DOCUMENTO PARA CLIENTES, PROVEEDORES O TERCEROS- POLÍTICAS DE SEGURIDAD EMTELCO

Las siguientes políticas de seguridad son aplicables a los clientes, proveedores y/o terceros, que tengan alguna relación con EMTELCO S.A. bien sea de tipo legal, contractual o de cualquier otra índole no laboral y que en razón de ésta, tengan acceso a aplicativos, centros de cómputo, redes u otros aspectos regulados en este documento.

1. POLÍTICA DE ACCESO PORTÁTILES SEDES EMTELCO.

Todo portátil que ingrese por cualquier portería de las sedes, deberá ser registrado en los formatos definidos por el área de Seguridad de la Subdirección de Tecnología de EMTELCO y podrá ser revisado por el personal de Mesa de Ayuda, con el fin de determinar si los equipos cumplen con los requisitos mínimos establecidos por esta área.

Estos requisitos son:

1. software de antimalware del PC, actualizado a las últimas definiciones liberadas por el fabricante.
2. Actualizado el sistema operativo con los últimos parches liberados por el fabricante.
3. Tener activado el descansa pantalla protegido con contraseña.
4. En equipos Windows tener deshabilitado IP Routing
5. Tener deshabilitado la conexión compartida de Internet en todas las interfases
6. tener habilitado el firewall de Windows

2. REQUERIMIENTOS DE SEGURIDAD – CONEXIÓN CON CLIENTES.

2.1. INTRODUCCIÓN

Con el fin de minimizar los riesgos que se puedan presentar al entregar información sensitiva de Emtelco S.A. a un Cliente, proveedor o un tercero, para que sea el quien la administre, la haga disponible para Emtelco S.A., y la proteja, se hace necesario contar con fuertes elementos de seguridad físicos, lógicos y procedimentales por parte de éstos.

2.2. SEGURIDAD DE LA RED DE CONEXIÓN CON EMTELCO

El cliente, proveedor o tercero, deberá presentar un diagrama detallado y completo de su arquitectura de red, en el cual se especifique también la relación con otras redes, en especial las de otros CLIENTES.

2.3. ESQUEMA MÍNIMO DE CONEXIÓN

El esquema mínimo de seguridad para conexión con EMTELCO S.A. se presenta en la siguiente figura:

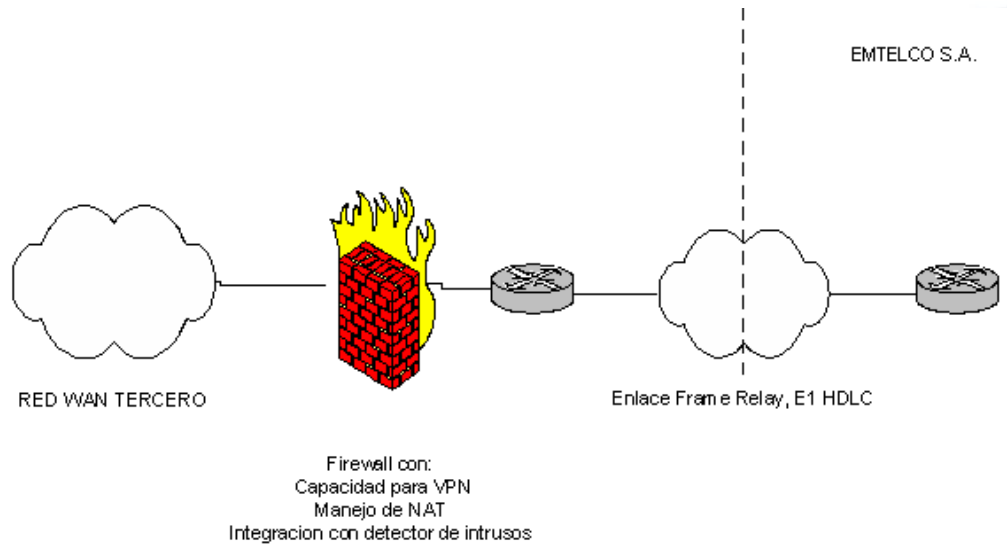

Figura 1 – Esquema mínimo de conexión

En este esquema se presentan los siguientes elementos principales:

- Enlace de comunicaciones: El enlace de comunicaciones deberá utilizar protocolo frame-relay, ADSL o HDLC. Los carriers que actualmente EMTELCO S.A. utiliza es UNE. Si el cliente proveedor o tercero requiriera que la conectividad se realice por medio de un carrier diferente, deberá asumir todos los gastos que se generen para conectar el enlace al Firewall de EMTELCO S.A.

Firewall: El firewall podrá ser cualquier hardware y software que se encuentre catalogado como firewall, mas no como equipo de comunicaciones con capacidades de firewalling. Deberá tener, como mínimo, capacidad para VPNs (IPSEC), NAT, e integración con detector de intrusos, o posibilidad para instalar un detector de intrusos.

2.4. ACCESO A TRAVES DE ENLACE DEDICADO PRIVADO

El cliente, proveedor o tercero deberá garantizar que su red de conexión con otros CLIENTES (incluyendo a EMTELCO S.A.) se encuentra separada de la zona desmilitarizada de Internet (DMZ).

El cliente, proveedor o tercero deberá garantizar que el enlace dedicado de EMTELCO S.A. llegará a una zona específicamente dispuesta para ello.

El cliente, proveedor o tercero deberá garantizar la independencia del tráfico de los diferentes CLIENTES que acceden a la red de los primeros por este medio. Para ello, el cliente, proveedor o tercero deberá ofrecer adicionalmente a EMTELCO S.A. esquemas de conexión que incluyan VPNs.

2.5. ACCESO VIA VPN – INTERNET

El cliente proveedor o tercero, podrá ofrecer adicionalmente a EMTELCO S.A. esquemas de conexión que incluyan VPNs vía Internet. Para esto, el cliente, proveedor o tercero, deberá garantizar que la red VPN se encuentre separada de la zona desmilitarizada de Internet (DMZ), así como garantizar la independencia del tráfico VPN de los diferentes clientes que se conecten por este medio.

2.6. SEGURIDAD EN LAS REDES LAN DE EL CLIENTE Y COMPUTADORES DE USUARIO FINAL

La versión de Software del cliente proveedor o tercero que se ejecutarán en las estaciones de usuario final deben ser compatibles con TODAS las actualizaciones de seguridad emitidas por parte de Microsoft y su programa de actualizaciones de definiciones mensual para corrección de vulnerabilidades detectadas a sus sistemas operativos y todos sus componentes como son: Internet Explorer, MDAC, SQL, etc.

La versión de Software del cliente, proveedor o tercero que se ejecutarán en las estaciones de usuario final deben ser compatibles con versiones de Antivirus conocidas, en particular con la instalada en la actualidad Symantec End Ponit Protection 11 o superior, así como son sus definiciones y actualizaciones liberadas por la casa matriz de Symantec.

2.7. USUARIOS, CONTRASEÑAS Y ROLES

El cliente, proveedor o tercero deberá cumplir las políticas de seguridad para el manejo de contraseñas establecido por EMTELCO S.A.

El cliente, proveedor o tercero deberá tener y presentar la información relacionada con sus políticas de seguridad con respecto al manejo de contraseñas.

El cliente proveedor o tercero deberá proporcionar información sobre la forma en la cual se realiza la identificación, autenticación y autorización de los usuarios en la red de este.

El cliente proveedor o tercero deberá tener y presentar la información sobre la forma en la cual se administra la creación / modificación / eliminación de las cuentas de los usuarios en la red de cada uno de estos.

3. VERIFICACIÓN DE LA SEGURIDAD

3.1. VERIFICACIÓN DURANTE LA ETAPA DE ANÁLISIS Y EVALUACIÓN DE PROPUESTAS

EMTELCO S.A. podrá verificar a su discreción y sin previo aviso, el cumplimiento por parte de el cliente proveedor o tercero de los requerimientos anteriormente establecidos.

3.2. VERIFICACIÓN CON EL CLIENTE PROVEEDOR O TERCERO PARA FIRMAR EL CONTRATO, O CON CONTRATO EN EJECUCIÓN

EMTELCO S.A. podrá verificar a su discreción y sin previo aviso, el cumplimiento por parte del cliente, proveedor o tercero de los requerimientos anteriormente establecidos. Estas verificaciones podrán llevarse a cabo en las instalaciones del cliente proveedor o tercero, o fuera de ellas al menos una (1) vez en cada mes calendario.

EMTELCO S.A. podrá realizar auditorias no intrusivas a la red sin previo aviso, y auditorias intrusivas coordinadas con un tiempo mínimo de advertencia de cuarenta y ocho (48) horas. En todo caso, EMTELCO S.A. entregará la información de la dirección IP desde la cual se realizarán este tipo de auditorias.

EMTELCO S.A. podrá tener acceso a las reglas del firewall que afecten la operación de EMTELCO S.A. Así mismo, el cliente proveedor o tercero deberá permitir el acceso a los logs de los detectores de intrusos, ya sea de forma constante o cada vez que EMTELCO S.A. lo requiera.

EMTELCO S.A. podrá solicitar modificaciones a los parámetros, arquitectura, políticas y procedimientos de seguridad que el cliente proveedor o tercero posee, debido a probables deficiencias observadas. En caso que el cliente, proveedor o tercero no encuentre procedente la solicitud de EMTELCO S.A., deberá justificar el motivo por el cual no se realizará la modificación, y las alternativas con las cuales ya gestiona o con las que subsanará las deficiencias en seguridad planteadas.

3.3. ACCESO A RECURSOS Y APLICACIONES DE EMTELCO S.A.

EMTELCO S.A. utilizará servicios de acceso remoto para la conexión del cliente, proveedor o tercero, a las aplicaciones y recursos requeridos. Este será el único medio permitido por EMTELCO S.A. para el acceso a las aplicaciones.

EMTELCO S.A. Se reserva el derecho a cambiar a su discreción la forma de acceso a las aplicaciones. Para esto, y si EMTELCO S.A. encuentra que la red del cliente proveedor o tercero se

puede ver afectada en un alto grado, EMTELCO S.A. avisará a este con una anticipación no mínima a treinta (30) días calendario sobre las modificaciones a las que haya lugar.

Si por la funcionalidad de las aplicaciones es necesario tener otro tipo de accesos a recursos de la red corporativa de EMTELCO S.A., será EMTELCO S.A. Quien decida el esquema en que estos accesos se realizarán.

3.4. POLÍTICA PARA EL ACCESO, USO Y ADMINISTRACIÓN DE ÁREAS ESPECIALIZADAS DE CENTRO DE CÓMPUTO

1. Operar el sistema de computación central y mantener el sistema disponible para los usuarios.
2. Ejecutar los procesos asignados conforme a los programas de producción y Calendarios preestablecidos, dejando el registro correspondiente en las solicitudes de proceso.
3. Revisar los resultados de los procesos e incorporar acciones correctivas conforme a instrucciones de su superior inmediato.
4. Realizar las copias de respaldo (back-up) de la información y procesos de cómputo que se realizan en la Dirección, conforme a parámetros preestablecidos.
5. Marcar y/o señalizar los productos de los procesos ejecutados.
6. Llevar registros de fallas, problemas, soluciones, acciones desarrolladas,

Respaldos, recuperaciones y trabajos realizados.

7. Aplicar en forma estricta las normas de seguridad y control establecidas.
8. Cumplir con las normas, reglamentos y procedimientos establecidos por la

Dirección para el desarrollo de las funciones asignadas.

4. PROHIBICIONES A LOS CLIENTES, PROVEEDORES O TERCEROS

Se encuentra prohibido a todos los clientes, proveedores o terceros que guarden alguna relación con Emtelco S.A., cuando tengan acceso a la red o a los centros de cómputo de EMTELCO S.A. las siguientes conductas:

1. La descarga de programas, fotos, música, videos y demás tipo de información digital vía Internet, al igual que del tráfico de información vía Messenger o mensajería instantánea, a excepción de los medios autorizados por la compañía.

2. Instalar en los equipos cualquier Software no autorizado, sin importar su modo de distribución, ya sea electrónica o físicamente.
3. Compartir carpetas, transferir archivos por la red ya sea por Email o cualquier otro transporte, con fines diferentes a los laborales, ya sea para diversión, intrusión o cualquier otro tipo de interés.
4. Dañar física o lógicamente los equipos o la infraestructura informática.
5. Conectar, desconectar, desmantelar, retirar o cambiar partes, reubicar equipos o cambiar de configuración a los mismos sin autorización expresa del oficial de seguridad de Emtelco S.A.
6. Instalar dispositivos o tarjetas de acceso remoto, módems, RDSI, routers o cualquier otro dispositivo de comunicaciones en los equipos e infraestructura tecnológica destinados para la prestación del servicio.
7. Usar cuentas de equipos sin autorización. Obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario. Comunicar a otros la contraseña para que puedan entrar en la cuenta.
8. Realizar cualquier acto que interfiera en el correcto funcionamiento de los equipos informáticos o de la infraestructura tecnológica para la prestación del servicio, estaciones de trabajo de escritorio o portátiles, equipos terminales de telefonía o terminales de comunicaciones alámbricas o inalámbricas, equipos periféricos, red de comunicaciones, canal de comunicaciones de voz, datos o Internet.
9. Instalar o ejecutar programas que perjudiquen la estabilidad de los equipos, su sistema operativo o sus programas internos o aplicaciones de las empresas. Esto incluye los programas conocidos como virus informáticos, cualquier tipo de ensayo o experimento, hardware, software, spammers, spimmers, troyanos, keyloggers, entre otros.
10. Uso del servicio de manera tal que constituya una molestia, abuso, amenaza o que de cualquier forma atente contra la integridad del equipo e infraestructura tecnológica.
11. Tratar de evitar o alterar los procesos o procedimientos de medida del tiempo, utilización del ancho de banda o cualquier otro método utilizado para documentar el uso de los productos y servicios.
12. Extraer información física o electrónica que viole los derechos de autor y/o la confidencialidad de EMTELCO, sus clientes o sus proveedores.
13. Instalar o ejecutar programas que traten de descubrir la información distinta de la del propio usuario. Esto incluye los sniffer, scanner de puerto, analizador de protocolos, detectores de redes, herramientas de ping Dos, Ddos, entre otros.
14. Intentar sobrepasar protecciones de datos o sistemas de seguridad informática.

15. Hacer uso abusivo de las claves o permisos que posea en virtud de cualquier tipo de relación con EMTELCO S.A., para fines particulares o beneficio de terceros o para acceder a información de equipos ajenos.
16. Los equipos de Emtelco S.A deben ser usados sólo con propósitos legítimos. La transmisión, distribución, reproducción o almacenamiento de cualquier tipo de información, datos o material en violación de cualquier ley aplicable o regulación al respecto, está estrictamente prohibido. Sin que esta enunciación pueda considerarse limitativa, está estrictamente prohibido crear, transmitir, reproducir, distribuir o almacenar cualquier información, data o material que:

    - Infrinja cualquier derecho de autor, propiedad intelectual o industrial.
    - Sea obscena o constituya cualquier tipo de pornografía.
    - Sea injuriosa, calumniosa o constituya una amenaza a la integridad de las personas, de acuerdo a la ley.
    - Viole las leyes y/o regulaciones de exportación.
    - Incite a conductas que puedan constituirse en ofensas criminales o puedan comprometer la responsabilidad civil o penal.

17. Trasmitir cualquier información con fines personales diferentes a los a la relación contractual o de cualquier otra índole con EMTELCO, o con fines políticos o religiosos, campañas de SPAM, SPIM, ventas de artículos, entre otros.
18. Uso de equipos portátiles propios, para acceso a los recursos tecnológicos de Emtelco S.A, sin previa autorización.
19. Uso de los recursos de Email, impresoras, fax, scanner, y demás herramientas informáticas para fines que no corresponden al objeto de la relación con EMTELCO S.A.

5. OTORGAMIENTO DE PERMISOS

Para la obtención de permisos para la instalación de programas, software, dispositivos entre otras herramientas informáticas especiales que se requieran para el cumplimiento de los objetivos relacionados con su vínculo como cliente, proveedor o tercero de EMTELCO S.A. Se deberá contar con documento escrito debidamente firmado por el Subdirector de Tecnología.