Protección al usuario

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).

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.

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 envíe información de claves a través del correo u otro medio que no esté encriptado

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 clic 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 reenvíe 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.

MECANISMOS DE SEGURIDAD

Hughesnet 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).

Hughesnet 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.

Hughesnet 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 este elemento de red se hace la primera protección perimetral en las redes de 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 Hughesnet son protegidos a través de sistemas anti-códigos maliciosos.

Control parental

Característica especialmente útil para padres y responsables educativos que desean impedir que niños o adolescentes puedan acceder a páginas Web inapropiadas. Se sugiere instalar además sistemas adicionales de control parental.

Filtrado de URLs

Hughesnet para el bloqueo de sitios con contenido de pornografía infantil, utiliza Servidores para realizar el filtrado de estos sitios. El objetivo principal de este filtrado es denegar el acceso a los sitios que contengan o promuevan la pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales. Se sugiere instalar además sistemas parentales.

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.

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.

HERRAMIENTAS RECOMENDADAS

- control parental Google®, ESET Parental Control, KidLogger
- antivirus Avast, Panda
- antispam Avast antispam

MODELOS DE SEGURIDAD HUGHESNET

En el modelo de seguridad HUGHESNET se establecen lineamientos para la implementación de mecanismos, compatibles con las recomendaciones X.800 de la UIT, en lo relacionado con autenticación, acceso, no repudio, confidencialidad de datos, integridad de datos y disponibilidad.

Autenticación

En la actualidad Hughesnet protege la información de identidad de sus clientes mediante un esquema de seguridad segmentada por redes en los beams de transporte hacia los gateway, así como con el aseguramiento y actualización de software, controles de acceso físico y lógico por medio de usuarios y contraseñas, mecanismos de contingencia y recuperación, entre otros.

Acceso

Para los Servicios de Internet Hughesnet implementa mecanismos de control de acceso con protocolos y configuraciones de enrutamientos que permiten identificar y autenticar la conexión de los usuarios previa validación de su cuenta y contraseña de conexión, asegurando que solo quienes tienen derecho al servicio podrán utilizarlo.

No repudio

Las mismas ventajas del control de acceso de los usuarios que se realiza mediante los protocolos de Autenticación, Autorización y cuentas de usuario SAN son trasladados al servicio de NO REPUDIO, gracias a los mecanismos de SAN “Subcriber User Number” por sus siglas en inglés. Con esta funcionalidad, las conexiones y desconexiones de nuestros usuarios son registradas que permiten validar la evidencia de la identidad del usuario que hace uso del servicio.

Los logs generados por las plataformas de seguridad -como firewall son analizados con el fin de determinar el origen y tipo de amenazas comunes, de tal forma que puedan implementarse rápidamente los mecanismos de mitigación necesario.

Confidencialidad

Hughesnet posee múltiples controles para asegurar que la información de nuestros clientes no será accedida o divulgada a entidades, individuos o procesos no autorizados. De esta forma los datos de los clientes son cuidadosamente custodiados, implementando múltiples zonas de seguridad sobre los elementos de TI en donde esta información reside. Dichos controles inician en dispositivos de seguridad perimetral como Firewalls, y dispositivos de almacenamiento controlado por personal de IT en cada uno de los datacenter de los Gateway con redundancia 1+1.

Integridad

Hughesnet garantiza la no modificación, indebida o errónea de la información de los clientes que es transportada. En caso de que los datos sean recibidos con errores en distintos puntos de enrutamiento, los dispositivos y protocolos de red se encargan de solicitar las correcciones y retransmisiones requeridas para completar la recepción de los datos transmitidos, garantizando así la Integridad de la información.

Disponibilidad

Los servicios se apoyan en una estructura de red redundante 1+1 de interconexión en los Gateway a través de redes de fibra óptica para el transporte los datos de los clientes, una vez recibidos en el backbone transporte, así como sobre los múltiples puntos de conexión internacional a Internet distribuidos en todo Estados Unidos donde se garantiza la dispersión geográfica.