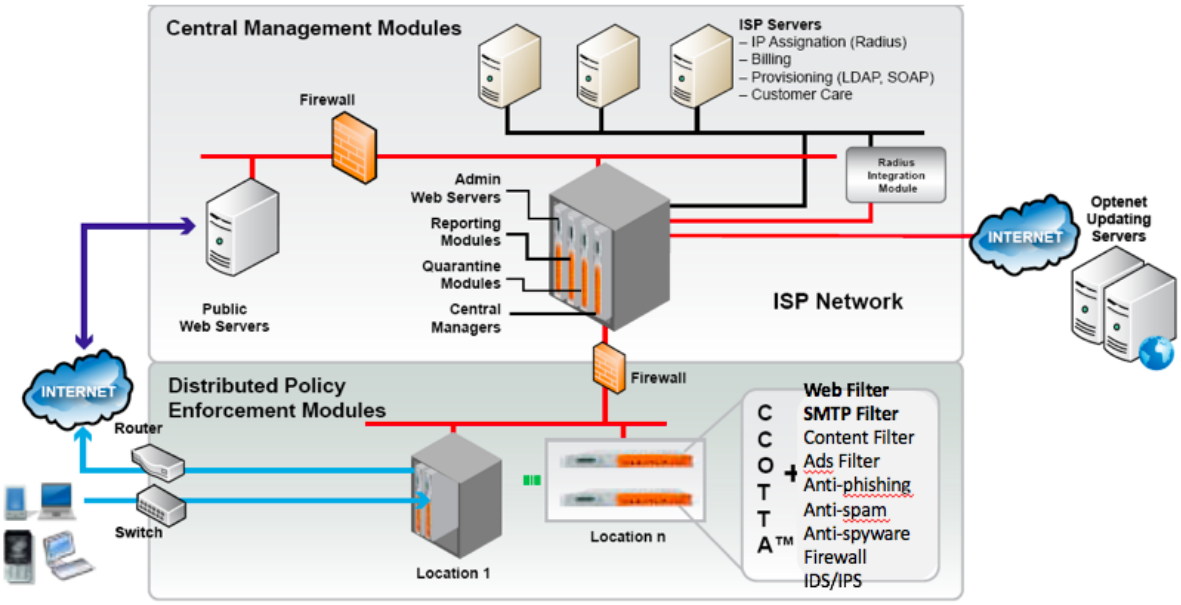
AUDITORIA MINT TIC

Acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtro antivirus, prevención del spam, phishing y malware.

Los procedimientos mediante los cuales la GUENT implementa modelos de seguridad, para los usuarios de internet son asumidos por diferentes plataformas, las cuales se pueden ver resumidas en la siguiente imagen: Plataformas de servidores del ISP, Firewall's, equipos de filtrado de contenido entre otros.



Proyectos en proceso: Servicio de no repudio

En el 2018, se realizaron las reservas presupuestales para invertir en certificados SSL para ciertos dominios de la GUENT y dominios que se desprenden de EMCALI, en donde se garantizara la compatibilidad con todos los Navegadores. Estos certificados permitirán validar toda la información que se encuentre alojada dentro del servidor que haga referencia el dominio a ser protegido. Dentro de las funcionalidades se encuentra el de verificar la ruta de acceso a la plataforma de pagos en línea que se utilice verificando que esta es una conexión segura para realizar pagos. Esta inversión aplica para dominio y subdominios de EMCALI y permite el cambio de protocolo HTTP a HTTPS usando Certificado de 2048 bits y hasta 256 bits de encriptación de serie.

Procedimientos mediante los cuales se implementan modelos de seguridad

- **Autenticación**
  EMCALI protege a sus clientes mediante un esquema de seguridad por capas, donde se incluye segmentación de redes y Vlan's en las etapas de acceso y transporte, así como con el aseguramiento y verificación de los usuarios para el caso de los servicios xDSL, donde se usa el esquema de autenticación a través de servidores Radius. Servidores que están centralizados en los data center de EMCALI donde la plataforma hace las tres funciones: autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting).

- **Acceso**
  Para el servicio de Acceso a Internet se usa un control de acceso por puerto físico y se cuenta con controles de acceso por software diseñados específicamente de acuerdo a lo contratado por los usuarios y a las funcionalidades provistas por el software RADIUS y/o tecnología utilizada, asegurando que sólo usuarios autorizados puedan ingresar para efectuar las tareas requeridas.

  En los Servicios de Internet xDSL, se implementan mecanismos de control de acceso con protocolos y configuraciones de enrutamiento que permiten identificar y autenticar la conexión de cada usuario previa validación de su cuenta y puerto de conexión, asegurando que solo clientes verificados tendrán acceso al servicio y podrán utilizarlo

- **Servicio registro**.
  Con esta funcionalidad, las conexiones y desconexiones de nuestros usuarios son registradas y permiten validar la evidencia de la identidad del usuario que hace uso del servicio.

  Para los servicios de Internet instalados con diferentes medios de acceso físico, se almacenan los registros CDRs que registran la cantidad de tráfico de datos del suscriptor así como el 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 EMCALI hace uso de los registros de eventos o “log’s” producidos por las plataformas de seguridad, para apoyar la resolución de incidentes, que puedan afectar los servicios prestados.

También los “log’s” generados por las plataformas de seguridad como los firewalls 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.

- **Principio de confidencialidad de datos**
  Todas las personas que en Nodo de internet, administren, manejen, actualicen o tengan acceso a informaciones de cualquier tipo que se encuentre en Bases de Datos, están obligadas a garantizar la reserva de la información, por lo que se comprometen a conservar y mantener de manera estrictamente confidencial y no revelar a terceros, toda la información que llegaren a conocer en la ejecución y ejercicio de sus funciones; salvo cuando se trate de actividades autorizadas expresamente por la ley de protección de datos.

- **Principio de integridad de datos**
  EMCALI provee una red MULTISERVICIOS 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.

- **Principio de disponibilidad**
  Los servicios se apoyan en una estructura de red multiservicios 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 puntos de conexión internacional a Internet. Esta infraestructura de red está protegida por firewall’s y apoyada por plataformas de servicios IP como servidores DNS, servidores de RADIUS alojados en los data center para dar redundancia geográfica asegurando una alta disponibilidad del servicio en todo momento entregando al cliente la mejor experiencia de navegación.

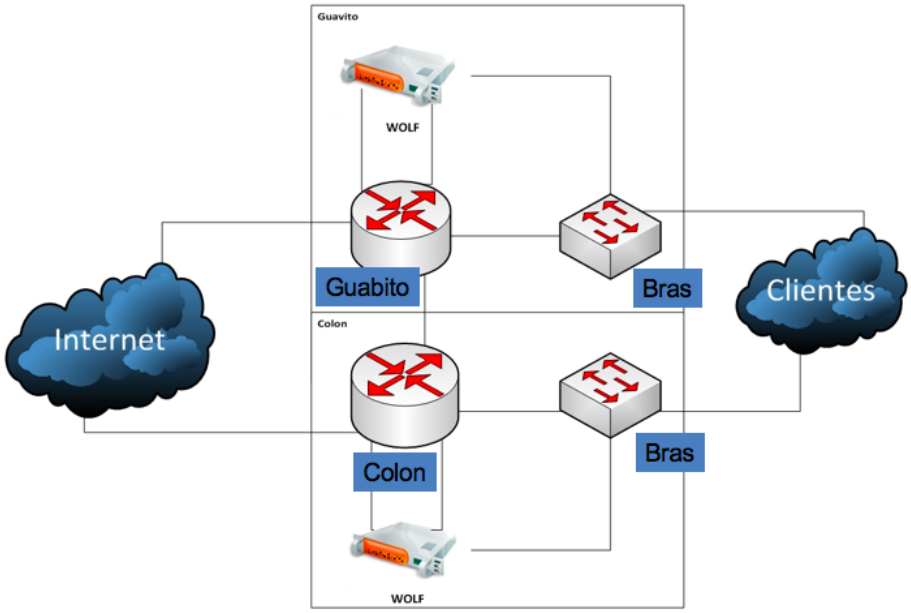
Modo bloqueo páginas con contenido de pornografía infantil

De forma resumida la solución de filtrado de pornografía infantil consiste en 2 servidores distribuidos físicamente en los centros de datos de COLÓN y GUABITO ubicados en la ciudad de Santiago de Cali, en el Valle del Cauca los cuales filtran todos los contenidos de internet de EMCALI.

El primer paso llevado a cabo es el establecimiento de la sesión BGP contra el router de BORDE, una vez la sesión BGP es establecida, el servidor hace resolución DNS de las url's de pornografía infantil con el fin de obtener las direcciones IP's de los servidores que albergan estas url's, una vez se obtienen las direcciones IP'S, el servidor envían un paquete de actualización BGP anunciando las IPS a los routers de borde COLÓN y GUABITO contra los que se han establecido sesión.

Cuando un cliente hace un requerimiento http y este es desviado hacia la solución de filtrado, esta petición es revisada, si la petición de la página http tanto la IP como la url son coincidentes, el trafico debe ser bloqueado y por consiguiente cerrar la conexión no dejando visualizar la página al cliente final. Si la petición es coincidente en IP pero no en URL, esta es dirigida hacia internet.

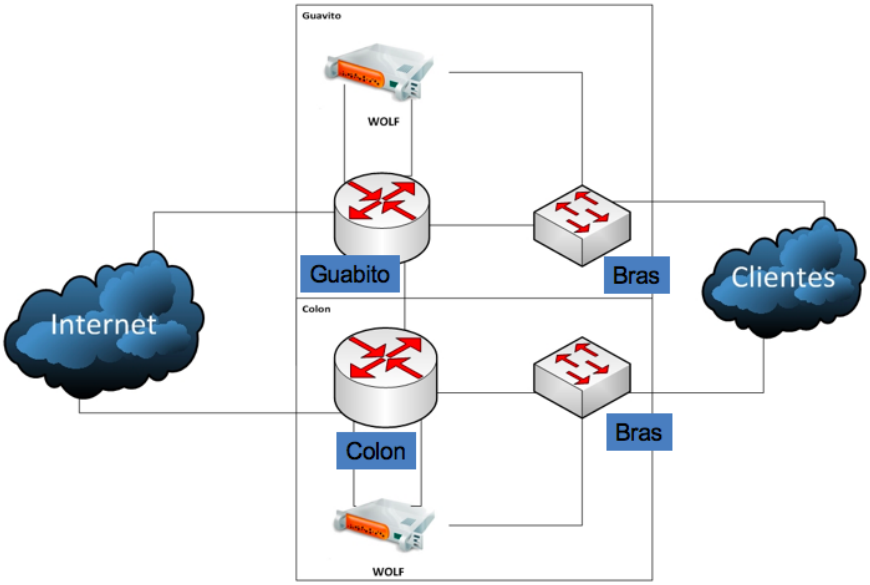
La plataforma de filtrado legal WOLF (fabricante ALLOT antes Optenet), se implementa como mecanismo para el cumplimiento de la ley 679 de 2001, La arquitectura que se observa en la imagen adjunta, ilustra en resumen los principales componentes que conforman la solución:



Información sobre los mecanismos de filtrado para prevenir y contrarrestar el acceso de pornografía a los menores de edad.

Mecanismos de filtrado

La plataforma de filtrado legal WOLF (fabricante ALLOT antes Optenet), se implementa como mecanismo para el cumplimiento de la ley 679 de 200, La arquitectura que se observa en la imagen adjunta, ilustra en resumen los principales componentes que conforman la solución:



Sistemas internos de seguridad, encaminados a evitar el acceso no autorizado

EMCALI posee firewall's del fabricante fortinet instalados en Cluster los cuales protegen la red NGN, estos tienen configuradas políticas de inspección profunda de todos los paquetes de datos que circulan por la red de los servidores, evitando la propagación de virus y denegando accesos no solicitados. Para Cada servidor se aplican políticas definidas por puerto de forma que se pueda inspeccionar todo nivel de conexión a la aplicación que se está protegiendo.

Los servicios más críticos que ofrece la plataforma son para protegen los servidores de internet de EMCALI, para los clientes internos, clientes externos, servicios propios de infraestructura como DNS usuarios masivo, DHCP usuarios masivo, RADIUS usuarios masivo, Correo usuarios masivo, Hosting usuarios masivo, VPNs, etc. Estos son elementos fundamentales que han permitido tener una estabilidad cercana al 99.999%, en los últimos seis años de estar implementada la plataforma.

Sistemas internos de para la red, encaminados a evitar el acceso no autorizado

EMCALI posee firewall's del fabricante fortinet instalados en Cluster los cuales protegen la red NGN, estos tienen configuradas políticas de inspección profunda de todos los paquetes de datos que circulan por la red de los servidores, evitando la propagación de virus y denegando accesos no solicitados. Para Cada servidor se aplican políticas definidas por puerto de forma que se pueda inspeccionar todo nivel de conexión a la aplicación que se está protegiendo.

Los servicios más críticos que ofrece la plataforma son para protegen los servidores de internet de EMCALI, para los clientes internos, clientes externos, servicios propios de infraestructura como DNS usuarios masivo, DHCP usuarios masivo, RADIUS usuarios masivo, Correo usuarios masivo, Hosting usuarios masivo, VPNs, etc. Estos son elementos fundamentales que han permitido tener una estabilidad cercana al 99.999%, en los últimos seis años de estar implementada la plataforma.

Están configurados en modo cluster, y esto ha permitido una alta capacidad y respuesta inmediata de la plataforma. Ubicados en la telefónica de Colón y Guabito donde han brindado la disponibilidad para todos los servicios de internet que actualmente soporta el proveedor de servicios de telecomunicaciones de EMCALI E.I.C.E E.S.P.

Para la operación de la normal prestación del servicio de internet se requiere que funcione de manera ininterrumpida los filtros de seguridad aplicados en más de 1.600 políticas generadas, 1.234 objetos, además de traslaciones internas configuradas. Los recursos de CPU se hallan entre el 1 y 3% máximo, con un 52% memoria, hablan del eficiente desempeño de la plataforma que Ingeniería concibió para el ISP (proveedor de servicios de internet de la GUENT). Igualmente se cuenta con una plataforma de Forti-Analizer que nos muestra los flujos de datos que son egresados y recibidos por la plataforma, para sus respectivos análisis e informes ante solicitudes de los entes de control.

El Departamento Multiservicios, soporta en su mantenimiento y operación todo lo concerniente a la normal prestación del servicio de Internet de la GUENT, el DNS es imprescindible para ofrecerlo y consta de una plataforma de 6 servidores distribuidos en los centros de datos de LIMONAR y SANFERNANDO y están a cargo de la resolución de nombres para todos los usuarios que utilizan la plataforma de Internet a través de los canales internacionales y su funcionalidad básica comprende el hacer uso de la resolución de nombres de dominio a las

direcciones IPv4 y no solo resuelven los dominios propios alojados en el ISP, sino a los dominios que se hallan en internet.

Este proceso le permite a nuestros usuarios tener una plataforma segura, desde que estén usando los servicios de resolución de nombres de EMCALI E.I.C.E E.S.P., con sus sistemas de nombres de cache los cuales son utilizados para resolver nombres de dominios ajenos a nuestra plataforma y que corresponde al 99.999% de todo lo que utiliza el internet y tan sólo una pequeña fracción para los dominios alojados en nuestra plataforma pero no menos importante, ya que sin esta resolución autoritaria no podríamos hacer presencia en internet como un ISP propiamente. Este servicio se presta para los aproximadamente 100.000 usuarios que tenemos en el internet masivo y grandes clientes, siendo un servicio básico asignado para garantizar una navegación confiable y rápida.

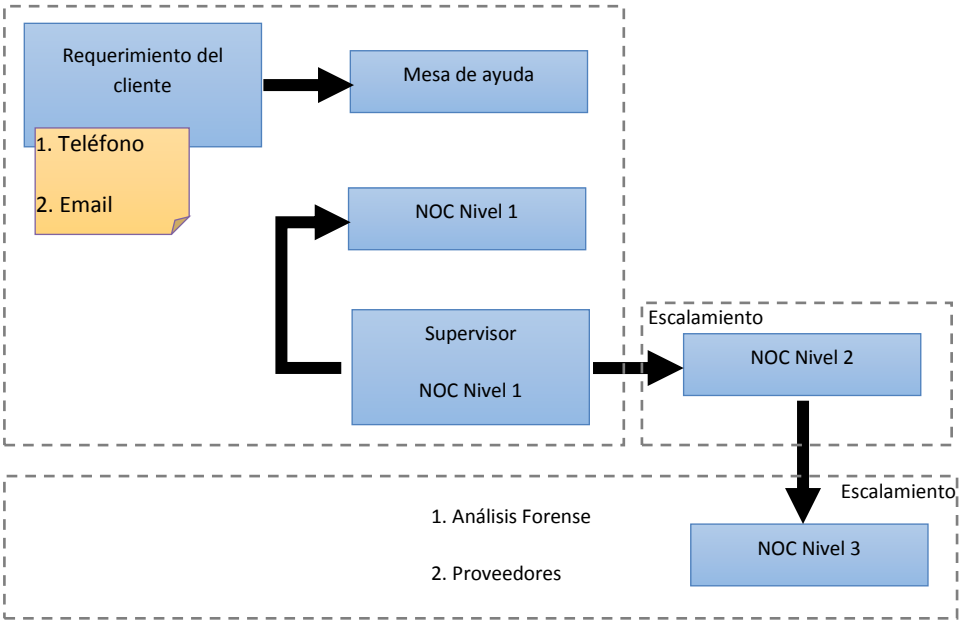
Infraestructura, técnicas de control, basadas en la clasificación de contenidos que tengan como objetivo fundamental evitar el acceso a sitios con contenidos de pornografía infantil

Los servidores tienen bloqueado el acceso a internet por default y se habilita en el firewall el acceso sólo a los protocolos o puertos que lo requiera. Ejemplo salida para consulta a DNS. Salida para envío de correo o salida a determinados sitios para actualizaciones.

En el caso del servidor de los hosting. Este utiliza cpanel y frecuentemente actualiza las versiones de apache, php, msql y librerías con el objetivo de mantenerse seguro y evitar vulnerabilidades que permitan que intrusos coloque contenidos no autorizados.

Soportes de la documentación y procedimientos de las herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de las redes

Los procesos de atención al cliente siguen el siguiente diagrama:



Como se detalla en el ítem número 8, la prevención de fraudes y controles depende de varias plataformas y cada una de ellas puede iniciar la alerta sobre un evento o un ataque perpetrado o en su etapa más crítica, se detecta trafico invalido que ataca otros clientes desde o en dirección a redes IPV4, para la GUENT el éxito en la detección y solución rápida de eventos de seguridad informática se da con la participación activa del usuario afectado, por lo que cada caso detectado se investiga y clasifica por los funcionarios del nodo de internet, según el tipo de ataque se realiza un análisis forense y se contacta al usuario para darle las instrucciones que necesita seguir para remediar la vulnerabilidad o el ataque y para prevenirlo en un futuro.

Recomendaciones de Seguridad:

Emcali recomienda implementar seguridad informática en sus equipos con antivirus como **ESET INTERNET SECURITY**