POLÍTICAS DE SEGURIDAD

IMPLEMENTACIÓN (RESC. CRC No. 2258 DE 2009)

ANTECEDENTES

Es evidente que la seguridad tiene que provenir de un proceso cuidadosamente desarrollado que contemple desde la concepción y el diseño del sistema, a través de su implementación, hasta las políticas y prácticas necesarias para su instalación, funcionamiento y utilización. Es indispensable que la seguridad esté presente desde un principio en el desarrollo de las normas y no durante su aplicación, pues los puntos vulnerables suelen aparecer desde el comienzo.

Al desarrollarse al ritmo de un entorno comercial cada vez más mundializado, la industria de las comunicaciones ha contribuido a incrementar la productividad y a interconectar las comunidades de todo el mundo, en prácticamente todos los ramos de la industria. Buena parte de este éxito se debe al desarrollo de las normas efectuado por organizaciones como el UIT-T.

Si bien las normas existentes facilitan la eficacia de las redes y sistemas actuales y preparan el terreno para las futuras, el incremento de la utilización de protocolos e interfaces abiertos, la variedad de nuevos actores, la impresionante diversidad de aplicaciones y plataformas y las implementaciones no siempre eficientemente probadas han provocado un incremento de la posibilidad de que se produzcan utilizaciones malintencionadas de las redes. En los años recientes, se ha venido observando un significativo aumento de violaciones de seguridad informática (por ejemplo, la diseminación de virus y la violación de la confidencialidad de datos almacenados) en las redes mundiales, lo que con frecuencia provoca efectos costosos.

Así las cosas, cabe preguntarse cómo se puede soportar una infraestructura abierta de comunicaciones sin que se exponga su información a problemas de seguridad. La respuesta reposa en los esfuerzos de los grupos de normalización tendientes a combatir las amenazas a la seguridad en todas las áreas de infraestructura de telecomunicaciones, y que van desde detalles en las especificaciones de los protocolos y en las aplicaciones hasta la gestión de las redes. COLOMBIA MAS TV se apoya en las diferentes recomendaciones desarrolladas por el UIT-T para garantizar la confiabilidad y calidad de su infraestructura de telecomunicaciones y los servicios y aplicaciones correspondientes.

En ese orden de ideas, y conforme a como se encuentra establecido en el Artículo 6 de la Resolución 2258 de 2009, rendimos informe de estrategias para la seguridad de la red, así:

1. Definiciones generales.

Para un mayor entendimiento de los planteamientos que COLOMBIA MAS TV hace en el presente documento, el mismo ha de ser interpretado conforme a las siguientes dediciones generales, que se encuentran establecidas en el Artículo 1.8 de la Resolución CRT 1740 de 2007, y en el Artículo 1 de la Resolución CRC 2258 de 2009:

1.1. Acceso a internet: Acceso físico que incluye todas las funcionalidades y conexiones nacionales y/o internacionales necesarias para permitir a un usuario establecer comunicación con un nodo de internet, entendido éste último como un punto TIER-1 o un punto de acceso nacional (NAP).

1.2. Acceso conmutado: Forma de acceso a internet en la cual la conexión entre el terminal de usuario y el equipo de acceso del operador que presta el acceso a Internet, se hace a través de la marcación sobre una línea telefónica de la red de TPBC.

1.3. Banda ancha: Es la capacidad de transmisión con ancho de banda suficiente para permitir de manera combinada la provisión de voz, datos y video, ya sea de manera alámbrica o inalámbrica. Para efectos de la comercialización, debe tenerse en cuenta que será considerada una conexión de "banda ancha" aquella en la que las velocidades efectivas de acceso cumplan los siguientes valores mínimos:

Sentido de la Conexión Velocidad efectiva Mínima

ISP hacia usuario 512 Kbps o"downstream"

Usuario hacia ISP 256 Ps o"upstream"

1.4. Banda angosta: Es la capacidad de transmisión alámbrica o inalámbrica con velocidad efectiva de transmisión de datos inferior a la establecida en la definición de banda ancha.

1.5.Calidad de servicio (QoS): El efecto global de la calidad de funcionamiento de un servicio que determina el grado de satisfacción del servicio por parte de un usuario.

1.6. Velocidad de transmisión de datos: En sistemas digitales corresponde a la cantidad de información que puede ser transmitida en el tiempo a través de un canal de comunicación, expresada en bits por segundo (bps) y sus múltiplos.

1.7. Autenticación: Proceso destinado a permitir al sistema asegurar la identificación de una parte.

1.8. Autorización: Proceso de atribución de derechos o concesión de permisos para realizar determinadas actividades y su relación con determinados procesos, entidades, personas jurídicas o naturales.

1.9. Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

1.10. Ciberseguridad: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

1.11. Confidencialidad de datos: Impedir que los datos sean divulgados sin autorización.

1.12. Disponibilidad: Acceso por parte de una entidad autorizada a la información y sistemas informáticos, cuando esta entidad lo requiera.

1.13. Entidad: Persona natural o jurídica, organización, elemento perteneciente a un equipo o a un programa informático.

1.14. Infraestructura crítica: Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una Nación.

1.15. Integridad de datos: Propiedad o característica de mantener la exactitud y completitud de la información.

1.16. Interceptación: Es la adquisición, visualización, captura o copia de contenido, datos o parte de contenido de una comunicación transmitida por medio alámbrico, electrónico, óptico, magnético u otras formas, realizada durante la transmisión, utilizando medios electrónicos, mecánicos, ópticos o electromagnéticos.

1.17. Interferencia: Es la acción de bloquear, ocultar, impedir o interrumpir la confidencialidad, la integridad de programas computacionales, sistemas computacionales, datos o información, mediante la transmisión, daño, borrado, destrucción, alteración o supresión de datos, de programas de computación o tráfico de datos.

1.18. Interrupción: Es el evento causado por un programa computacional, una red de telecomunicaciones o sistema computacional que interfiere o destruye un programa computacional, una red de telecomunicaciones, datos e información que esta contenga.

1.19. No repudio: Servicio que tiene como objetivo garantizar la disponibilidad de pruebas que pueden presentarse a terceros y utilizarse para demostrar que un determinado evento o acción ha tenido lugar, con el propósito de evitar que una persona o una entidad niegue haber realizado una acción de tratamiento de datos, proporcionando prueba de dichas acciones en la red.

1.20. Pharming: Es la acción de modificar el servidor (DNS) Domain Name System, cambiando la dirección IP correcta por otra, de tal manera que haga entrar al usuario a una IP diferente con la creencia de que accede a un sitio personal, comercial o de confianza.

1.21. Phishing: Acto de enviar un correo electrónico cuyo objeto es engañar al usuario dirigiéndolo a una página web falsa y por este medio, obtener de este, información privada que será utilizada para fines no autorizados o ilícitos como el robo de identidad y de contraseñas.

1.22. Software Malicioso (Malware): Es un programa computacional que es insertado en un computador o sistema computacional sin autorización, con el objeto de comprometer la confidencialidad e integridad del sistema computacional, de la red de telecomunicaciones, datos y del tráfico de datos. Esta clase de programa se presenta en forma de virus, gusanos, y troyanos electrónicos y demás, que se pueden distribuir a través de email, web site, shareware o freeware.

1.23. Vulnerabilidad: Cualquier debilidad que pudiera explotarse con el fin de violar un sistema o de la información que contiene".

1.4. Garantía en la seguridad de la red, y la integridad del servicio, para evitar interceptación, interrupción, e interferencia del mismo.

Permanentemente, COLOMBIA MAS TV realiza monitoreos sucesivos sobre cada uno de los servicios q provee, de tal forma que puede identificar en tiempo y forma cualquier evento o anomalía en la red, para ello utiliza equipos dispuestos en puntos estratégicos de la red que monitorean entre otras cosas:

• Estado de los equipos de red

• Logs de Actividades realizadas en los equipos

• Monitoreo del comportamiento del tráfico en diferentes sectores de la red tales como puntos de interconexión, peering, y concatenación de nodos.

• Informes detallados Vía control de Firewall donde se especifica y detalla el tráfico cursado por puntos críticos de red, signatures de ataques, análisis permanentes de vulnerabilidades en dispositivos y servidores de misión crítica. Backups de dispositivos de red, backups y redundanica absoluta de bases de datos y protegidas bajo estructuras de mínima exposición pública.

• Comités de Evaluación de Seguridad, donde se detallan y exponen vulnerabilidades y puntos críticos de red y se establecen herramientas que puedan cubrir las falencias detectadas.

1.5. Modelos de seguridad, de acuerdo con las características y necesidades propias de la red, que contribuyan a mejorar la seguridad de las redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT

COLOMBIA MAS TV COLOMBIA, en el ejercicio de su actividad como prestador de servicios de telecomunicaciones, y dando cumplimiento a lo ordenado por las autoridades de vigilancia y control de la actividad, ha implementado los modelos que a continuación se relacionan, para efectos de la protección de las redes y los usuarios finales, en los términos establecidos por la normatividad vigente:

1.5.1. Autenticación.

De acuerdo a lo referenciado en las normas UIT X.805 y X.811, la autenticación consiste en probar la veracidad de la identidad reclamada por una entidad. En este contexto, se consideran entidades no solamente a las personas sino también los mecanismos, servicios y aplicaciones. Con la autenticación se pretende también garantizar que una entidad no esté tratando de usurpar una identidad o de emitir una respuesta no autorizada a una comunicación previa.

Los servicios de mensajería y colaboración ofrecidos por COLOMBIA MAS TV a sus clientes tienen sistemas de autenticación basados en arquitectura LDAP, la cual además de ser robusta y confiable, permite el uso de encripción de contraseñas , de tal forma que las credenciales solo sean conocidas por el usuario final, garantizando así un nivel adicional para la confidencialidad de la información.

Para nuestros servicios de hosting web compartido y dedicado, COLOMBIA MAS TV aplica el modelo de seguridad a nivel de dominio, entendiéndose por dominio el ámbito de seguridad que encapsula los servicios de cada cliente. Bajo este modelo, una vez autenticado, el suscriptor tiene acceso total a su información, incluyendo las bases de datos de las cuales es propietario, y con este control podrá crear usuarios con privilegios específicos dentro de su dominio de seguridad, cuya responsabilidad recae directamente sobre el cliente propietario del dominio.

En los servicios de hosting dedicado, COLOMBIA MAS TV entrega el control total de los sistemas de hardware, sistema operativo base y software al cliente, de tal forma que la administración de los servicios de autenticación está bajo responsabilidad total del cliente.

1.5.2. Control de acceso

La dimensión de seguridad del control de acceso, protege contra la utilización de recursos de red sin autorización. El control de acceso garantiza que sólo las personas y los dispositivos autorizados pueden

acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. El control de acceso se define en la cláusula 6.3/X.810 y en la Rec. UIT-T X.812. Aunque tiene que ver con la autenticación, está fuera del alcance de ésta.

a) Seguridad Física, COLOMBIA MAS TV tiene varios años de experiencia en diseñar, construir y operar data centers a mediana escala en todos nuestros puntos de presencia directa Colombia. Esta experiencia ha sido aplicada a nuestra plataforma e infraestructura.

Los data centers de COLOMBIA MAS TV están ubicados en facilidades con perímetros físicamente protegidos incluyendo sistemas de vigilancia con cubrimiento en horario de 7 x 24 x 365.. El acceso físico es estrictamente controlado tanto en el perímetro como en los puntos de ingreso al edificio por profesional de seguridad apoyándose en sistemas de video, sistemas de detección de intrusos y otros medios electrónicos.

Los miembros del staff autorizado deben cumplir al menos dos factores de autenticación para acceder físicamente a un data center. Todos los visitantes y contratistas deben presentar identificación y firma, luego de lo cual son acompañados en todo momento por un miembro del staff autorizado.

COLOMBIA MAS TV solo provee acceso a los data centers a empleados quienes tienen una necesidad de negocios legitima para obtener tal privilegio, su acceso es inmediatamente revocado cuando dicha necesidad culmina, incluso si continúan siendo empleados de COLOMBIA MAS TV. Todo acceso físico y electrónico de los empleados a los data centers de COLOMBIA MAS TV es registrado y auditado rutinariamente.

b) Seguridad de acceso lógico. La seguridad de acceso lógico a las diferentes plataformas de Hosting de COLOMBIA MAS TV es suministrada en múltiples niveles: sistema operativo, instancias virtuales, aplicaciones y firewall. Cada uno de estos ítems se construye sobre las capacidades de los demás. La meta es asegurar que los datos contenidos dentro de las diferentes plataformas de Hosting de COLOMBIA MAS TV no pueden ser interceptados por sistemas o usuarios no autorizados y que las diversas instancias de servicios de COLOMBIA MAS TV brindar la mayor seguridad posible sin sacrificar la flexibilidad en configuración y funcionalidad que demandan los clientes.

- Seguridad a nivel de Sistemas Operativo: Los Administradores de sistemas de COLOMBIA MAS TV con una necesidad de negocios relacionada con los servicios de Hosting, deben suministrar credenciales para lograr el acceso con privilegios básicos a los diferentes sistemas. Dicho proceso de acceso se lleva a cabo en un entorno de seguridad centralizado a través de autenticación LDAP, y haciendo uso de protocolos SSH y Kerberos dependiendo del sistema operativo al cual se accede.

Este bastión de seguridad de acceso a nivel del sistema operativo permite la construcción de sistemas que son diseñados y configurados para proteger el plano de administración de las plataformas de hosting. Una vez conectado a este bastión inicial, los administradores autorizados pueden hacer uso de comandos para escalar los privilegios con un segundo nivel de autenticación. Tales accesos son registrados y auditados rutinariamente. Cuando deja de existir la necesidad del negocio respectiva, los privilegios y accesos al bastión de seguridad a nivel de sistema operativo son revocados.

- Instancias virtuales: las instancias virtuales conocidas también como servidores virtuales, son controladas completamente por el cliente, quien tiene acceso total administrativo sobre la instancia y sobre las cuentas adicionales, servicios y aplicaciones que corren sobre ella. Los administradores de sistemas de COLOMBIA MAS TV no tienen acceso a las instancias virtuales de los clientes, y no pueden autenticarse para lograr acceso a ellas a nivel de sistema operativo. Por lo anterior, los clientes deben emplear un mecanismo de elevación de privilegios basados en autenticación para acceder al sistema operativo de la instancia virtual.

- Firewall: COLOMBIA MAS TV provee una solución de firewall para las diferentes plataformas de Hosting Compartido, como hosting web, y sistemas de mensajería y colaboración. Este firewall es configurado en modo de denegación por defecto para tráfico entrante, y es el cliente quien debe especificar explícitamente los puertos y el protocolo para los cuales se debe permitir el tráfico siempre y cuando esté relacionado directamente con el servicio contratado. El cliente también debe especificar la IP, el conjunto de IP´s o las redes de origen permitidas para su servicio.

Para los servicios de hosting dedicado, incluyendo las instancias virtuales, el servicio de firewall es optativo para el cliente, y en caso de no adquirirlo, es su responsabilidad cualquier incidente relacionado con una intromisión no autorizada a su sistema desde Internet.

El acceso administrativo vía SSH o RDP para los Administradores de sistemas de COLOMBIA MAS TV solo es permitido a través de conexiones VPN basadas en PPTP o L2TP, logrando así un máximo nivel de encapsulación de la información y de las credenciales de acceso.

1.5.3. Servicio de no repudio

Las normas UIT X.805, X.813 y X.843 se refieren al servicio de No Repudio como la capacidad de evitar que un usuario niegue más adelante haber efectuado una acción. Entre éstas se incluyen la creación, origen, recepción y entrega de contenidos, por ejemplo envío o recepción de mensajes, establecimiento o recepción de llamadas, etc. Gracias a los requisitos de no repudio, es posible colectar pruebas infalsificables del envío y/o recepción de datos a fin de evitar que el remitente niegue haber enviado un mensaje o el destinatario haberlo recibido. COLOMBIA MAS TV implementa este servicio en sus diferentes plataformas de hosting.

En sus servicios de mensajería y colaboración, COLOMBIA MAS TV mantiene un registro de los correos enviados y recibidos a nivel del servicio SMTP. El periodo de retención de dicho registro es establecido por COLOMBIA MAS TV e informado al cliente dentro del proceso de oferta de servicios previo a la contratación por parte del cliente. Como parte del portafolio de productos de valor agregado de mensajería y colaboración, COLOMBIA MAS TV ofrece servicios opcionales de respaldo y auditoria de correos que cumplen con regulaciones internacionales incluso a los niveles exigidos por las entidades financieras en Estados Unidos.

Para los servicios de hosting web compartido, COLOMBIA MAS TV mantiene un registro de los accesos y actividades de manipulación de contenidos. El periodo de retención de dicho registro es establecido por COLOMBIA MAS TV e informado al cliente como parte del proceso de oferta de servicios previo a la contratación por parte del cliente.

COLOMBIA MAS TV registra todas las tareas realizadas por los administradores de sistemas de la compañía sobre las diferentes plataformas de Hosting, y realiza una auditoria regular sobre las mismas. Este registro se hace mediante un sistema centralizado de almacenamiento de logs.

Dado que el cliente tiene el control total de la administración de los servicios de Hosting dedicado, incluyendo los servicios virtualizados, es responsabilidad del cliente el registro de logs y las labores relacionadas con los servicios de No repudio.

1.5.4. Principio de confidencialidad de datos

COLOMBIA MAS TV Hosted Services ofrece una plataforma escalable de alta disponibilidad, y permite a los usuarios el manejo de una amplia gama de productos. Asegurar la privacidad y confidencialidad, de los sistemas y datos de los clientes es de vital importancia para COLOMBIA MAS TV.

El estándar UIT-T X.805 establece una diferencia explícita entre la privacidad y la confidencialidad de datos, la primera tiene que ver con la protección de la asociación de la identidad de los usuarios y sus actividades, mientras que la segunda se refiere a la protección contra accesos no autorizados al contenido de los datos.

1.5.5. Privacidad

Las políticas internas de COLOMBIA MAS TV que hacen referencia a la privacidad de datos de acuerdo a lo establecido en el estándar UIT X.805 garantizan que la información suministrada por los usuarios en el momento del registro a cualquiera de nuestros sistemas no es divulgada a terceros sin la autorización previa del cliente.

a) Confidencialidad de datos. Para garantizar la confidencialidad de datos se suele utilizar métodos del tipo encriptación, listas de control de acceso y permisos de acceso a ficheros.

El acceso web a los servicios de correo ofrecidos a nuestros clientes se realiza a través de sitios seguros que usan certificados SSL expedidos por entidades reconocidas a nivel mundial. Adicionalmente se ofrecen a nuestros clientes sistemas de mensajería y colaboración cuyo acceso a través de sus clientes de correo tradicionales se realiza a través del protocolo RPC sobre HTTPS, garantizando así la confidencialidad de su información.

Como parte de nuestros productos de valor agregado, el cliente tiene la opción de adquirir servicios de encripción de correo en los cuales se garantiza que únicamente los destinatarios autorizados previamente pueden acceder a la información contenida en los mensajes enviados por nuestros usuarios. Estos servicios basados en criptografía asimétrica (o de clave pública) , y a los cuales hace referencia el estándar UIT X.809, involucran un par de claves, a saber una pública y una privada. Como su nombre lo indica, una se hace pública

mientras que la otra se mantiene secreta. Ambas son diferentes y aunque exista una relación matemática entre ellas no es posible calcular la clave privada a partir de la pública.

Para nuestros servicios de hosting web compartido y dedicado, aplicamos políticas de seguridad basadas en listas de control de acceso, que garantizan que el acceso a la información y su manipulación solo pueden ser realizadas por un usuario valido y con privilegios previamente autorizadas por el cliente. Todos los paneles de control ofrecidos a los clientes para la administración de sus servicios de hosting están protegidos con certificados SSL.

1.5.6. Principio de integridad de datos

Según lo referenciado en las recomendaciones UIT X.800 y X.815, el principio de integridad de datos es una propiedad que consiste en que los datos no han sido alterados de una manera no autorizada. Además, la integridad de los datos garantiza que la información esté protegida contra las siguientes operaciones no autorizadas: modificación, supresión, creación, y copia de los datos. Se proporciona también un indicador de estas actividades no autorizadas.

En todos los servicios de Hosting compartido de COLOMBIA MAS TV se usa un marco común de seguridad que protege la integridad de la información del cliente mediante el uso de ACL's y perfiles con diferentes niveles de acceso, con los cuales se asegura que la información solo puede ser manipulada por su usuario propietario, y de acuerdo a los privilegios previamente establecidos de acuerdo al servicio contratado.

COLOMBIA MAS TV realiza actualizaciones periódicas sobre todos sus sistemas de Hosting compartido con el fin de evitar manipulación intencional de información que pueda ser realizada por un agente externo aprovechando vulnerabilidades a nivel de sistema operativo, motores de bases de datos, o software de correo.

Por otro lado, COLOMBIA MAS TV cuenta con software antivirus para aquellos sistemas, tanto de correo como de web hosting, que pueden ser objetivo de ataques de virus informáticos, los cuales pueden afectar la integridad de la información del cliente.

Los clientes de Hosting dedicado, incluyendo los de servicios virtualizados, son responsables por garantizar la integridad de la información que se almacena en dichos sistemas, pues COLOMBIA MAS TV no tiene control alguno de los mismos a nivel lógico.

1.5.7. Principio de disponibilidad

La dimensión de seguridad disponibilidad que estipula la recomendación UIT X.805 garantiza que una interrupción de la red no impida el acceso autorizado a los elementos de ésta, la información almacenada, los flujos de información, los servicios y las aplicaciones. Esta categoría incluye soluciones para recuperación en caso de desastre y para restablecimiento de la red.

COLOMBIA MAS TV garantiza los niveles de disponibilidad previamente acordados con el cliente durante el proceso de contratación mediante una infraestructura diseñada e implementada para cada uno de los servicios ofrecidos a nivel de Hosting.

Todos los Data Centers de COLOMBIA MAS TV a nivel regional cuentan con sistemas de redundancia en los sistemas de alimentación eléctrica. Para nuestros Data Centers, se cuenta con esquemas de redundancia n+1 para los sistemas de alimentación eléctrica, control de temperatura y de humidificación, que permiten brindar una alta disponibilidad para los servicios de hosting compartido alojados en dichas facilidades.

Dependiendo del nivel de criticidad de cada sistema, y según lo estipulado previamente en los acuerdos de niveles de servicio, las distintas plataformas de Hosting cuentan con granjas de servidores que permiten ofrecer una alta disponibilidad en caso de un fallo a nivel de sistema operativo, de hardware o incluso a nivel de servicios.

Los equipos de almacenamiento implementados por COLOMBIA MAS TV para los sistemas de misión crítica en sus distintas plataformas de Hosting compartido cuentan con opciones de procesamiento redundante en caso de fallo de una de sus controladoras, de igual forma todos nuestros sistemas de almacenamiento se implementan haciendo uso de tecnologías de RAID para minimizar los impactos en la disponibilidad causados por fallos físicos a nivel de discos.

En caso de una eventualidad que afecte la disponibilidad de los servicios y que sobrepase los alcances de los sistemas y métodos de alta disponibilidad anteriormente descritos, COLOMBIA MAS TV cuenta con sistemas de respaldo que garantizan la posibilidad de recuperación de la información en caso de una contingencia informática para todos sus servicios de hosting compartido.

Estos sistemas de respaldo, acompañados de los métodos y procedimientos establecidos por el equipo de administradores de sistemas de COLOMBIA MAS TV permiten restablecer la prestación de los servicios en caso de un desastre informático y según los tiempos establecidos en los niveles de disponibilidad ofrecidos a nuestros clientes.

1.6. Medidas en relación con las redes y servicios suministrados, en lo que atañe a asegurar los principios (confidencialidad, integridad y disponibilidad) y servicios de seguridad (autenticación, autorización y no repudio) de la información, requeridos para garantizar la inviolabilidad de las comunicaciones, la información que se curse a través de ellas y los datos personales de los suscriptores y/o usuarios, en lo referente a las redes y/o sentidos suministrados por dichos operadores.

El conjunto de actividades, acciones y métodos están detallados en los pasos anteriores, es todo el conjunto de parámetros de autenticación, protección, servicios de encripcion encaminados hacia el desarrollo y aseguramiento de cada uno de los componentes de red, de igual manera los servicios de diagnóstico control y monitoreo permiten visualizar en forma permanente cambios en la estructura de red.

De igual manera COLOMBIA MAS TV cuenta con personal exclusivamente dedicado a la gestión de red, dicho personal administra y visualiza en forma permanente el comportamiento de la red y de cada uno de los servicios ofrecidos, permitiendo así una rápida visualización de amenazas o problemas que atente contra la estabilidad de los servicios ofrecidos y el Backbone de red.

1.7. Medidas en relación con la interceptación, violación o repudio de las comunicaciones que cursen por redes.

Controles de acceso a los equipos de Backbone y CPE (Equipos ubicados en las instalaciones de los abonados), adicionalmente los sistemas de detección y monitoreo de eventos sobre todo el Backbone de red, red de acceso y Customer-Side permiten una visualización sobre las acciones ejecutadas y/o denegadas a usuarios y terceros vinculados en las comunicaciones side-to-side

1.8. Procesos formales de tratamiento de incidentes de seguridad de la información propios de la gestión de seguridad del proveedor, cuando la violación proviene de un tercero, y el proveedor de redes y/o servicios de telecomunicaciones tienen conocimiento de dicha violación, además del informe de medidas necesarias para que la conducta cese e información ante las autoridades competentes la presunta violación.

El análisis forense es un conducto regular, aplicado en situación de desastre inminente. COLOMBIA MAS TV, tiene dispuesto equipamiento capaz de recobrar información post-disaster, de tal forma que puede obtener información detallada acerca de Origen, tipo de Acción ejecutada, afectación indirecta, afectación potencial a mediano, largo e inmediato plazo, mecanismos de fast-recovery y rastreo de información, estructuras de almacenamiento y bases de datos en modalidad HD. Para ellos dispone de sensores de tráfico y mecanismos de observación de tráfico (origen-destino-servicio) configurados sobre interfaces de acceso, UP-LINKS, NAPs y demás puntos de interacción e integración de redes públicas multioperador y multiacceso.

1.9. Mecanismos de garantía del manejo de la confidencial, la integridad y disponibilidad de los datos de los suscriptores y/o usuarios, los cuales solo pueden ser intercambiados con otros proveedores para efectos de la prevención y control de fraudes en las telecomunicaciones y el cumplimiento de las obligaciones regulatorias que así lo exijan.

Teniendo en cuenta las tendencias de las telecomunicaciones y la globalización en la información es necesario que entes gubernamentales regulen constantemente y a través de herramientas legales el intercambio de información de los usuarios entre proveedores de servicios de telecomunicaciones con el fin que se garantice la confidencialidad de la información de estos y de esta manera evitar un mal uso y mal manejo de dicha información.