# Protocolo De Seguridad Web

## INTRODUCCIÓN.

Dado que la inseguridad se da en muchas maneras en nuestro entorno social, en las redes no es la excepción. Las empresas y hogares, buscan tener la mayor seguridad en sus esquemas, para no tener pérdidas en su economía, de su privacidad y de su confidencialidad, es por eso que este protocolo le permitirá tomar medidas preventivas para combatir actos ilícitos, ya sea de herramientas de seguridad para los sistemas operativos y también, dar capacitación al personal, que es fundamental para tener una buena seguridad.

## NORMATIVIDAD QUE APLICA.

RESOLUCIÓN No. 3067 DE 2011: “Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones”

**ARTÍCULO 2.3. SEGURIDAD DE LA RED.** Los proveedores de redes y servicios de telecomunicaciones que ofrezcan acceso a Internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo. Para tal efecto, deberán informar en su página Web sobre las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtros antivirus y la prevención de spam, phishing, malware entre otras. La responsabilidad a cargo de los proveedores de redes y servicios de telecomunicaciones que ofrezcan acceso a Internet no cubre los equipos del cliente, dado que los mismos son controlados directamente por el usuario del servicio. Los proveedores de contenidos o de cualquier tipo de aplicación deberán tomar las respectivas medidas de seguridad de conformidad con lo que para el efecto disponga la normatividad que les sea aplicable.

## GLOSARIO.

**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.

**Firewall:** Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

**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.

**Ingeniería social:** Arte de sacar información a alguien sin que la persona que está siendo "atacada" se dé cuenta. Este sería el resumen corto, y en un sentido más amplio se utiliza también para inducir al usuario a realizar acciones que o bien le pondrán en una posición de baja seguridad o bien nos ayudará a crear una situación en la que nosotros como atacantes estamos en posición ventajosa para lograr el objetivo que estamos persiguiendo.

**Internet:** La internetwork de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la llamó Internet DARPA, y no debe confundirse con el término general internet.

**Phishing:** 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.

**MAC:** Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.

**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 vías, lo más común es hacerlo vía correo electrónico.

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

**MECANISMO DE SEGURIDAD.**

**MUROS DE FUEGO (FIREWALLS).**

Básicamente un firewall es una computadora que se encarga de filtrar el tráfico de información entre dos redes.

El problema no es el controlar a los usuarios de un sistema sino el prevenir accesos no autorizados de hackers que pudieran atacar la seguridad.

La ventaja de construir un firewall entre una red confiable y una insegura, es la de reducir el campo de riesgo ante un posible ataque. Un sistema que no cuente con este tipo de protección es propenso a sufrir un acceso no autorizado en cualquier nodo que compone la red confiable. En el momento de proteger el sistema con un firewall, el peligro se reduce a un solo equipo.

La mejor manera de proteger una red interna es vigilando y con un firewall bien diseñado obtenemos esta ventaja. Este medio nos puede proveer información de los paquetes de datos que entran a la red, los que son rechazados, el número de veces que tratan de entrar, cuantas veces un usuario no autorizado ha querido penetrar en la red, etc. Con esta información se puede actualizar el sistema de seguridad y prevenir una posible violación al mismo.

Un firewall debe proveer los fundamentos de seguridad para un sistema, pero no es lo único que necesitamos para proteger la red ya que no está exento de ser pasado por un hacker. Esencialmente se instala entre la red interna y la Internet. El firewall previene el acceso del resto del mundo al sistema y sobre todo a la información que circula por la Intranet12. Un firewall combina hardware y software para proteger la red de accesos no autorizados.

**Anti-virus.**

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, siendo los más utilizado:

a) Avast: https://www.avast.com

b) Avira 2016: https://www.avira.com

c) ESET: https://www.eset.com

d) Kaspersky: http://latam.kaspersky.com

e) 360 total security: https://www.360totalsecurity.com

**Contrarrestar 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.

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 más 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.

**Como Protegerse del phishing.**

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.

Para visitar sitios Web, introduzca directamente la dirección URLen 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 dé 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 entes reguladores pidiendo al ISPel bloqueo de la misma.

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

**CRIPTOGRAFÍA.**

Este es un medio para proveer seguridad a las transmisiones de datos. En Internet, la información viaja por la red en forma de paquetes bajo el protocolo TCP/IP y algunos hackers pudieran interceptarlos, esto es un peligro potencial de manera individual y organizacional. Cuando se obtiene acceso a estos paquetes, la comunicación entre dos nodos es insegura porque existe una persona que puede recibir al mismo tiempo información confidencial.

Una manera de protección es la criptografía ya que el mensaje es codificado por medio de un algoritmo y sólo puede ser leído o decodificado con el mismo algoritmo en el nodo receptor. En otras palabras, el mensaje es oculto dentro de otro mensaje haciéndolo imposible de leer para todos excepto para el receptor. Al algoritmo de encriptación se le conoce como llave secreta o pública según sea el caso.

**Filtrado de URLS:**

ESG COMUNICACIONES S.A.S. realiza el filtrado MAC, si el cliente desea este servicio toma su nombre de la dirección MAC, siglas en inglés de Media Access Control, de las tarjetas de red de los distintos dispositivos que están preparados para conectarse a una red, como puede ser un ordenador, una tablet o un smartphone. Cada dispositivo tiene una dirección MAC única que identifica a su tarjeta de red -si hablamos de un equipo con varias tarjetas de red tendrá varias direcciones MAC-. Sería algo similar a nuestro carnet de identidad.

El filtrado MAC utiliza una lista de direcciones MAC que nosotros introduciremos, es decir, una lista de dispositivos. Tomando en cuenta esta lista, hay dos modos en los que se puede configurar:

a) Permitiendo la conexión a los dispositivos añadidos a la lista de direcciones MAC, quedando cualquier otro sin posibilidad de conectarse a nuestra red. Esto es bastante útil cuando queremos que solo unos determinados dispositivos puedan conectarse a nuestro Wifi, pero presenta el inconveniente de que si recibimos invitados no podrán hacer uso de nuestra red.

b) Denegando la conexión a los dispositivos que aparecen en la lista de direcciones MAC, circunstancia en la que cualquier otro dispositivo podrá conectarse. Esta forma sería adecuada para no permitir la conexión a un determinado dispositivo del que conozcamos la dirección MAC, por ejemplo, el teléfono móvil de nuestro hijo o el equipo del vecino que se conecta a nuestra red sin permiso.

También los clientes pueden realizar filtrado de URLa través de sus navegadores Web.

**MUY BUENAPRIVACIDAD (PGP).**

PGP (Pretty Good Privacy) es un sistema de protección de E-mail y de archivos de datos, que proporciona una comunicación segura a través de canales inseguros. Fue desarrollado a principios de los 90's, por Phill Zimmermann, con el fin de otorgar confidencialidad y autentificación. Es decir, sólo aquellos que deben recibir un mensaje pueden leerlo y el origen de un mensaje es comprobable. Permite una administración de llaves además de la compresión de datos. Es usado en las firmas digitales.

**RECOMENDACIONES.**

A continuación, le entregamos algunas recomendaciones y obligaciones que nuestros suscriptores deben cumplir para apoyar las acciones que realizamos y fortalecer su seguridad.

- Utilizar claves seguras: usar símbolos, números, una mezcla de letras minúsculas, mayúsculas, números y caracteres especiales.
- No dejar los usuarios y claves por defecto en las diferentes cuentas de correo electrónico u ordenadores.
- Rotar claves periódicamente.
- Rotar claves periódicamente.
- 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 la ley 1336 de 2009.

- 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.
- Si sus programas o el trabajo que realiza en su computador no requieren de popup, 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.
- 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.
- Usar Claves de Acceso que no estén asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares, etc.
- Las carpetas compartidas, dentro de una Red, deben tener una Clave de Acceso, la misma que deberá ser cambiada periódicamente.
- Verificar cualquier software que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.
- Tomar precauciones con los contenidos de applets de Java, JavaScripts y Controles ActiveX, durante la navegación, así como los Certificados de Seguridad. Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos.
- De ninguna manera se debe ejecutar ningún archivo con doble extensión.
- No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos, tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, etc.
- Si el servidor no reconoce su nombre y clave de acceso o servicio de correo, podría ser que ya esté siendo utilizado por un intruso. Amenos que haya un error en la configuración, la cual deberá ser verificada.
- Borre constantemente los cookies, archivos temporales e historial, en la opción Herramientas, Opciones de Internet, de su navegador.