Servicio de Internet
Seguridad en la red

Genesis Data ha dispuesto para la protección de los elementos informáticos de sus usuarios, herramientas de hardware que permiten controlar hasta cierto punto las amenazas informáticas mas relevantes entre las que encontramos phishing, spoofing, spam, malware y ataques de denegación de servicios. Esta protección se realiza a través de **la solución centralizada basada en hardware (Appliance) Fortigate, la cual se encuentra instalada e implementada en nuestro Centro Nacional de Monitoreo (NOC), sitio desde el cual se efectúa el control total y monitoreo de los servicios objeto de la prestación del servicio**. A través de esta solución se han configurado políticas de seguridad que permiten efectuar claramente el filtrado antispam y filtrado de URL´s , para de esta forma controlar el tráfico de salida y entrada dependiendo de los puertos.

Sin embargo como proveedor de servicio Genesis Data está en la obligación de recomendar a sus usuarios la autoprotección contra amenazas como:

PHISHING

Este delito informático busca robarle al usuario su identidad para suplantarlo con transacciones con tarjeta de crédito, cuentas personales, contraseñas y otros engaños.
El delincuente informático envía mensajes, correos electrónicos, links de páginas, todos ellos falsos con la intensión de suplantar entidades financieras o de confianza para el usuario y le solicita información relevante como lo son contraseñas, números de cuentas y otros datos personales.
Algunas recomendaciones para que los usuarios puedan protegerse ante este delito informático:

- Ingrese a los sitios web de entidades financieras digitando la dirección desde su navegador y no ingresando desde links que encuentre en los correos electrónicos.
- Cuando necesite ingresar sitios web en los cuales maneje información sensible como la mencionada anteriormente, utilice el modo seguro del protocolo HTTP. Esto se logra simplemente digitando en el navegador web https:// antes de digitar la dirección web a la que se quiere ingresar.
- Mantenga el antivirus, firewall y cualquier otro tipo de software de seguridad de su computador actualizado.
- No responda a solicitudes de información personal enviadas a su correo electrónico, por el contrario, establezca comunicación directa con la entidad que le solicita la información y tenga en cuenta que entidades bancarias y paginas reconocidas de compras online no realizan ningún tipo de actualización de datos a través de este medio.
- Evite enviar correos cadena a otros remitentes.
- Verifique que los sitios web que manejan su información sensible posean el certificado digital vigente, esta verificación la puede realizar ubicando el icono de seguridad (o), en alguna de las esquinas del espacio donde digita la dirección web del navegador y no en la página web como tal.

www.genesisdata.com.co
Calle 43 No. 29 - 13 Piso 7 Edificio Tempo II
PBX: (097) 657 07 77 Fax: (097) 657 35 72
Bucaramanga, Colombia

SPAM

Se considera spam aquellos correos electrónicos publicitarios, cadenas, pornográficos o aquellos que su contenido no tiene ninguna utilidad laboral. Además estos correos no son solicitados por el destinatario, por lo general son enviados de forma masiva y pueden perjudicar de alguna manera a los destinatarios, por ello estos correos son considerados basura.

Algunas recomendaciones para que los usuarios eviten ser inundados de spam:

- No abra ningún correo electrónico del cual no conozca el remitente y mucho menos abra los archivos adjuntos que este tipo de correo pueda tener, debido a que estos archivos pueden contener software malicioso para su computador.
- Mantenga activo los filtros de spam en su correo electrónico e indique manualmente que correos considera spam.
- No utilice los links que se encuentran en correos electrónicos cuyo remitente no conozca, debido a que este puede ser ataque phishing.
- Evite hacer pública su dirección de correo electrónico, con esto a su vez evita que su dirección de correo electrónico sea agregada a la lista de las personas que envían spam.
- Evite hacer pública la dirección de correo electrónico de sus contactos agregándolos a la casilla de "Con copia oculta" o "CCO" cuando requiera enviar un correo masivo.
- No responda, ni reenvíe este tipo de correo, por el contrario elimínelo de su bandeja de entrada.

MALWARE

Este concepto corresponde a todo tipo de código o software que se introduce en un sistema intencionalmente con un fin malicioso o no autorizado aprovechándose de las vulnerabilidades del sistema y está diseñado para que impacte en la infraestructura o en el usuario.
Algunos ejemplos de malware son: Virus, Adware, Spyware, Cookies, Dialers, Exploit, Troyanos, Keyloggers, entre otros.

VIRUS INFORMATICO

Es un Malware o código malicioso que se instala dentro del código de otros programas cuando se introduce en un sistema sin el consentimiento o conocimiento del usuario, con el fin de alterar su funcionamiento, modificar o generar daños irreparables en el sistema y propagarse.

Los principales medios de infección de los virus informáticos son:

- Redes sociales
- Archivos adjuntos de correos Spam
- Dispositivos USB, CDs, DVDs infectados
- Uso de aplicaciones P2P
- Sitios web infectados o fraudulentos

www.genesisdata.com.co
Calle 43 No. 29 - 13 Piso 7 Edificio Tempo II
PBX: (097) 657 07 77 Fax: (097) 657 35 72
Bucaramanga, Colombia

Algunas recomendaciones para que los usuarios se puedan proteger de los virus informáticos:

- Mantenga el antivirus, firewall y cualquier otro tipo de software de seguridad de su computador actualizado.
- Además mantener su antivirus actualizado, realice un escaneo general de su equipo periódicamente.
- Antes de ejecutar fichero o de abrir un archivo que ha descargado a su computador primero analícelo con su antivirus.
- No abra ni descargue los archivos adjuntos de los correos electrónicos de remitentes no conocidos, tampoco lo haga si conoce el remitente pero el contenido del correo no tiene relación con la persona que lo envía.
- Evite descargar software de sitios web que no sean directamente del autor.

Adicional se cuenta para la prestación del servicio con una solución basada en Hardware llamada FortiAnalyzer, la cual opera de forma centralizada y a través de la cual permite generar los reportes de aplicación de todas las políticas y elementos de seguridad que se encuentran dispuestos para la prestación del servicio. Dentro de los elementos relevantes presentados se destacan sin limitar a ello los siguientes:

a. Bandwidth and Applications (Ancho de Banda y Aplicaciones)
b. Top Applications by Bandwidth (Top de Aplicaciones por Ancho de Banda)
c. Application Usage By Category (Uso de Aplicaciones por Categorías)
d. Key Applications Crossing The Network (Principales Aplicaciones que se usan en la Red)

www.genesisdata.com.co
Calle 43 No. 29 - 13 Piso 7 Edificio Tempo II
PBX: (097) 657 07 77 Fax: (097) 657 35 72
Bucaramanga, Colombia