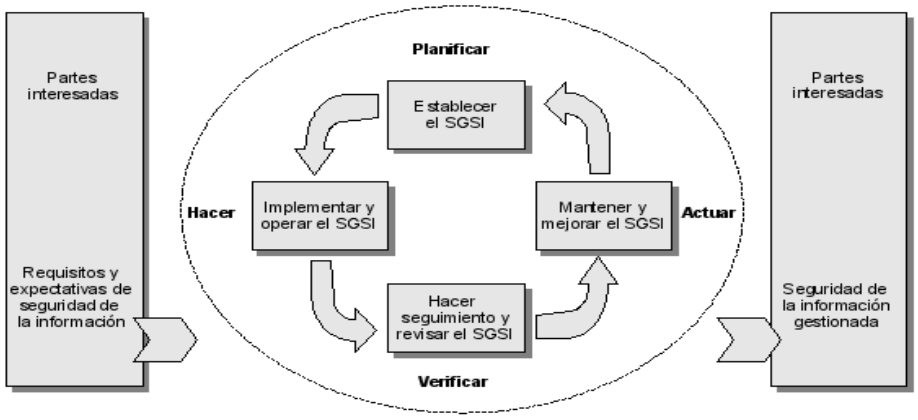
Seguridad en red – Resolución CRC 5050

En atención a la Resolución 5050 de 2016 en su artículo 5.1.2.3 a continuación se informa sobre las acciones adoptadas por ETB en relación con el servicio prestado al usuario final, en cuanto a seguridad de la red.

Modelos de Seguridad

ETB desarrolla el modelo de seguridad basado en los requerimientos de los clientes y bajo el marco de las normas ISO 27001 y 27002. El modelo extiende el gobierno de seguridad empresarial para todos los servicios y las redes de comunicaciones subyacentes. A través del mismo modelo 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.

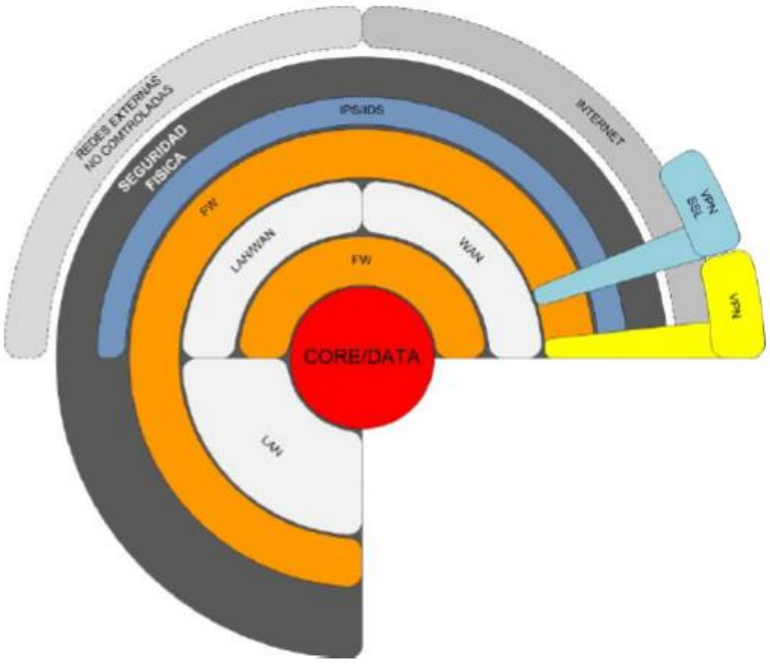
Mediante el siguiente esquema, resaltamos el *macroproceso* de implementación en Seguridad de la Información, que se está adelantando y gestionando bajo el marco de la familia de las normas ISO 27000.



Modelo de seguridad de la información

Fuente ISO 27001

Para la protección de los sistemas de información, que almacena información de usuarios y servicios de la Compañía, ETB cuenta con un modelo por capas que garantiza los controles necesarios para protegerla:



Modelo de Defensa en profundidad en los Centros de Datos de ETB

En particular, en lo concerniente con el modelo X.800, y basado en las acciones que ETB ha tomado sobre su infraestructura, se cuenta con los siguientes controles:

Autenticación

En la actualidad ETB protege la información de identidad de sus clientes mediante un esquema de seguridad por capas, segmentación de redes y VLANs, 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.

Para el caso de los servicios móviles, se usa el esquema de autenticación de los usuarios a través de SIM Cards, las cuales almacenan de forma segura la clave de servicio del suscriptor usada para identificarse ante la red. ETB usa el algoritmo de autenticación Milenage el cual se encuentra definido en el estándar ETSI TS 135 206. Este involucra el uso de constantes de autenticación como C y R así como la OPC de cada tarjeta, derivada de la llave maestra OP definida por el operador. Este algoritmo es el utilizado por la mayoría de los operadores a nivel internacional a fin de evitar principalmente clonación de SIMs asegurando la autenticidad del usuario en la red.

Los valores de las constantes de autenticación, así como la OP (llave maestra) que es la que define el operador, se encuentran resguardados bajo una política de seguridad interna de ETB. En ese proceso se establecieron las llaves de autenticación, así como su cargue en los sistemas de ETB, y la custodia y almacenamiento físico de las llaves de autenticación. Este documento está clasificado como CONFIDENCIAL.

Adicionalmente, para la gestión de los servicios, ETB ofrece a sus clientes un portal al que se ingresa con un identificador y contraseña única para cada cliente.

Acceso

Para todas las plataformas de red y servicios que hacen parte de la arquitectura del servicio de Acceso a Internet, se cuenta con controles de acceso diseñados específicamente de acuerdo a las funcionalidades provistas por el software y/o tecnología utilizada, asegurando que sólo usuarios autorizados puedan ingresar para efectuar las tareas requeridas.

Para los Servicios de Internet Fijo, ETB 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.

Para los Servicios de Planes de Datos Móviles, como se mencionaba en la sección anterior, se usan mecanismos de autenticación fuerte. El control de acceso al servicio

se basa en protocolos que autorizan el acceso a un usuario en función del plan del servicio contratado.

No repudio

Las mismas ventajas del control de acceso de los usuarios que se realiza mediante los protocolos de Autenticación, Autorización y *Accounting* son heredadas por los mecanismos de NO REPUDIO, gracias a los mecanismos de *accounting*. 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. Para el Servicio de Planes de Datos Móviles, se cuenta con CDRs que dan cuenta del tráfico de datos del suscriptor, así como del registro de fechas y horas de utilización del servicio. Este registro asegura que se pueda validar la evidencia de la identidad de usuario que hace uso del servicio.

A nivel de auditoría ETB hace uso de los registros de eventos o *logs* producidos por las plataformas de seguridad, para apoyar la resolución de incidentes, que puedan afectar los servicios prestados. Los *logs* generados por las plataformas de seguridad -como firewall e IPS- 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 necesarios.

Confidencialidad

ETB 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 e IPS, pasando por redes segmentadas, plataformas aseguradas y actualizadas y controles de acceso basados en roles, hasta auditorías y análisis de vulnerabilidades periódicos que garanticen la efectividad de los controles implementados.

A nivel de red, ETB garantiza que el acceso de los clientes a los servicios provistos en sus portales, en donde se ingresa información privada, sea confidencial, gracias a la utilización de protocolos seguros de conexión tales como SSL y/o TLS.

Integridad

Apoyados en las funcionalidades provistas por los protocolos de red en sus diferentes tecnologías tales como ETHERNET y sus evoluciones, MPLS, VPLS, VC, IP/TCP/UDP, etc.; ETB provee una red que 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.

IP/TCP/UDP, etc.; ETB provee una red que 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.

Cabe anotar que el servicio de Internet que se presta a nuestros clientes se basa en una funcionalidad que divide las fases de comunicación para la trasmisión de datos en capas, en donde la responsabilidad de garantizar la seguridad en las aplicaciones (de la capa 4 hasta la capa 7 del modelo OSI, generado por los equipos y software del cliente y del sitio que es accedido en Internet) es responsabilidad del usuario. En este caso, la red de ETB sólo consulta la información de capa la capa 3 del mencionado modelo, en los diferentes saltos o *hops* de la red y provee la conectividad requerida (capa 1 y capa 2) para garantizar el transporte de los datos de los usuarios hacia Internet, a excepción de los controles de navegación reglamentados por la Ley, tales

como la prohibición de acceso a pornografía infantil de acuerdo a lo estipulado en la ley 679 y 1336.

Disponibilidad

Los servicios se apoyan en una estructura de red altamente redundante que cuenta con múltiples caminos para transportar los datos de los clientes, ya sea sobre las diferentes redes de acceso, transporte y *backbone* disponibles, así como sobre los múltiples puntos de conexión internacional a Internet distribuidos en todo el país.

Esta infraestructura de red está apoyada por plataformas de servicios IP como el DNS, Servidores de Autenticación, Autorización y *Accounting* y servidores HLR/HSS (en particular para el servicio de Planes de Datos Móviles), los cuales poseen redundancia geográfica (estos servicios se ubican en dos nodos diferentes de la red) asegurando una alta disponibilidad del servicio en todo momento entregando al cliente la mejor experiencia de navegación posible.

Recursos Tecnológicos

Para la prestación del servicio de acceso a Internet, ETB posee sistemas de seguridad para la protección de sus equipos tanto en software como en hardware, así como para la protección de la información de sus suscriptores, almacenada en los Centros de Datos de ETB. Dentro de los sistemas y equipos se tienen:

Firewalls e IPS: ETB cuenta con sistemas de protección perimetral para sus plataformas de servicios IP replicados en cada Centro de Datos de ETB como ISP.

Sistema AVAS: Que protege a los clientes del servicio de Correo Electrónico alojados en ETB contra Virus y Spam.

Plataforma de Análisis de Vulnerabilidades para la identificación y evaluación periódica del riesgo sobre las infraestructuras de red y de servicios de ETB.

Sistema de Filtrado Pornografía Infantil y Phishing: bloquea las URL listadas por PoNAL y el MinTics, que proveen contenidos que atentan contra la infancia de acuerdo con la Ley 679 de 2001.

Redundancia geográfica para las plataformas que habilitan la prestación del servicio de Internet. Así como para los servidores HLR/HSS, que realizan la autenticación y autorización de los usuarios del servicio de Planes de Datos Móviles.

Seguridad EndPoint. Brinda la seguridad basada en host para servidores que hacen parte de la infraestructura de ETB y clientes de DataCenter, como parte de la estrategia de mitigación ante ataques horizontales.