamiento externo todo dispositivo como (USB, disco portable, MicroSD, entre otros sistema de almacenamiento externos), es recomendable analizar y desinfectar cualquier dispositivo que se conecte a nuestro ordenador, estos pueden ser quienes infecten nuestro sistema operativo, cabe aclarar que todos los sistemas operativos son vulnerables a virus, como Windows, Linux y MacOS. Utiliza un buen antivirus.

Actualizaciones del sistema operativo

Es muy importante mantener nuestro sistema operativo actualizado, por lo general todos los fabricantes liberan constante y periódicamente actualizaciones parchando vulnerabilidades y fallos en los sistemas. Esto lo hacemos con el fin de lograr mayor seguridad y evitar que un nuevo virus afecte nuestros dispositivos.

Amenazas de seguridad

Spam: Envío de cualquier correo electrónico, masivo o no, a personas a través de este medio que incluyen temas tales como pornografía, bromas, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

Ingeniería social: Es la manipulación de las personas para convencerlas de que ejecuten acciones, actos o divulguen información que normalmente no realizan, entregando al atacante la información necesaria para superar las barreras de seguridad.

Código Malicioso: Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Ejemplo: Troyanos, Works, Spyware, Rootkits, Adware, Backdoor, Cookies, Dialers, Exploit, Hijacker, keyloggers, Pornware, etc.

Tipos de virus

Adware: Un adware es un software que muestra anuncios. “Los adware se instalan generalmente sin que nosotros lo deseemos. “Los adware suelen rastrear nuestro uso del ordenador para mostrar publicidad que tiene que ver con nuestras búsquedas en diferentes buscadores o relacionados con los sitios que visitamos”.

Spyware: El spyware es un software espía que recopila información de un ordenador. “Tras obtener los datos, los transmite a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador”

Ransomware: Consiste en que el pirata bloquea el smartphone u ordenador con un mensaje en el que solicita un rescate para liberarlo. El usuario debe pagar dicho rescate en la moneda digital Bitcoin, para que no se pueda rastrear y se mantenga el anonimato del pirata.

Gusanos: Tiene la capacidad de replicarse en un sistema, por lo que el ordenador podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador a gran escala.

Troyano: Se trata de un tipo de programa que contiene otro dentro de él, al ejecutarlo instalará el virus en el ordenador, se suele ver comúnmente en activadores, cracks o KeyGens.

Hoax: Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena, aparte de ser molesto, congestiona las redes y los servidores de correo, pueden ser intencionales para la obtención de direcciones de correo para posteriormente ser utilizadas como spam. Algunos de los Hoax más conocidos son correos con mensajes sobre virus incurables, temática religiosa, cadenas de solidaridad, cadenas de la suerte, Regalos de grandes compañías, entre otros.

Suplantación: Hacerse pasar por algo o alguien, técnicamente el atacante se hace pasar por un servicio o correo original.

Fraudes

Phishing: Es la capacidad de duplicar una página Web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada.

Se tienen dos variantes de esta amenaza:

Vishing: Utilización de técnicas de phishing pero para servicios asociados con voz sobre IP (VoIP).

Smishing: Utilización de técnicas de phishing en los mensajes de texto de teléfonos móviles.

1. ¿Cómo funciona?

A través de Sitio Web

En primera instancia los atacantes crean un sitio Web similar al original, trascribiendo textos, pegando las mismas imágenes y los mismos formularios para digitar los datos.

Una vez creado el sitio, lo publican en la Web con un alias parecido al sitio original. Ej: Reemplazando un simple de caracteres, usando un dominio real como prefijo: o

Sitio oficial – www.sitiooriginal.com o Sitio falso: www.sitiooriginal.com.sitio.com

Variaciones:

www.sitiooriginal-account.com www.sitiooriginal.actualiza.com

Jugar con la percepción y la lectura del usuario:

www.sitiio.original.com www.sitio.original.com/bin/actualiza

Adicional a esto, fijan una imagen simulando ser un sitio seguro (con certificados digitales) que, a simple vista da mucha confianza, pero son FALSOS:

Una vez realizado esta labor y utilizando mecanismos masivos de comunicación como el spam, envían correos indicando a los "posibles" clientes o usuarios del portal a que actualicen sus datos, invocando la posibilidad de dar obsequios o premios si hacen esta acción.

A través de Correo electrónico

Esta modalidad es realizada enviando correos masivos a las personas solicitando informen sus datos personales, lo correos engañosos pueden indicar que existe un problema técnico y es necesario restablecer las contraseñas.

Los correos llegan a nombre de una empresa o razón social, donde el atacante suplanta el nombre de dicha empresa

2. ¿A quién le puede pasar?

A cualquier usuario que tenga un correo electrónico y acceso a Internet, donde periódicamente haga consultas y/o actualizaciones en portales que le presten servicios: Tiendas virtuales, Bancos, portal de correo, pago de servicios públicos, etc.

3. ¿Dónde está el peligro y cómo podemos ser víctimas?

El peligro radica en que, al ser una página falta, inducen a los usuarios a que ingresen los datos personales, como cuantas de correo, número de tarjetas de crédito, claves, etc. y estos datos son recogidos por el atacante en bases de datos ajenas a las entidades oficiales de los sitios. Al sitio Web "similar" al original, es difícil que el usuario se percate, en primera instancia, de que se trata de un engaño.

Cuando llega un correo indicando sean actualizados los datos, los usuarios validan las bondades de estar actualizados e ingresan desde el enlace o link del correo, directamente a la página falsa. Al ser un spam "atractivo", los usuarios hacen un reenvió de este a más usuario, formándose una cadena o Hoax para capturar más y más personas.

Y si es a través del correo, los usuarios enviarían los datos personales (usuario y contraseña) a un correo desconocido.

4. ¿Cuáles son las consecuencias?

Una vez se ingresen los datos personales, son almacenados en bases de datos del atacante, que posteriormente utilizará en beneficio propio para realizar estafas o robos de dinero, dado que tiene en número de la cuenta bancaria y la clave de acceso (si el sitio falso es una entidad bancaria).

5. ¿Cómo se puede evitar?

Siempre que llegue este tipo de mensajes, ingrese directamente al sitio oficial desde el browser o navegador, nunca desde el link enunciado en el correo, ni dando clic al enlace.

Evite el envío de mensajes cadena, pornografía, mensajes no solicitados, bromas a otros remitentes de correo.

Cuando ingrese al sitio, valide que la seguridad que se indica a través de certificados digitales, si estén respaldados, de doble clic el icono de seguridad, que debe estar ubicado en la parte inferior derecha del navegador (no dentro de la página).

- No ingrese a páginas web de bancos o páginas que usen usuario y contraseña sin que esta use el protocolo https.
- Verifique que la página web contenga un candado o un certificado válido.
- Verifique que la URL a la que está ingresando es la oficial.
- No abra POP UPs o ventanas emergentes en páginas web sospechosas.
- Si la página web a la que está ingresando no cumple con los parámetros de seguridad no ingrese sus datos personales o credenciales de acceso.
- Use doble factor de autenticación, las contraseñas ya no son seguras.
- Use contraseñas seguras, robustas.

Conozca de antemano cual es la dirección o URL del sitio real y valide este nombre cada que ingrese a realizar un proceso donde deba ingresar sus datos. Recuerde que el atacante utiliza técnicas que pueden engañar la percepción del sitio cuando se lee.

Si usted es un usuario frecuente de portales donde se ingresan datos personales, manténgase actualizado, consultando en la página de la policía nacional (http://www.policia.gov.co/), CAI virtual, los últimos eventos, recomendaciones y consultas en línea.

Pornografía Infantil:

Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se encuentren actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.

Control de virus y códigos maliciosos:

Mantenga siempre un antivirus actualizado en su equipo(s), procure correr éste periódicamente, de la misma manera, tenga en su equipo elementos como anti- spyware y bloqueadores de pop-up (ventanas emergentes).

Evite visitar páginas no confiables o instalar software de dudosa procedencia. La mayoría de las aplicaciones peer-to-peer contiene programas espías que se instalan sin usted darse cuenta.

Asegúrese que se aplican las actualizaciones en sistemas operativos y navegadores Web de manera regular.

Si sus programas o el trabajo que realiza en su computador no requieren de pop- up, Java support, ActiveX, Multimedia Autoplay o auto ejecución de programas, deshabilite estos.

Si así lo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.

Correo electrónico:

- No publique su cuenta de correo en sitios no confiables.
- No preste su cuenta de correo ya que cualquier acción será su responsabilidad.
- No divulgue información confidencial o personal a través del correo.
- Si un usuario recibe un correo con una advertencia sobre su cuenta bancaria, no debe contestarlo
- Nunca responda a un correo HTML con formularios embebidos.

• Si ingresa la clave en un sitio no confiable, procure cambiarla en forma inmediata para su seguridad y en cumplimiento del deber de diligencia que le asiste como titular de la misma.

Control de Spam y Hoax:

• Nunca hacer clic en enlaces dentro del correo electrónico aun si parecen legítimos. Digite directamente la URL del sitio en una nueva ventana del browser

• Para los sitios que indican ser seguros, revise su certificado SSL.

• No reenvié los correos cadenas, esto evita congestiones en las redes y el correo, además el robo de información contenidos en los encabezados.

Control de la Ingeniería social:

• No divulgue información confidencial suya o de las personas que lo rodean.

• No hable con personas extrañas de asuntos laborales o personales que puedan comprometer información.

Control de phishing y sus modalidades:

• Si un usuario recibe un correo, llamada o mensaje de texto con una advertencia sobre su cuenta bancaria, no debe contestarlo.

• Para los sitios que indican ser seguros, revise su certificado SSL.

• Valide con la entidad con quien posee un servicio, si el mensaje recibido por correo es válido.

• Robo de contraseñas:

• Cambie sus contraseñas frecuentemente, mínimo cada 30 días.

• Use contraseñas fuertes: Fácil de recordar y difícil de adivinar.

• Evite fijar contraseñas muy pequeñas, se recomienda que sea mínimo de una longitud de 10 caracteres, combinada con números y caracteres especiales.

• No envié información de claves a través del correo u otro medio que no esté encriptado.

Conexión Wi-FI

Todos usamos conexiones Wi-Fi ya sea en nuestros lugares de trabajo en en nuestros hogares, no podemos usar una red vulnerable y hacer nuestras transacciones bancarios sin prestar atención a ello, una red Wi-Fi insegura es aquella que está abierta o sin contraseña, una red que no cambia periódicamente su clave.

Nuestra Wi-Fi debe estar segura, alguien podría entrar en nuestra red y cometer un delito sin que nosotros lo sepamos y ser nosotros quienes tengamos que responder ante las autoridades por ser quienes contratamos el servicio.

Es recomendable, no compartir la clave Wi-Fi con todos, es recomendable cambiar la clave periódicamente, saber cuántas personas están conectadas a nuestra red.

Contraseñas seguras

El uso de contraseñas robustas evita en un alto porcentaje que nuestras cuentas sean robadas o pirateadas, una contraseña segura contiene letras, número, caracteres especiales y mayúsculas. Nunca se debe usar información personal para crear una contraseña, información tal como nuestro nombre, nuestra cédula de ciudadanía, teléfono fijo o celular, nombre de mascota o hijos, deportes favoritos, gustos entre otros.

¿Cómo crear una contraseña robusta?

Es tan sencillo como esto, crear una contraseña segura para algunas personas puede llegar a ser un dolor de cabeza, pero siguiendo estos pasos será mucho más fácil.

- Inicia con un carácter especial, * $ # entre otros.
- Usan una mayúscula al inicio y al final.
- Puedes usar nombres pero cambia las vocales por números por ejemplo la “i” por un “1” la “o” por un “0” cero.
- cambia tu contraseña periódicamente.

Rur@link
Conectamos el campo con el mundo

MECANISMOS DE SEGURIDAD DE RURALINK SAS

RURALINK SAS ha formulado este protocolo con el fin de establecer lineamientos claros y recomendaciones sobre el uso responsable del servicio de internet. con el manual se pretende:

- Fomentar prácticas seguras para proteger la privacidad y seguridad en la transmisión de datos
- Prevenir actividades que afecten la integridad del servicio o sus usuarios
- Dar cumplimiento a las regulaciones vigentes tanto a nivel nacional como internacional.

Mal Uso del Servicio

Este protocolo identifica usos inapropiados, ya sea por parte de usuarios o terceros, que vulneren los principios de seguridad y legalidad. Estas acciones pueden acarrear sanciones administrativas, contractuales o incluso penales.

"RURALINK SAS" se reserva el derecho de evaluar de forma unilateral si un comportamiento transgrede este protocolo. Ante denuncias de uso indebido, se notificará al usuario y se remitirá a las autoridades competentes. **"RURALINK SAS"** podrá tomar medidas preventivas incluso antes del pronunciamiento oficial.

Aplicabilidad y Modificaciones

- El protocolo aplica a todos los usuarios del servicio de Internet de **"RURALINK SAS"**
- Es un complemento del contrato suscrito por el usuario, sin sustituirlo
- En caso de discrepancia, primará el contrato
- Las actualizaciones se publicarán en: https://ruralink.com.co/

Usos Prohibidos:

Está prohibido utilizar el servicio para:

- Enviar mensajes masivos no solicitados (spam)
- Propagar virus, programa maligno o ejecutar ataques informáticos
- Saturar deliberadamente el ancho de banda
- Acceder a sistemas o redes sin autorización
- Suplantar identidad digital, modificar encabezados TCP/IP o correos electrónicos
- Instalar software no autorizado que afecte el funcionamiento de los equipos
- Distribuir contenidos que infrinjan derechos de autor o de propiedad intelectual
- Acceder o manipular dispositivos físicos (router, splitter, módem; sin autorización.

Actividades Ilegales

Queda expresamente prohibido el uso del servicio para:

- Violentar normas nacionales o internacionales
- Suplantar identidades, clonar sitios web, o cometer fraudes financieros
- Realizar prácticas de hacking, sniffing, escaneo de puertos o ataques de denegación de servicio
- Difundir material amenazante, difamatorio, terrorista, obsceno y/o discriminatorio

Responsabilidad del usuario

Cada usuario es responsable por mantener la seguridad de su red local, servidores y dispositivos asociados. Entre las buenas prácticas se incluye:

- Evitar la configuración de servidores abiertos (SMTP/FTP)
- Prevenir usos no autorizados desde su red por parte de terceros

Envío de SPAM

Está prohibido el uso del servicio para realizar campañas de publicidad no autorizada o masiva hacia otros usuarios.

Accesos Indirectos

El usuario será directamente responsable por el uso indebido que terceros hagan de la red mediante su acceso, aparte de cualquier consentimiento previo.

Consecuencias

- Suspensión inmediata del servicio
- Filtros o bloqueos del acceso a puertos (como SMTP 25)
- Denuncia ante autoridades competentes
- Terminación definitiva del contrato sin derecho a reembolso

Canales de Reporte: se requieren evidencias (registros, IP origen, fecha).

- **Terceros o usuarios externos**: A través de las diferentes herramientas dispuesta por **"RURALINK SAS"** en: : https://ruralink.com.co/

Glosario

Término	Definición
Autenticación	Verificación de identidad de usuarios, dispositivos o sistemas.
Autorización	Proceso que determina los permisos asignados a una entidad autenticada.
Cifrado (Encriptación)	Técnica que protege la información codificándola para evitar accesos no autorizados.
Firewall (Cortafuegos)	Herramienta que filtra y controla el tráfico entre redes, bloqueando amenazas.
Phishing	Estrategia fraudulenta para obtener datos personales mediante engaños.
Malware	Software malicioso diseñado para comprometer dispositivos o redes.
VPN (Red Privada Virtual)	Red segura que protege la conexión de usuarios en entornos públicos.
Control de Acceso	Mecanismos que limitan el uso o acceso a información y sistemas.
Actualizaciones de Seguridad	Correcciones que fortalecen sistemas ante vulnerabilidades detectadas.
Respaldo (Backup)	Copias de información que permiten su recuperación ante pérdidas o fallos.
Datos Sensibles	Información que requiere protección especial por su naturaleza
Brecha de Seguridad	Incidente en que se vulnera la confidencialidad, integridad o disponibilidad de los datos.
Seguridad de la Información	Prácticas destinadas a proteger activos digitales de riesgos diversos.
Antivirus	Software que detecta y elimina amenazas informáticas.
Ransomware	Malware que secuestra datos y exige un pago para liberarlos.
Ingeniería Social	Técnica que manipula a personas para extraer información confidencial.
Protección de Datos	Conjunto de prácticas legales y técnicas para garantizar la privacidad digital.
Hashing	Método que convierte datos en una cadena única irrepetible.
Seguridad Perimetral	Estrategias para proteger los accesos externos a una red.
Cookies	Archivos temporales que rastrean la actividad del usuario en la web.
Spoofing	Suplantación digital de identidad para lograr acceso ilegítimo.
IDS (Sistema de Detección de Intrusos)	Tecnología que analiza el tráfico para identificar ataques o accesos no autorizados.
Seguridad en la Nube	Medidas para proteger información almacenada en servicios cloud.

"RURALINK SAS" cuenta con sistemas de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, al igual que control es de autenticación para los usuarios (equipos terminales de acceso del usuario).

"RURALINK SAS" cuenta con diferentes protecciones para controlar el acceso a los servicios de Internet tales como los mecanismos de identificación y autorización respecto a los servicios. Para proteger las plataformas de los servicios de Internet,

"RURALINK SAS" ha implementado configuraciones de seguridad base en los diferentes equipos de red, lo que comúnmente se llama líneas base de seguridad, además del establecimiento de medidas de seguridad a través de elementos de control y protección como:

Firewall:

A través de éste elemento de red se hace la primera protección perimetral en las redes de **"RURALINK SAS"** y sus usuarios, creando el primer control que reduce el nivel de impacto ante los riesgos de seguridad.

Antivirus:

Tanto las estaciones de trabajo como los servidores de procesamiento interno de información en **"RURALINK SAS"** son protegidos a través de sistemas anti códigos maliciosos.

Antispam:

Todos los servidores de correo poseen antispam que reduce el nivel de correo basura o no solicitado hacia los usuarios, descongestionando los buzones y el tráfico en la red.

Filtrado de URLs:

"RURALINK SAS" para el bloqueo de sitios con contenido de pornografía infantil, utiliza Servidores para realizar el filtrado de estos sitios. El objetivo principal de este filtrado es denegar el acceso a los sitios que contengan o promueva pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales. Se sugiere instalar además sistemas parentales.

Seguridad a nivel del CPE:

Los dispositivos de conexión final ubicados en las premisas de los usuarios cuentan con elementos bases para la autenticación y autorización, con ello permiten hacer una conexión a Internet de manera más segura.

Rur@link

Conectamos el campo con el mundo

PBX: 604 74 95 311 774 71 26
C. comercial La Gran manzana piso 3 loc. 303
Marinilla Ant.

www.ruralink.com.co
e-mail. contacto@ruralink.com.co
@ruralinkoriente
@ruralink