POLITICAS DE SEGURIDAD IMPLEMENTACIÓN (RESC.CRC No. 2258 DE 2009)

ANTECEDENTE

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. DIGICOMS SAS 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 DIGICOMS SAS 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 inalambrico 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. 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 1024 Mbps o "downstream" Usuario hacia ISP 512 Ps o "upstream"

1.3. 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.

1.4. 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.

1.5. 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.

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

1.7. 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.

1.8. 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.

y mantengan las propiedades de seguridad de los activos y usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

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

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

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

1.12. 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.

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

1.14. 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.

1.15. 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.

1.16. 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.

1.17. 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.

1.18. 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.

1.19. 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.

1.20. 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.

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

• Firewall: DIGICOMS SAS 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 trafico 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.

• 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.