Genesis Data SAS.

Sistemas Internos de Seguridad

Objeto:

Este documento describe y detalla los sistemas de seguridad internos en la red, asi como las recomendaciones a los usuarios en esta materia.

CONTENIDO

www.genesisdata.com.co
Calle 43 No. 29 – 13 Edificio Tempo II Piso 7
PBX: (097) 657 07 77
Bucaramanga, COLOMBIA

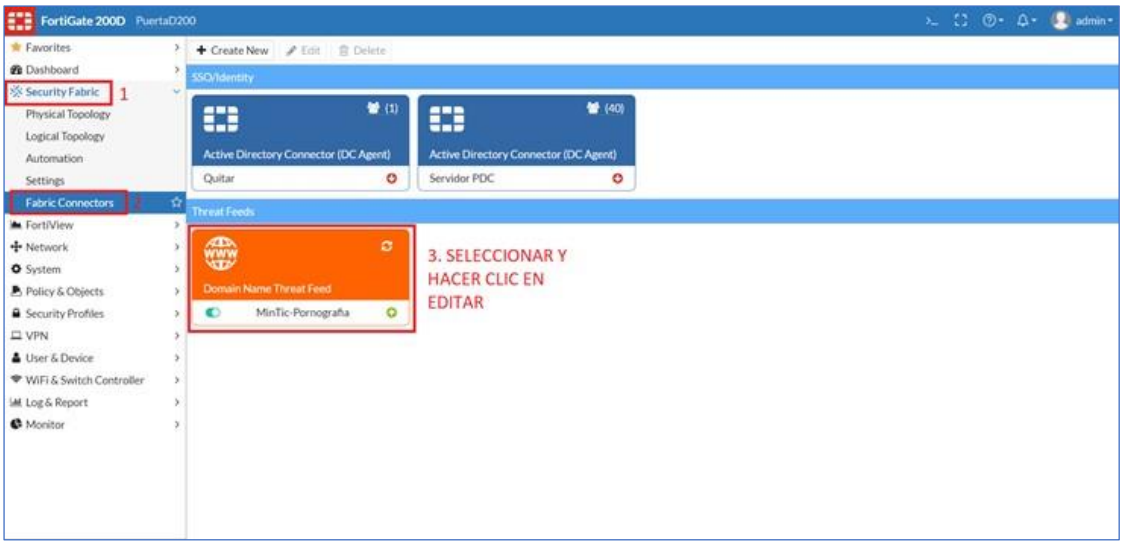
SISTEMAS INTERNOS DE SEGURIDAD EN LA RED

GENESIS DATA ha dispuesto para la protección de los elementos informáticos de sus usuarios, herramientas de hardware (firewalls, filtros antivirus, prevención de spam, phishing, malware entre otras) que permiten controlar hasta cierto punto las amenazas informáticas. 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.

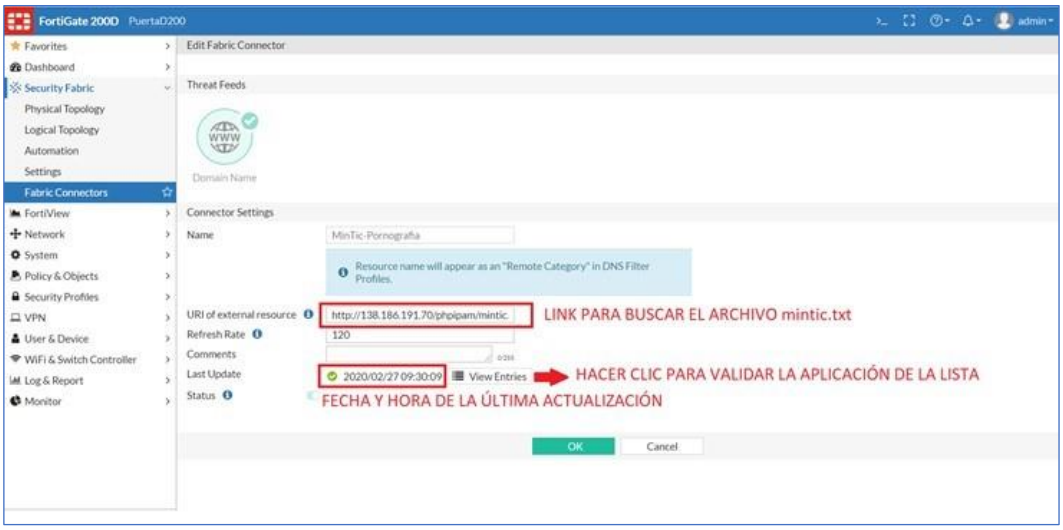
En concordancia a lo anteriormente expresado, y específicamente respecto al principio de Integridad de datos, **GENESIS DATA** cuenta con mecanismos de protección del CORE de la Red, como son: Firewalls y filtrado perimetral, evitando asi el riesgo de accesos no autorizado a la información transmitida por la infraestructura de telecomunicaciones.

GENESIS DATA acoge las disposiciones legales emanadas del MINTIC y por lo tanto realiza el filtrado de páginas de pornografía infantil de acuerdo con los listados publicados por esta entidad. Esto se realiza mediante la implementacion en los appliances de seguridad como puede observarse en la siguiente lamina.

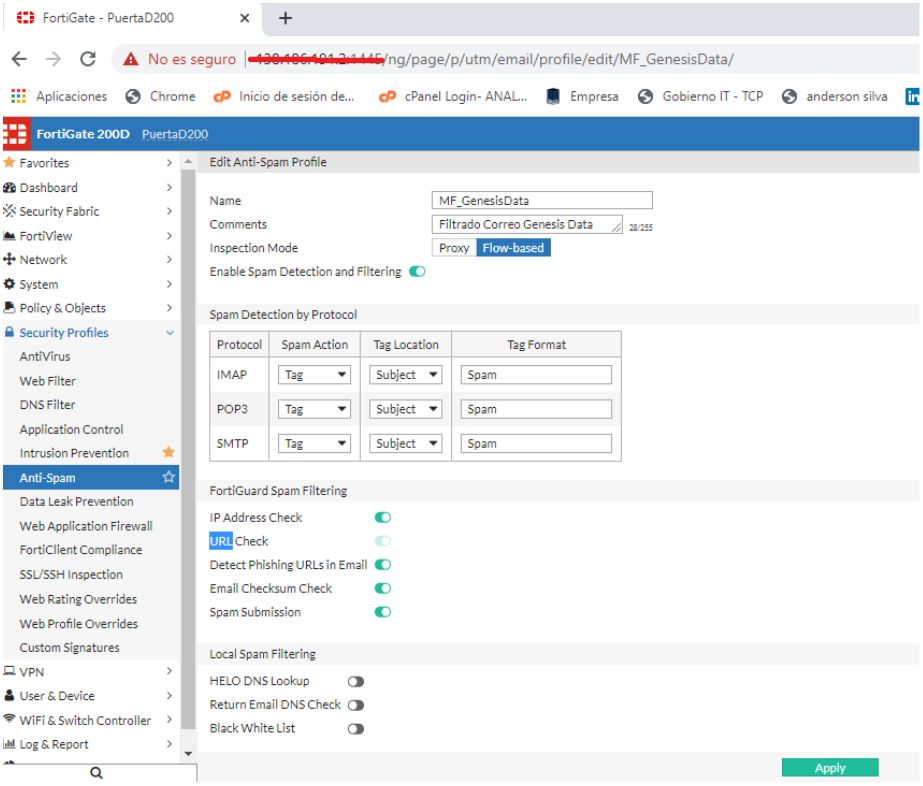
GENESIS DATA mantiene un fuerte compromiso y alta responsabilidad con la seguridad de la población infantil y la protección de los usuarios de la red.



www.genesisdata.com.co
Calle 43 No. 29 – 13 Edificio Tempo II Piso 7
PBX: (097) 657 07 77
Bucaramanga, COLOMBIA



De otra parte, La plataforma de seguridad implementada permite la protección del acceso no autorizado y control de intrusos en la red, permite el establecimiento de políticas de acceso, hacia los diferentes servidores y aplicaciones y servicios de los usuarios. Mediante mensajes de alerta de esta plataforma, permite monitorear procesos de intrusión a las redes internas, aplicaciones o servicios protegidos por el Firewall. A continuación se muestra evidencias de los controles antispam implementados en los appliance de seguridad: **Política de Control de ANTISPAM**



www.genesisdata.com.co
Calle 43 No. 29 – 13 Edificio Tempo II Piso 7
PBX: (097) 657 07 77
Bucaramanga, COLOMBIA

Internet se ha convertido en un servicio masivo y de uso cotidiano, por esta razón esta tecnología trae consigo riesgos que pueden afectar la seguridad y privacidad, es así que **GENESIS DATA**, se permite poner en conocimiento a sus usuarios sobre estos riesgos y sugiere algunas recomendaciones como medidas preventivas; Dentro de los riesgos más comunes se pude referir a: Phishing, spoofing, spam, malware y ataques de denegación de servicios.

RIESGOS RELATIVOS AL SERVICIO DE INTERNET

GENESIS DATA, consiente de los riesgos latentes en internet se permite allegar algunas recomendaciones y sugerencias a los usuarios que pueden contribuir y apoyar en los procesos de concienciación y formación en estas temáticas.

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.

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.

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

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.

GROOMING

Práctica de acoso y abuso sexual en contra de niños y jóvenes que, en la mayoría de los casos, sucede a través de las redes sociales.

RECOMENDACIÓN AL USUARIO FINAL DEL SERVICIO DE INTERNET

- Instalar herramientas antivirus.
- En uso de servicios financieros, utilizar siempre el mismo dispositivo (equipo de cómputo), preferiblemente cableado al modem, es decir sin conexión wifi
- Evitar utilizar redes públicas para operaciones financieras.
- Utilice contraseñas seguras en los portales, con combinaciones de letras, números y caracteres alfanuméricos. Su longitud debe ser de mínimo ocho caracteres.
- Cerrar siempre la sesión cuando se haya autenticado con usuario y contraseña en los portales donde haya navegado
- Así evita robo de información personal.
- Evite publicar información personal en redes sociales.
- No abrir los correos o noticias falsas o de dudosa procedencia.

CONTROL PARENTAL

El control parental es una característica especialmente útil para padres y responsables educativos que desean impedir que niños o adolescentes puedan acceder a páginas Web inapropiadas. Permitir o bloquear programas específicos puede impedir que los niños ejecuten determinados programas.

En los siguientes enlaces, puede ver un tutorial de cómo habilitar el servicio de control parental:
https://www.youtube.com/watch?v=iYFTaKN9Rmk
https://www.youtube.com/watch?v=N-0W7DTSSps

www.genesisdata.com.co
Calle 43 No. 29 – 13 Edificio Tempo II Piso 7
PBX: (097) 657 07 77
Bucaramanga, COLOMBIA