- **PRÁCTICAS DE GESTIÓN DEL TRÁFICO**

Las siguientes son las prácticas que La UT Andired utiliza para ofrecer gestión de tráfico al usuario en cuanto a transparencia y seguridad:

- **SEGURIDAD Y GESTIÓN DE TRÁFICO**

Función de bloqueo de páginas web, asociadas a pornografía infantil y aquellas indicadas por el ICBF.

El control de seguridad en los dispositivos de los usuarios finales (Smart Phone, PC, laptop, etc) es responsabilidad del usuario

- **AUTENTICACIÓN Y ACCESO**

La responsabilidad del uso de internet o los dispositivos que se conecten mediante el dispositivo de acceso (TPLINK) residencial es directamente del usuario sin embargo la UT Andired provee soporte para cambio en el acceso y la autenticación en el dispositivo teniendo en cuenta que es propiedad de la UT Andired.

La UT Andired no provee autenticación de aplicaciones de terceros.

- **SERVICIO DE INTEGRIDAD DE DATOS**

El tráfico de datos y voz del usuario está cifrado en la capa de acceso para proteger la información.

- **PRÁCTICAS DE GESTIÓN DE TRÁFICO**

La UT Andired implementa una gestión de tráfico, que garantiza la NO discriminación respecto de algún proveedor, servicio, contenido o protocolo específico. Por otra parte, La UT Andired tiene implementados procedimientos de detección y mitigación de los efectos de la congestión sobre la red; así como mecanismos que buscan garantizar la seguridad e integridad de la red mediante un Firewall que se encuentra dispuesto en nuestro Datacenter además de garantizar el aseguramiento de la calidad del servicio.

- **RECOMENDACIONES DE USO CLIENTE EXTERNO E INTERNO**

Recomendaciones para evitar ataques Pishing

1. Confirmar el emisor del mensaje. La mayoría de ataques de 'phishing' proviene de personas desconocidas. Antes de abrir cualquier mensaje, el usuario debe ver de dónde procede. También conviene prestar especial atención por si hay algo extraño en la dirección, como una 'o' donde debería haber un cero, o letras mal ordenadas (Amaozn en lugar de Amazon, por ejemplo).

2. Revisar mensajes enviados. Otro aspecto a tener en cuenta es comprobar cuánta gente ha recibido el mismo mensaje. Si no son conocidos, lo mejor es no abrirlo. Un ataque de 'phishing' apunta a grandes grupos de personas a la vez, por lo que, si un 'email' tiene muchos receptores, se recomienda eliminarlo.

3. Coherencia en el asunto. Los mensajes que lleguen a la bandeja de entrada de un email corporativo deben estar relacionados con la actividad realizada en el trabajo. Un correo con un asunto que no se corresponda con las funciones de un trabajador, o una respuesta a un mensaje que ni siquiera se ha enviado en primer lugar, es muy probable que contengan 'malware'. O, en el mejor de los casos, 'spam'.

4. Analizar la hora de envío. ¿Hay en tu bandeja de entrada mensajes que no se correspondan con los horarios normales para tu trabajo? En la actualidad muchas empresas trabajan con equipos de diferentes países, pero es relativamente sencillo identificar 'emails' que no son los habituales.

5. Desconfiar de archivos adjuntos e hipervínculos extraños. La mayoría de ataques de 'phishing' incluyen enlaces y adjuntos fraudulentos. Son la puerta de entrada a través de las que los hackers consiguen acceder a las redes y a los equipos de las empresas. Check Point recomienda eliminarlo sin siquiera abrirlos.

6. Contenidos alarmantes. Los correos urgentes que requieren una acción inmediata por parte del usuario son a menudo ataques de 'phishing'. Por ejemplo, en caso de un mensaje que parezca del banco, es mejor llamar a la sucursal para asegurarse de que el 'email' es legítimo.

http://www.diarioinformacion.com/vida-y-estilo/tecnologia/2016/11/14/seis-consejos-evitar-ataques-phishing/1828183.html

Recomendaciones evitar ataques Spam

Usa GMail: El correo web con el mejor filtro antispam te ahorrara muchos problemas.

Evita los correos en cadena: Tanto enviarlos como recibirlos. Esta es **una de las principales fuentes de e-mails para los spammers**. Al reenviar un correo (*FW:*) se agregan al cuerpo del mensaje el correo entero incluyendo las direcciones de todos aquellos que han recibido el correo incluido tú.

Si vas a enviar un correo a varios destinatarios **usa el campo CCO**. Si un contacto tuyo te reenvía muchos correos en cadena sin usar el campo CCO pídele que lo haga, háblale de este post o dile que entre a Te aprecio mucho, pero… donde se lo explican con suavidad.

Nunca publiques tu e-mail completo en tu web: Por ejemplo, **no pongas un enlace mailto en tu blog** para que contacten contigo. ¿Por que? Porque **tu correo será indexado, al igual que el resto de tu web/blog por los buscadores**. Y si los spammers hacen una búsqueda avanzada pueden dar con muchos correos, incluido el tuyo.

Si quieres que contacten contigo en tu web pon un **formulario de contacto** o tu correo en forma de imagen usando E-Mail Icon Generator o bien **usa un formato tipo usuario[arroba]dominio[punto]com**, pero nunca escribas *usuario*@dominio.com por lo anteriormente mencionado.

Evita registrarte en páginas con tu correo: Nunca se sabe **lo fiable que puede ser un sitio con tus datos**. Si vas a registrarte en un sitio web de descargas, por ejemplo, **usa una cuenta de correo desechable** como puede ser MierdaMail u otras similares. Otra buena técnica puede ser usar dos cuentas de correo, una para registrarte en sitios web y

recibir publicidad y otra para el correo personal. O bien puedes utilizar BugMeNot y utilizar una cuenta compartida.

En Bitelia ya te hemos acercado esta y otras herramientas para evitar el spam, échales un vistazo.

Comprueba si es spam: Si, suena absurdo, pero puede ser que lo que estés recibiendo no sea spam propiamente dicho, si no que en algún momento que no recuerdes, al registrarte en alguna web **autorizaste a recibir información en forma de boletines o anuncios de terceros**. En ese caso es probable (debería serlo) que puedas darte de baja. En esos correos, **la información para darse de baja viene al final del mismo**.

https://hipertextual.com/archivo/2008/02/5-consejos-para-evitar-el-spam/