SEGURIDAD EN LA RED

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.

NICE COMUNICACIONES SAS como proveedor del servicio de TELECOMUNICACIONES está convencida de 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 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 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 necesario 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.

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.

¿CÓMO FUNCIONAN?

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:

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.

¿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.

¿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.

¿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).

¿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 l 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:

Certificado SSL

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 portales donde se ingresan datos personales, manténgase actualizado, consultando en la página de la policía nacional www.policia.gov.co, CAI virtual, los últimos eventos, recomendaciones y consultas en línea.

ENFOQUE EN PHISHING, SPAM, VIRUS.

PHISHING:

Definición: El "phishing" es una modalidad de estafa diseñada con la finalidad de robarle al usuario su identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

Como funciona: En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como un banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aún más reales, el estafador suele incluir un vínculo (link) falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el

usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Como Protegerse: Este tipo de fraude debe contenerse a través del ISP y vía usuario.

El usuario debe seguir estas recomendaciones para evitar que sea víctima de robo de su identidad:

Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la entidad que supuestamente le ha enviado el mensaje. Tener especial cuidado en correos que supuestamente han sido enviados por entidades financieras y compras por Internet, como eBay, PayPal, bancos, etc. Solicitando actualizar datos de cuentas y/o accesos, ya que ninguna de estas entidades solicita este tipo de información por este medio.

Asegúrese que su PC cuente con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes (Microsoft, Mac, etc...)

Para visitar sitios Web, introduzca directamente la dirección URL en la barra de direcciones.

Asegúrese de que el sitio Web utiliza cifrado.

Si tiene instalado servidores Web, asegúrese que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes. Muchas veces los phishers buscan en la red servidores Web vulnerables que puedan ser utilizados para montar páginas que intentan suplantar la identidad de una entidad financiera, sin que el usuario se de cuenta. Para el cliente, esto tiene como repercusión la afectación directa en su servicio de Internet, ya que la IP donde se encuentra alojada la página fraude es reportada por entidades internacionales pidiendo al ISP (Telmex Hogar) el bloqueo de la misma.

Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

A nivel del ISP, actualmente NICE COMUNICACIONES SAS implementa filtros anti-spam que ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con el phishing recibidos por el usuario.

SPAM

Definición:

Se llama spam, correo basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera a los usuarios que reciben este correo. Aunque su difusión se puede hacerse por distintas ví s, lo mas común es hacerlo vía correo electrónico.

Actualmente NICE COMUNICACIONES SAS cuenta con una plataforma que protege a los usuarios de este tipo de correos

Normas básicas para evitar y reducir al mínimo el spam

El spam es un problema que debe ser controlado desde diferentes frentes, tanto a nivel de usuarios como a nivel de los proveedores de Internet.

A nivel de usuario, se pueden seguir estas recomendaciones para evitar ser inundado por correo spam:

Si no se reconoce un remitente de un correo, no abrir los archivos adjuntos del mensaje, incluso si usted tiene un software bloqueador de spam y/o filtro de aplicación ejecutándose en su PC. Los archivos adjuntos a menudo incluyen software o aplicaciones malintencionadas que pueden tener efectos muy negativos sobre su PC, desde borrar su información mas valiosa hasta capturar contraseñas, números de tarjetas de crédito, etc... sin que el usuario ni siquiera se entere. Estas aplicaciones no se pueden incluir en un mensaje de correo electrónico en texto plano, la cual es la razón por la que se empaquetan en los archivos adjuntos.

Si recibe un correo spam, nunca haga clic en el vínculo “Quitar spam”, ya que lo que buscan los spammers es que el cliente verifique que esta dirección de correo está activa, añadiendo posiblemente su cuenta de correo a más y más listas de spam, lo cual ocasionará que usted reciba mayor cantidad de correo no deseado.

Algunos programas que utilizan los spammers tratan de adivinar las cuentas de correo a las cuales enviar correo no deseado, por lo cual es recomendable utilizar cuentas que contengas números y letras para que no sean fácilmente ubicadas.

Nunca dar click sobre enlaces (links) que se encuentren dentro de un mensaje de correo electrónico de un remitente desconocido. Probablemente pueda ser un caso de phishing para tratar de robar la identidad del usuario o puede activar un programa que silenciosamente descargue aplicaciones en su PC.

En caso de que usted conozca al remitente, igual la recomendación es no dar click sobre enlaces (links) que se encuentren dentro del mensaje. Uno nunca puede estar seguro de que quien envía el mensaje es realmente quien dice ser, ya que los spammers pueden cambiar la cuenta remitente, suplantando la identidad de otra persona.

Para acceder a un enlace (link) dentro del mensaje, se recomienda cerrar el mensaje, y visitar el sitio en cuestión, introduciendo manualmente la URL (por ejemplo, www.google.com) en su navegador de Internet. Es la única manera de estar seguro que la página a la cual se está accediendo es la real.

Para tratar de evitar que su cuenta sea ingresada en listas de correo utilizadas por los spammers, se recomienda que el usuario preste cuidado a los sitios donde ingresa y que le solicita registrarse (mediante una cuenta de correo), ya que existen muchos sitios Web inescrupulosos que venden estas cuentas registradas a redes de spammers.

Si tiene instalado servidores de correo, asegúrese que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes. En muchos casos, los servidores de correo, debido a configuraciones deficientes, permiten que cualquier persona, desde Internet, utilice estos servidores para enviar correos (conocido como Open Relay), afectando el servicio de correo del cliente y muy posiblemente será bloqueado en listas negras de Spam mantenidas a nivel mundial.

En caso que ud como cliente tenga problemas en el envío de correos, para verificar que su IP no se encuentra reportada en listas negras de spam, puede revisar los siguientes enlaces para realizar la consulta:

https://mxtoolbox.com/blacklists.aspx

En caso que su IP se encuentre reportada acceder al siguiente enlace para tramitar el desbloqueo:
https://check.spamhaus.org/

Para que pueda ser efectivo este desbloqueo, el cliente deberá tomar las medidas correspondientes para evitar que se continúe enviando correo spam.

Hay que tener en cuenta que el tiempo de desbloqueo depende del sitio en el cual ha sido reportado una IP. Entre los sitios más frecuentes, están:

www.aol.com: Tiempo de desbloqueo aprox. 48 horas
www.lashback.com: Tiempo de desbloqueo aprox. 1 hora
www.uceprotect.net: Tiempo de desbloqueo aprox. 7 días
www.spamcop.net: Tiempo de desbloqueo aprox. 24 horas
www.dsbl.org: Tiempo de desbloqueo aprox. 7 días
WWW.WPBL.INFO: Tiempo de desbloqueo aprox. 1 hora
WWW.MOENSTED.DK: Tiempo de desbloqueo aprox. 1 hora
www.comcast.com: Tiempo de desbloqueo aprox. 48 horas
www.abuso.cantv.net: Tiempo de desbloqueo aprox.48 horas
www.spamhaus.org: Tiempo de desbloqueo aprox. 24 horas

VIRUS

Definición: Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del PC, sin el permiso o el conocimiento del usuario. Los virus pueden destruir, de manera intencionada, los datos almacenados en un PC aunque también existen otros más "benignos", que solo se caracterizan por ser molestos

Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Como Protegerse:

Similar al spam, los virus son un problema que debe ser controlado desde diferentes frentes, tanto a nivel de usuarios como a nivel de los proveedores de Internet.

A nivel de usuario, se pueden seguir estas recomendaciones para evitar ser víctima de los efectos de un virus informático:

Si no se reconoce un remitente de un correo, no abrir los archivos adjuntos del mensaje, incluso si usted tiene un software antivirus y/o filtro de aplicación ejecutándose en su PC. Los archivos adjuntos a menudo incluyen software o aplicaciones malintencionadas que pueden tener efectos muy negativos sobre su PC. Evite caer en técnicas conocidas como de Ingeniería social en la cual llega un correo electrónico con un mensaje del estilo “ejecute este programa y gane un premio”.

Evitar la instalación de software pirata o de baja calidad, mediante la utilización de redes P2P, ya que muchas veces, existen ciertos sitios que “prometen” la descarga de un aplicativo en particular pero en realidad lo que el usuario descarga es un virus.

Asegurarse que su equipo PC cuente con las últimas actualizaciones a nivel de seguridad tanto a nivel de sistema operativo como de los aplicativos instalados, dadas por el fabricante. Existen algunos tipos de virus que se propagan sin la intervención de los clientes y que aprovechan debilidades de seguridad de los diferentes sistemas y aplicaciones, como por ejemplo los virus Blaster y Sasser.

Instalar software antivirus en el PC, el cual esté actualizado con las últimas firmas dadas por el fabricante respectivo.

A nivel de ISP, **NICE COMUNICACIONES SAS** cuenta actualmente con equipos especializados en la detección y filtrado de correos con virus, mediante filtros de tipo heurístico, firmas de virus reconocidos y adicional cuenta con filtros de tipo preventivo, que aunque a nivel público no se halla liberado una firma para contener una nueva amenaza, el sistema coloca en cuarentena este tipo de tráfico, hasta determinar si el tráfico es legal o hasta que se tenga la firma correspondiente a la propagación del

nuevo virus o gusano. Todos los correos que los usuarios reciben y envían son filtrados por esta herramienta.

INTERNET SANO

La Internet, el invento más significativo del final del siglo XX ha representado un avance gigantesco para el intercambio de información alrededor del mundo. Si bien la Red Mundial de Información ha sido aprovechada con beneficio por la mayor parte de la humanidad, hay delincuentes que la utilizan para realizar sus actividades delictivas, entre ellas uno de los crímenes más repugnantes, la explotación sexual infantil.

INTERNET SANO es una estrategia nacional que se ubica en el marco de la Ley 679 del 3 de agosto de 2001 expedida por el Congreso de la República y el decreto 1524 del 24 de julio de 2004 con el fin de prevenir y contrarrestar la pornografía, la explotación sexual y el turismo sexual con menores.

La estrategia invita a la ciudadanía a participar activamente de la prevención de la explotación sexual con menores de edad en Internet, a denunciar, a mantener una comunicación de los padres, adultos responsables y maestros con los menores enfatizando en la importancia de poder navegar seguros y gozar así de un INTERNET SANO. Generar opinión y conocimiento en los públicos objetivo en torno al tema de la explotación infantil en Internet, destacando mensajes de prevención, de denuncia, informativos e institucionales.

El nombre INTERNET SANO, busca identificar la campaña de medios y crear un icono que pueda ser utilizado por los I.S.P. (Internet Sevice Provider) en sus distintas páginas con base o temática colombiana, es un nombre que significa que las instituciones del Estado Colombiano están activas y pendientes para evitar la pornografía infantil.

Ministerio de Comunicaciones
Teléfono: 01800 09 12667
Internet sano es la campaña del Ministerio de Comunicaciones para que todos los colombianos comprendamos el significado de la prevención de la pornografía infantil y juvenil en Internet.
Página Web: www.mintic.gov.co

Otras entidades para hacer su denuncia: Dirección Central de Policía Judicial – DIJIN

Policía Nacional de Colombia

Carrera 59 26-21 CAN, Bogotá - Colombia
Lunes a viernes de 08:00 a.m – 12:00 p.m y

02:00 p.m – 05:00 p.m
Conmutador o PBX: +57 6015159000

Link de Denuncia
https://adenunciar.policia.gov.co/Adenunciar/Login.aspx?ReturnUrl=%2fadenunciar%2ffrm_denuncia_pi.aspx

Fiscalía General de la Nación
Teléfono: 01800 09 12280
e-mail: contacto@fiscalia.gov.co
Pagina Web: www.fiscalia.gov.co

Instituto Colombiano de Bienestar Familiar
Teléfonos Bogotá: 01-8000-91-8080 – PBX: 4377630
Pagina Web: www.icbf.gov.co

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: 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 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

NICE COMUNICACIONES SAS cuenta con sistema 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). NICE COMUNICACIONES 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, NICE COMUNICACIONES 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 primer protección perimetral en las redes de NICE COMUNICACIONES SAS 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 NICE COMUNICACIONES 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 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. NICE COMUNICACIONES SAS 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.

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.

Fuentes.

Conceptos Básicos de Seguridad Informática.
http://www.bradanovic.cl/pcasual/ayuda3.html

Amenazas Técnicas Informáticas. http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas- comunes-disi2010/

Phishing, Spam, Virus.
http://www.claro.com.co/wps/wcm/connect/co/claro2013.colombia/pc/personas/legal-y- regulatorio/lightbox-fijo/phishing

Seguridad en la Web. http://www.mediacommerce.net.co/seguridad-en-la-web/