Serkoi
Servicios de conectividad inalámbrica
Internet al alcance de todos

ELEMENTOS DE SEGURIDAD

La red mundial Internet y sus elementos asociados 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.

SERKOI como proveedor del servicio de conectividad está convencido de que las relaciones con nuestros clientes se deben fortalecer desde una comunicación asertiva, sana y orientada a proporcionar las herramientas y consejos prácticos necesarios para la protección adecuada de los elementos de cómputo y los servicios asociados a la Internet.

Por esta razón ponemos a disposición de todos nuestros clientes y de la comunidad en general, conceptos teórico - prácticos 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

Confidencialidad: Se refiere a que la información solo puede ser conocida por individuos autorizados Integridad Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.

Disponibilidad. Se refiere a que la información pueda ser recuperada o esté disponible en el momento que se necesite.

Seguridad de la Información. 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.

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).

• **Anti-spam:** Programas capaz de detectar, controlar y eliminar correos spam.

• **Criptografía:** Es el arte de 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.

AMENAZAS TÉCNICAS 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, key loggers, Pornware, etc.

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:

- Sitio oficial – www.sitioReal.com
- Sitio falsos:
    - www.sitioReal.com.sitio.com
    - Variaciones: www.sitioReal-account.com
    - www.sitioReal.actualiza.com

- Jugar con la percepción y la lectura del usuario:
    www.sitiio.Real.com
    www.sitio.Rea1.com
    www.sitio.Real.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:

Aunque en algunos casos, los atacantes adquieren un certificado original para hacer el fraude.

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** Ésta 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.

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

   El peligro radica en que al ser una página falsa, inducen a los usuarios a que ingresen los datos personales, como cuentas 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 usuarios, 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, suplantaciones o robos de dinero, dado que éste atacante posee las claves de acceso a los sistemas y servicios.

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 enlace link enunciado en el correo, ni dando clic a dicho 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).

Ejemplo:

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.

TIP DE SEGURIDAD

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:

1. Mantenga siempre un antivirus actualizado en su(s) 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).
2. 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.
3. Asegúrese que se aplican las actualizaciones en sistemas operativos y navegadores Web de manera regular.
4. 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.
5. 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 click 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.
- Utilice los canales de comunicación adecuados para divulgar la 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.

MECANISMOS DE SEGURIDAD

SERKOI cuenta con sistemas de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, al igual que controles de autenticación para los usuarios (equipos terminales de acceso del cliente).

SERKOI 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, **SERKOI** 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 SERKOI y sus clientes, 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 SERKOI 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 clientes, descongestionando los buzones y el tráfico en la red.

Filtrado de URLs: Los clientes pueden realizar filtrado de URL a través de sus navegadores Web, se sugiere instalar además sistemas parentales. SERKOI cuenta con varios mecanismos capaces de realizar el bloqueo de URLs, entre ellos se encuentran los sistemas DNS y una herramienta para todo el tráfico hacia Internet, el objetivo principal de bloquear las que contengan o promuevan la pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales.

De igual manera, los clientes pueden ejecutar las siguientes acciones como control parental:

- Para el control a través del navegador Chrome, abra las preferencias () y active el “Filtros SafeSearch”
- Para internet Explorer, abra la pestaña de “herramientas” de la parte superior derecha. De clic en “opciones de Internet” -> contenidos -> clic en habilitar.
- Para el navegador Mozilla Firefox, se puede descargar el complemente “BlockSite” y “Anti-Porn Pro”.

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

LIMITACIONES DE ACCESO

Si bien se cuenta con mecanismos de seguridad, filtrado y se hace un control de navegación acorde a los estipulado en la ley (en especial la ley 679 de 2001 y sus decretos reglamentarios), en ningún caso SERKOI restringe, bloquea o hace uso de software o programas que eviten la libre navegación y acceso a Internet (salvo lo estipulado en la ley), por consiguiente, SERKOI no tiene limitaciones en el acceso hacia Internet para sus clientes y usuarios, dando cumplimiento a lo estipulado por el Ministerio de las TIC.