UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO – CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

MENCIÓN TELEMÁTICA

GESTIÓN DE SEGURIDAD EN LA RED DE DATOS DE LA CORTE CONSTITUCIONAL MEDIANTE EL DISEÑO DE UN CSIRT (EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD)

TESIS PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERO DE SISTEMAS

HERNÁN ANDRÉS ARMAS MEDINA

DIRECTOR ING. JORGE LÓPEZ

Quito, Agosto 2012

DECLARACIÓN

Yo Hernán Andrés Armas Medina, declaro bajo juramento que el trabajo aquí descrito es de mí autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

_____

Hernán Andrés Armas Medina

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Hernán Andrés Armas Medina bajo mi dirección.

_____

Ing. Jorge López

Director de Tesis

AGRADECIMIENTOS

Para lograr este objetivo, primeramente agradezco a la Corte Constitucional, por abrirme las puertas de la entidad y facilitarme el desarrollo del presente proyecto de titulación, principalmente al Departamento de Tecnología, representado por el Ing. Gabriel Novoa como Director del mismo, y al grupo de amigos que son parte del departamento ya que nunca me negaron ningún tipo de apoyo, para todos ellos Gaby, Marco, Edwin, Víctor y Ángel, un agradecimiento muy especial.

En segundo lugar agradezco a mi Director de Tesis, el Ing. Jorge López, porque semana a semana supo guiarme con sus consejos para cumplir el objetivo final que es la presentación de este proyecto de tesis.

Y por último pero no por ello menos importante, agradezco a Dios, a mi Abuelita, a mi Abuelito, a mi tío Edison, a mi tía Sonia y a mi tío Fabián, que desde el cielo me han dado esa fuerza espiritual para continuar, a mi familia, tíos/as, primos/as, que siempre han estado presentes con el ánimo necesario para seguir adelante, a mí novia Pame por su respaldo diario y su ayuda incondicional, a Fer, porque ha sido ese apoyo dentro de casa, pero principalmente a mis Padres, mi Papá que siempre me ha aconsejado y nunca me ha dejado solo, y por supuesto como no, a mi Mamita, que es la persona más incondicional, más fuerte y más luchadora, que siempre ha confiado en mí y que es la razón principal para intentar conseguir este objetivo.

Hernán

DEDICATORIA

Este proyecto está dedicado a la memoria de mis Abuelitos, Tía y Tíos que desde el cielo nos cuidan y siempre permanecerán en mi corazón, a mis tíos, tías, primos, primas, mi novia y Fer, que están presentes conmigo para compartir este momento de felicidad y que son indispensables en mi vida.

Pero principalmente se encuentra dedicado para mi Padre y Madre, para mi papá, porque siempre ha confiado en mí y me lo ha demostrado con su apoyo incondicional, y para mi mamita, que es la razón principal por la que lucho a diario para ser alguien mejor, por estas razones es que este logro es para ustedes, porque los Amo.

Hernán

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El presente trabajo de tesis consta de los siguientes temas que serán resumidos a continuación:

Capítulo 1. En primera instancia se analizarán los antecedentes relacionados con la Corte Constitucional como, su misión, visión y objetivos dentro de la estructura jurisdiccional del Ecuador, con el fin de representar un servicio para los usuarios, así como también, se detallará su estructura organizacional y su estructura orgánica por procesos, que son los pilares fundamentales para el buen funcionamiento de la entidad, pero principalmente, el estudio se enfocará en la problemática del Departamento de Tecnología y su necesidad de reforzar la seguridad de la red de datos que poseen actualmente, con referencia a lo propuesto en su POA y en su Plan de Fortalecimiento de Infraestructura Tecnológica para el año 2012, respaldando todo este proceso con las respectivas leyes que rigen las implementaciones e investigaciones tecnológicas dentro del sector público y que servirán como punto de partida.

Capítulo 2. El análisis de la situación actual de la red de datos de la Corte Constitucional aclarará los detalles sobre la distribución de la infraestructura, para realizar este proceso se utilizará el modelo TCP/IP dividiéndolo de la siguiente forma, la capa de enlace y la capa de internet, en donde se analizarán todos los detalles sobre servidores, enlaces de internet y datos, cableado estructurado, equipamiento tecnológico de interconexión y la distribución entre el edificio principal y sus oficinas regionales, a continuación, la capa transporte, en donde se estudiarán tanto los protocolos como el enrutamiento utilizado dentro de la institución para brindar conectividad entre estaciones de trabajo, dispositivos y servidores, y por último, la Capa Aplicación, en donde se analizarán detalles sobre el tráfico de red con referencia a los servicios que corren diariamente, incluyendo datos estadísticos sobre la tasa de transferencia de la red, las visitas a la página web oficial de la entidad y el promedio de mails enviados y recibidos.

Capítulo 3. Aquí se realizará el análisis de riesgos y vulnerabilidades en la red de datos de la Corte Constitucional, que constará de una introducción teórica sobre lo que es riesgo y lo que es vulnerabilidad, para posteriormente seleccionar 5 direcciones IPs de distintos servicios, de las cuales, 2 se utilizarán solo para análisis de vulnerabilidad y las 3 restantes para las pruebas de vulnerabilidad e intrusión que servirán como muestra para respaldar el estudio de seguridad, para realizar este proceso se intentará generar pruebas de acceso utilizando el sistema operativo Backtrack, con el objetivo de demostrar que pueden existir fallas de seguridad en la red y que estas pueden ser explotadas, para posteriormente proceder a mencionar métodos de mitigación y solución a los problemas detectados; backtrack posee herramientas para escanear dispositivos conectados a la red, escanear vulnerabilidades y escanear puertos, así como también, aplicaciones para crear intentos de ataques de fuerza bruta o ataques de tipo diccionario con el propósito de obtener credenciales de seguridad, que ayudarán con la vulneración de servicios, pero principalmente se intentará ingresar al servidor web para modificar su contenido, ya que este, es uno de los principales servicios a ser atacado por los piratas de la red.

Capítulo 4, en esta sección se abordará el tema sobre lo que es un CSIRT como método de innovación en seguridad, se mencionarán todos los detalles que conciernen al diseño de este tipo de equipos de respuesta ante incidentes, el objetivo de esta metodología es poder incrementar la gestión de seguridad, para esto primeramente se definirá de forma conceptual lo que es un CSIRT y su propósito de seguridad dentro de una organización, para luego, dar una introducción sobre los servicios proactivos y reactivos que es capaz de brindar en favor de la seguridad de la información, con este antecedente se detallarán los distintos tipos de CSIRT que es posible implementar dependiendo del sector empresarial y los servicios que sean necesarios de acoplar, y por último, se especificarán las distintas estructuras para escoger a los miembros del equipo que serán los responsables de cumplir con labores de investigación, respuesta y mitigación de los daños detectados, priorizando la labor proactiva.

Capítulo 5, con el respaldo de capítulos precedentes y como culminación de este trabajo de investigación, se diseñará un modelo de CSIRT para la Corte Constitucional, con el fin de fortalecer de manera proactiva los procesos de seguridad que tiene actualmente el Departamento de Tecnología, para comenzar con este diseño primeramente se realizará la comparación entre la metodología propia del CSIRT y la de ISACA para evaluar cual de las dos es la más convenientes tomando en cuenta el objetivo del negocio de la entidad, luego de exponer los 2 modelos, se escogerá uno de ellos con sus respectivas justificaciones, para posteriormente poder realizar el diseño contemplando detalles como: el sector en el que se desarrollará, los integrantes del equipo de respuesta con sus respectivas funciones y responsabilidades, así como también, su misión, visión y los servicios que proveerá a las personas que se beneficiarán con este diseño de equipo de respuesta ante incidentes de seguridad.

PRESENTACIÓN

Actualmente la seguridad de la información debería ser el tema principal para el desarrollo tecnológico de una empresa, pero usualmente no se le presta la importancia que merece exponiendo la infraestructura a distintos tipos de ataques, por esta razón, es que gran parte de las entidades ya sean públicas o privadas creen que nunca serán víctimas de un suceso como este, y no crean planes de contingencia para responder ante estos inconvenientes si es que llegaran a ocurrir, especialmente tomando en cuenta la constante evolución de las herramientas tecnológicas que existirán posteriormente.

Por estos motivos y priorizando el tipo de información que se maneja en la Corte Constitucional y a sus responsabilidades de justicia a nivel nacional, se ha visto la necesidad de realizar un análisis sobre las vulnerabilidades que pueda presentar la red de datos, y de esta forma, poder encontrar las respuestas más óptimas para mitigar los daños encontrados en el menor tiempo posible, pero sobre todo, que sirva como antecedente para seguir implementando este tipo de estudios en la infraestructura.

Una de las estrategias que se está utilizando dentro de las empresas para lograr una correcta gestión de la seguridad de la información, es la creación de Equipos de Respuesta a Incidentes de Seguridad CSIRT, este tipo de equipos se encarga de buscar las mejores estrategias para garantizar la protección de la información y sobre todo de brindar servicios proactivos y reactivos para el manejo de incidencias, esta metodología se la está implementando a nivel mundial obteniendo excelentes resultados por sus métodos de detección y respuesta.

Con todo este antecedente, es que el presente trabajo de investigación busca dejar planteado el diseño de un CSIRT para la Corte Constitucional, que sirva como modelo para contribuir con la seguridad que tiene actualmente la institución, tomando en cuenta aspectos como, el tipo de equipo a implementar, los servicios que brindará a la institución y la comparación respectiva con respecto a la metodología que se deberá utilizar para lograr una adecuada gestión de seguridad

CAPITULO 1

CORTE CONSTITUCIONAL

1.1 ANTECEDENTES CORTE CONSTITUCIONAL [1]

Hasta principios del año 2008 la Corte Constitucional era conocida como Tribunal Constitucional, pero con la publicación de la Constitución de la República el 20 de octubre del 2008, ésta adopta el nombre de Corte Constitucional, con la cual todos los bienes del antiguo Tribunal se transfirieron a la Corte, así como su personal de funcionarios y empleados; por lo tanto en la actualidad la Corte es la entidad responsable y garante de la justicia constitucional[1] del Ecuador.

Por esta razón el artículo 429 de la Constitución de la República, nombra a la Corte Constitucional como el máximo órgano de control, interpretación constitucional y administración de justicia en esta materia. Esta entidad ejercerá jurisdicción[2] a nivel nacional, con su sede en Quito. Los valores institucionales que promulga la Corte Constitucional son:

Figura 1.1: Valores institucionales
Autor: Corte Constitucional
Fuente: http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=353&Itemid=7

[1] **Constitución,** es la norma suprema, escrita o no, de un Estado soberano u organización, establecida o aceptada para regirlo. Obtenido de, http://es.wikipedia.org/wiki/Constituci%C3%B3n.
[2] **Jurisdicción,** es la potestad de aplicar el Derecho en el caso concreto, resolviendo de modo definitivo e irrevocable una controversia. Obtenido de, http://es.wikipedia.org/wiki/Jurisdicci%C3%B3n

En cuanto a su estructura orgánica, la Corte Constitucional estará integrada por nueve miembros con títulos de jueces y se desempeñarán en sus cargos por un período de nueve años, sin reelección inmediata y serán renovados cada tres años.

Con respecto a la estructura de la Administración de Justicia Constitucional, de acuerdo con la Ley de Garantías Jurisdiccionales y Control Constitucional, la justicia constitucional comprende:

1. Los juzgados de primer nivel
2. Las Cortes Provinciales
3. La Corte Nacional de Justicia
4. La Corte Constitucional

La Corte Constitucional también cuenta con 8 oficinas denominadas Regionales, distribuidas de tal manera que puedan acoger cualquier inquietud de la ciudadanía a lo largo del territorio nacional, las oficinas regionales se encuentran en las provincias de:

- Esmeraldas,
- Imbabura,
- Manabí,
- Chimborazo,
- Guayas,
- Azuay,
- El Oro, y
- Loja

Las personas que vivan fuera de la ciudad de Quito, deberán acercarse a cualquiera de las oficinas regionales más cercana a su localidad para poder presentar sus denuncias e inquietudes, y de no poder ser resueltas ahí mismo serán direccionadas a Quito para buscar la solución más efectiva.

1.1.1 MISIÓN

La misión de la Corte Constitucional para poder desempeñar sus funciones es:

"Garantizar la vigencia y supremacía de la Constitución, el pleno ejercicio de los derechos constitucionales y garantías jurisdiccionales, mediante la interpretación, el control y la administración de justicia constitucional"[3].

1.1.2 VISIÓN

La visión con la que trabaja la Corte Constitucional es:

"La Corte Constitucional será un órgano autónomo e independiente de administración de justicia constitucional, de reconocido prestigio nacional e internacional".

1.1.3 OBJETIVOS [2]

Los objetivos de la Corte Constitucional han sido desarrollados para ayudar a los usuarios y estos son:

1. Ser el máximo órgano de interpretación de la Constitución, de los tratados internacionales de derechos humanos, ratificados por el Estado ecuatoriano, a través de sus dictámenes.
2. Declarar de oficio la inconstitucionalidad de normas conexas[4], cuando en los casos sometidos a su conocimiento concluya que una o varias de ellas son contrarias a la Constitución.
3. Conocer y resolver, a petición de parte, las acciones por incumplimiento que se presenten con la finalidad de garantizar la aplicación de normas o actos administrativos de carácter general, cualquiera que sea su naturaleza o jerarquía, así como para el cumplimiento de sentencias o informes de organismos internacionales de protección de derechos humanos que no sean ejecutables por las vías judiciales ordinarias.

---

[3] **Misión, Visión y Objetivos,** son conceptos que hacen referencia a la estructura y organización de la Corte Constitucional del Ecuador. Obtenidos en, http://www.corteconstitucional.gob.ec.

[4] **Conexas,** de la cosa que está enlazada o relacionada con otra. Obtenido de, http://es.thefreedictionary.com /conexas.

4. Expedir sentencias que constituyan jurisprudencia[5] vinculante respecto de las acciones de protección, cumplimiento, hábeas data[6], acceso a la información pública y demás procesos constitucionales, así como los casos seleccionados por la Corte para su revisión.
5. Dirimir conflictos de competencias o de atribuciones entre funciones del Estado u órganos establecidos en la Constitución.
6. Efectuar de oficio y de modo inmediato el control de constitucionalidad de las declaratorias de estados de excepción, cuando impliquen la suspensión de derechos constitucionales.
7. Conocer y sancionar el incumplimiento de sentencias y dictámenes constitucionales, aspecto relacionado directamente con la reparación integral.
8. Conocer acciones extraordinarias de protección contra sentencias, autos definitivos, resoluciones con fuerza de sentencia.
9. Emitir dictámenes previos y vinculantes de constitucionalidad en los siguientes casos, además de los que determine la ley.

1.1.4 CENTRO DE ESTUDIOS Y DIFUSIÓN DEL DERECHO CONSTITUCIONAL [3]

A partir del año 2008 y ya con la Constitución vigente, la Corte Constitucional, además de sus atribuciones jurisdiccionales, se le agrega una nueva función que es la de impulsar en el Ecuador el modelo constitucional garantista y contribuir al cambio de la cultura jurídica ecuatoriana[7].

En otras palabras la Corte Constitucional tiene la misión de promover y desarrollar la investigación jurídica en áreas tales como Teoría Constitucional, Derechos Constitucional Comparado y Ecuatoriano, Derechos Humanos e Historia del Derecho, e impulsar procesos de formación, capacitación entre los jueces, fiscales y operadores jurídicos del país, así como difundir los contenidos constitucionales

[5] **Jurisprudencia,** es el conjunto de sentencias que han resuelto casos iguales o similares de la misma manera o en el mismo sentido. Obtenido de http://es.wikipedia.org/wiki/Jurisprudencia.
[6] **Habeas data,** es el derecho en ejercicio de una acción constitucional, que tiene cualquier persona que figura en un registro, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio. Obtenido, http://es.wikipedia.org/wiki/Habeas_data
[7] **Centro de Estudios y Difusión del Derecho Constitucional,** concepto textual obtenido de la página oficial de la Corte Constitucional, http://www.corteconstitucional.gob.ec

entre la ciudadanía, y para realizar toda esta labor es que se creó el “Centro de Estudios y Difusión del Derecho Constitucional”

Con la creación del Centro de Estudios y Difusión del Derecho Constitucional se podrá dar un mayor sustento teórico y académico a las sentencias que emitan los jueces de la Corte, y en el mediano plazo se constituirá en un centro de generación de pensamiento en temas constitucionales a nivel Latinoamericano.

1.1.5 ESTRUCTURA ORGANIZACIONAL [4]

Con respecto a la estructura interna de la Corte Constitucional[8], de conformidad con la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y el Reglamento de Sustanciación de Procesos de Competencia de la Corte Constitucional, se encuentra organizada de la siguiente manera:

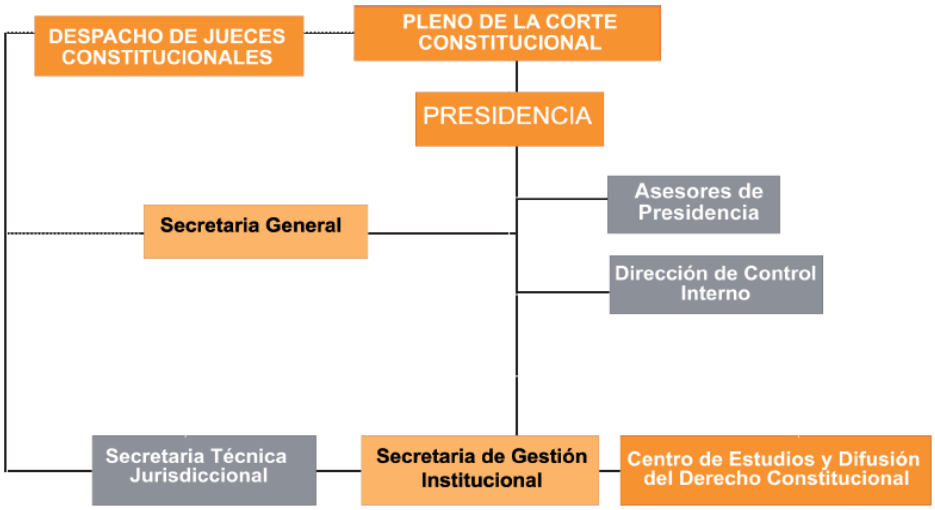


Figura 1.2: Estructura Organizacional
Autor: Corte Constitucional
Fuente: http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=54&Itemid=27

1. Pleno de la Corte Constitucional
2. Sala de admisión
3. Sala de selección de procesos constitucionales
4. Sala de revisión de procesos constitucionales
5. Presidencia

[8] **Estructura Organizacional de la Corte Constitucional,** información adjunta obtenida de, http://www.corteconstitucional.gob.ec.

6. Secretaría General
7. Secretaría Técnica Jurisdiccional y órganos de apoyo
8. Centro de Estudios Constitucionales.

Como se muestra en la Figura 2, La Corte Constitucional está integrada por un Presidente, Dr. Patricio Pazmiño Freire; el pleno está integrado por jueces que desarrollarán su función a través de tres salas: Admisión, Selección y Revisión; y, el personal técnico/administrativo, que trabajan y ejercen el mandato con responsabilidad y en total apego a la Constitución del Ecuador.

1.1.6 ESTRUCTURA ORGÁNICA POR PROCESOS

La Estructura Orgánica por Procesos es un reglamento que tiene por objeto establecer la estructura, los procesos y definir los mecanismos de gestión organizacional de la Corte Constitucional.

Para comprender como fue desarrollada la estructura por procesos de la Corte Constitucional se debe tener en cuenta el significado de los siguientes conceptos:

a) Macro Proceso: Conjunto de dos o más procesos que se orientan a cumplir un objetivo común.

b) Proceso: Conjunto de actividades relacionadas entre sí, que emplean insumos y les agregan valor, a fin de entregar un bien o servicio a un usuario interno o externo, utilizando recursos de la Institución.

c) Subproceso: Conjunto de actividades relacionadas entre sí, que producen un bien o servicio que se integra o complementa a otro producto de mayor valor agregado.

d) Producto: Bien o servicio que genera la institución y que entrega a un usuario interno o externo.

e) Usuarios: Personas naturales y jurídicas, públicas y privadas.

Los procesos que generan los servicios de la Corte Constitucional se ordenan y clasifican en función de la contribución o beneficio que aportan al cumplimiento de la misión institucional, por lo tanto, y para cumplir con estos requerimientos los procesos son los siguientes:

- Procesos gobernantes,
- Procesos generadores de valor,
- Procesos habilitantes de asesoría, y
- Procesos habilitantes de apoyo.

Procesos Gobernantes

Figura 1.3: Procesos Gobernantes
Autor: Corte Constitucional
Fuente: http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=54&Itemid=27

Los procesos gobernantes dentro de la Corte Constitucional son:

1. El direccionamiento estratégico se encuentra bajo la responsabilidad del Pleno de la Corte Constitucional; y,

2. La gestión estratégica está a cargo de la Presidencia de la Corte Constitucional.

Procesos Generadores de Valor

Figura 1.4: Procesos Generadores de Valor
Autor: Corte Constitucional
Fuente: http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=54&Itemid=27

Los procesos generadores de valor dentro de la Corte Constitucional son:

1. La administración de Justicia Constitucional, está a cargo del Pleno, Juezas y Jueces de la Corte Constitucional; dentro de este proceso a su vez se encuentran las tres salas[9] que son:

Sala de admisión.- está encargada de calificar y admitir la procedencia de acciones constitucionales en los casos y términos establecidos en la ley. Esta sala estará integrada por tres juezas o jueces, que actuarán mensualmente de manera rotativa.

Sala de selección.- está encargada de sentencias en materia de garantías jurisdiccionales y las resoluciones de medidas cautelares, las decisiones que se tomen dentro de la ésta sala serán discrecionales y no cabrá ningún recurso contra ellas. De la misma manera la Sala de Selección estará compuesta por tres juezas o jueces que actuarán mensualmente de manera rotativa.

Sala de revisión.- la labor de esta sala será la revisión de sentencias de protección, cumplimiento, hábeas corpus[10], hábeas data, acceso a la información pública y resoluciones de medidas cautelares, la Corte Constitucional tendrá salas de revisión de procesos, compuestas cada una, por tres juezas o jueces designados por el Pleno para cada caso, de manera rotativa y al azar. Cada una de estas salas estará presidida por una de las tres juezas o jueces de la respectiva sala.

2. La Gestión de Investigación bajo la responsabilidad del Centro de Estudios y Difusión del Derecho Constitucional, que tiene la labor de:

a) **Investigar.-** nuevos avances en materia constitucional y jurídica.
b) **Formación y capacitación.-** de los integrantes del centro de estudios.
c) **Publicaciones.-** de los avances encontrados para informar a la sociedad.
d) **Biblioteca Constitucional.-** mantener al día la biblioteca de la entidad.

[9] **Sala de admisión, selección y revisión,** información obtenida de, http://www.corteconstitucional.gob.ec
[10] **Habeas corpus,** es una institución jurídica que garantiza la libertad personal del individuo, con el fin de evitar los arrestos y detenciones arbitrarias. Obtenido en, http://es.wikipedia.org/wiki/H%C3%A1beas_corpus.

Procesos Habilitantes

Los procesos habilitantes se dividen en Asesoría y Apoyo:

Figura 1.5: Procesos Habilitantes
Autor: Corte Constitucional
Fuente: http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=54&Itemid=27

Los procesos habilitantes de asesoría son:

1. La Secretaria Técnica Jurisdiccional se encarga de brindar asesoría Jurisdiccional a las Juezas, Jueces, Salas y al Pleno de la Corte Constitucional, gracias a sus diferentes procesos que son:

- Proceso asistencia técnica de admisión,
- Proceso asistencia técnica de sustanciación,
- Proceso asistencia técnica de selección, y
- Proceso asistencia técnica de revisión.

2. La Gestión de Control Interno, que se encuentra bajo la responsabilidad de Auditoría Interna de la Corte.

Los Procesos habilitantes de apoyo son:

1. La Secretaría General se encarga de la gestión operativa al despacho de los procesos jurisdiccionales y la generación de la información histórica jurisdiccional para su publicación y difusión. La Secretaría General tiene a su cargo los siguientes procesos:

- Proceso operacional y de despacho a los procesos jurisdiccionales,
- Proceso de prosecretaria,
- Proceso de seguimiento de sentencias y dictámenes constitucionales,
- Proceso de relatoría,
- Proceso documentología, archivo y reproducción, y
- Proceso oficinas regionales

2. La Secretaría de Gestión Institucional tiene a su cargo la gestión de recursos humanos, materiales tecnológicos, comunicacionales, financieros y de asesoría legal. Sus procesos son los siguientes.

- Proceso de planificación,
- Proceso de relaciones internacionales,
- Procesos de asesoría legal,
- Proceso de comunicación,
- Proceso de recursos humanos,
- Proceso de tecnología e informática,
- Proceso financiero, y
- Proceso administrativo.

De todo esto se compone la estructura por procesos de la Corte Constitucional que ayudará para dar un mejor servicio a todos los usuarios que necesitan del apoyo jurisdiccional de esta institución.

1.1.7 PROCESO DE TECNOLOGÍA E INFORMÁTICA [5]

Al ser el “Proceso de Tecnología e Informática” el área donde se desarrollará el presente tema de tesis, será necesario ampliar la información referente a este proceso y todas las responsabilidades que le competen.

Los procedimientos propios de esta área son los siguientes:

1. Ejecución de proyectos tecnológicos

Lo que trata de lograr la ejecución de proyectos tecnológicos es, alinear al Departamento de Tecnología con las bases del negocio de la Corte Constitucional, y de esta manera poder agilitar, facilitar y almacenar la información de toda la entidad, cumpliendo con la normativa de control interno para instituciones públicas emitidas por la Contraloría.

Para poder implementar un proceso de este tipo, se deberán presentar todos los proyectos y planes de tecnología a principio de año dentro del "Plan Operativo Anual[11]", el cual será revisado y aprobado por el pleno de la Corte Constitucional, en base al presupuesto institucional. A su vez, todo proyecto que requiera de una inversión pública deberá ser presentado en la Secretaría Nacional de Planificación y Desarrollo, entidad que se encarga de planificar y regular las compras públicas de todas las instituciones a nivel nacional.

Cada proyecto tecnológico será diseñado por el Director de Tecnología de la Corte Constitucional, que previo a su aprobación, tendrá que enviar el proyecto al Secretario de Gestión Institucional, el cual, deberá solicitar una certificación al Director Administrativo en la que se detallará si es que existen los fondos necesarios para ésta inversión, en caso de tener una respuesta favorable, se requerirá pasar al Departamento Legal para que emita su criterio sobre el tema y por último se entregará el proyecto aprobado por todos estos departamentos al Presidente de la Corte, el mismo que dará el visto bueno para que se continúe con la ejecución del proyecto.

2. Desarrollo de soluciones tecnológicas de información

Posterior a la aprobación del proyecto, se deberá desarrollar todo el pan sobre la solución tecnológica que incluirá los siguientes puntos:

---

[11] **Plan Operativo Anual o POA**, es un documento oficial en el que los responsables de una organización enumeran los objetivos y las directrices que deben marcar el corto plazo, por lo general el plazo será de 1 año. Obtenido de, http://es.wikipedia.org/wiki/Plan_operativo.

a. Realizar estudio de viabilidad

Para realizar el estudio de viabilidad, el Director de Tecnología tendrá que basarse en los siguientes análisis:

Análisis de los requerimientos de la institución.- este análisis incluirá como punto principal, el asegurarse de que la implementación tecnológica va a ser necesaria para cumplir con la política de negocio de la Corte Constitucional y que satisfará las necesidades de los usuarios que estarán dentro de la red.

Análisis de la tendencia de mercado.- el análisis de mercado contempla la tendencia de las empresas dentro del sector público que han implementado una solución tecnológica similar o a su vez que la desean implementar a futuro, y de esta manera poder tener una base técnica de instituciones que han hecho lo mismo.

Análisis de productos.- para el desarrollo de la solución tecnológica se deberá tener en cuenta una amplia gama de empresas que oferten el mismo producto, con las respectivas diferencias que incluirán, costo, garantía, servicio técnico, instalación, mantenimiento, entre otras, características muy importantes al momento de elegir la empresa proveedora de la respectiva solución.

Análisis de costos.- este tipo de análisis tiene que ver mucho con el costo y beneficio que se adquiera al implementar el nuevo proyecto dentro de la Corte Constitucional, su impacto favorable hacia la comunidad y los usuarios sin que represente un costo exorbitante.

b. Diseño

Una vez realizado todo el estudio sobre la viabilidad del proyecto y según las necesidades de la Corte Constitucional, se procederá a realizar el diseño con referencia en dos puntos:

Diseño físico.- a través de este diseño se logrará cumplir las tareas del sistema, lo que incluye la manera de juntar sus componentes y las funciones que realizará cada uno de éstos, además, se especificarán las características que requieran los componentes del proyecto, para luego de esto poner en marcha el diseño lógico. En esta fase deberán delinearse las características de cada uno de los elementos que serán parte del diseño como el hardware, software, bases de datos, seguridad, personal.

Diseño lógico.- este diseño hará referencia a lo que va a realizar el nuevo sistema a ser implementado, es decir, que se detallarán las funciones del sistema para resolver los problemas identificados en el análisis previo.

Este tipo de diseño deberá incluir un plan sobre el propósito de cada elemento del sistema. Las especificaciones de diseño lógico deberán contemplar la entrada y salida de información, el procesamiento, el almacenamiento, los archivos, los usuarios.

c. Construcción y pruebas

Habrá que diferenciar estos dos aspectos, ya que si se contrata una empresa externa, el proveedor contratado será el responsable de la solución técnica del proyecto, y en caso de que ésta sea desarrollada internamente por parte de la Corte Constitucional, el responsable será el Departamento de Tecnología, por esta razón es que:

Construcción.- el proveedor ó Departamento de Tecnología deberán entregar un cronograma tentativo con las fechas, actividades, recursos, que se requieran para la consecución del proyecto, además de que, una vez adjudicado el proyecto, este cronograma deberá ser actualizado y presentado a la contratante para el respectivo seguimiento y control.

Los retrasos en la construcción y sus motivos deberán ser comunicados oportunamente, sin perjuicio de que estos retrasos signifiquen la imposición de multas al proveedor por el incumplimiento.

Pruebas.- el proveedor ó Departamento de Tecnología deberán presentar un plan de pruebas que revisado conjuntamente con la Corte Constitucional valide el correcto funcionamiento de todos y cada uno de los componentes de la solución, tomando en cuenta detalles como configuración del nuevo equipo, conectividad, funcionalidad, entre otras.

d. Implantación, estabilización y aceptación.

De la misma forma, estos tres puntos dependerán de que la solución tecnológica haya sido contratada de forma externa a la Corte Constitucional o desarrollada internamente, en donde los responsables de la implantación, estabilización y aceptación, serán la empresa proveedora y el Departamento de Tecnología respectivamente.

Implantación.- ya sea por parte del proveedor de servicio o el Departamento de Tecnología, se tendrá que considerar entregar la solución tecnológica configurada e instalada correctamente y en forma completa en las instalaciones de la Corte Constitucional incluyendo montaje y conexión, garantizando que ésta nueva adquisición no afectará el desempeño funcional de la institución, además, se deberán responsabilizar del soporte de la tecnología instalada.

Estabilización.- durante el tiempo de soporte para la estabilización, el proveedor o el Departamento de tecnología tendrán la obligación de brindar soporte en sitio y de ser necesario volver a configurar los elementos que sean parte de la solución adquirida hasta que ésta quede operativa y totalmente funcional.

Aceptación.- para realizar el proceso de aceptación el proveedor o el Departamento de Tecnología deberán entregar la documentación necesaria para tener respaldos técnicos de la presente implementación, como por ejemplo, esquemas de interconexión[12], manuales técnicos, descripción de configuraciones, garantías, respaldo de configuraciones y contacto de soporte técnico.

[12] **Esquema de interconexión,** son diagramas que indican cómo fueron instalados los equipos dentro de un área determinada. Obtenido en, http://www.internationaltrading.com.mx/diagramas.htm.

3. Administración de la infraestructura[13]

La administración de la infraestructura dentro del Departamento de Tecnología se realizará en base a dos aspectos importantes, el primero que trata sobre los acuerdos de mantenimiento que se mantenga con las empresas proveedoras, y el segundo, propio del departamento que le confiere velar por el cuidado, mantenimiento y soporte de toda la información de la Corte Constitucional.

a. Administración de redes

La administración y configuración de la red de la Corte Constitucional estará a cargo del Administrador de la Red de Datos, el mismo que es responsable de proveer el mejor servicio y ofrecer la mejor capacidad de la red para todos los usuarios, garantizando la confidencialidad de datos.

b. Administración de servidores

La administración de los servidores también estará a cargo del Administrador de la Red de Datos que se encargará de las configuraciones más adecuadas para obtener el máximo rendimiento a cada uno de los equipos que se encuentren en su custodia, sin descuidar su respectivo mantenimiento preventivo-correctivo y el respaldo de la información contenida en cada uno de ellos.

c. Administración de Data Center[14]

La administración del data center estará a cargo del Coordinador de Sistemas y el Asistente de Sistemas que se responsabilizarán de la seguridad, mantenimiento, garantía, y soporte de hardware y software de los diferentes equipos dentro del data center.

---

[13] **Infraestructura Tecnológica,** es el conjunto de todos los elementos tecnológicos que integran un proyecto o sustentan una operación. Obtenido en, http://proactinfo.com/index.php?option=com_content& view=article&id= infratecnologica.

[14] **Data center o Centro de procesamiento de datos,** es la ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Obtenido en, http://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos.

4. Gestión de Soporte

El soporte técnico es parte primordial para mantener los equipos en un óptimo funcionamiento, y será competencia del Departamento de Tecnología atender y garantizar este requerimiento. Solo en caso, de que el Departamento de Tecnología a través de un contrato previo tenga garantía vigente con algún proveedor, éste se responsabilizará del soporte técnico a dichos equipos o plataformas.

a. Soporte técnico a usuario

El soporte a todos los usuarios de la Corte Constitucional será de responsabilidad del personal técnico que labore en el Departamento de Tecnología, así bien, se deberá atender cualquier requerimiento de los funcionarios de la institución para lograr un mejor desempeño en sus funciones. Y en caso de que el proveedor fuera el responsable de esta función se deberá hacer cargo de por lo menos un año de soporte técnico; para cualquiera de los dos casos el soporte técnico podría incluir:

- Limpieza interna y externa de los equipos,
- Revisión de fallas,
- Actualizaciones y configuraciones,
- Drivers[15] de los equipos, y
- Help desk[16], etc.

b. Soporte técnico de plataformas[17]

Al igual que en el caso del soporte a usuarios, el soporte de plataformas será responsabilidad del Departamento de Tecnología, y más aún, si éstas plataformas fueron desarrolladas internamente para el uso de los funcionarios de la Corte

---

[15] **Drivers o controladores,** son los encargados de actuar como interfaz entre el sistema operativo y los dispositivos que componen un ordenador, es así- como todos los componentes se entienden y trabajan conjuntamente. Obtenido en, http://www.helpdrivers.es/Que_son_los_drivers/faq_1275.

[16] **Help Desk o Mesa de Ayuda,** se denomina así al punto de contacto para atender cualquier requerimiento de soporte tecnológico a los usuarios finales. Obtenido en, http://www.ibm.com/ec/services/eus/support/help_desk.phtml.

[17] **Plataforma,** en informática es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible. http://es.wikipedia.org/wiki/Plataforma_%28inform%C3%A1tica%29

Constitucional; si el soporte de alguna plataforma fuera responsabilidad del proveedor de la misma manera deberá acercarse a ayudar con los requerimientos necesarios para que el sistema siga funcionando de manera óptima. Estos requerimientos podrían incluir:

- Revisión de código fuente, y
- Configuración de sistema, etc.

1.1.8 ESTRUCTURA DEL DEPARTAMENTO DE TECNOLOGÍA

El Departamento de Tecnología se encarga del acceso y buen aprovechamiento de los avances existentes para la automatización y comunicación de toda la entidad; esto a través de un sistema que favorece el flujo de trámites y procesos con celeridad y capacidad. Con respecto al diagrama organizacional del Departamento de Tecnología se distribuye de la siguiente manera:

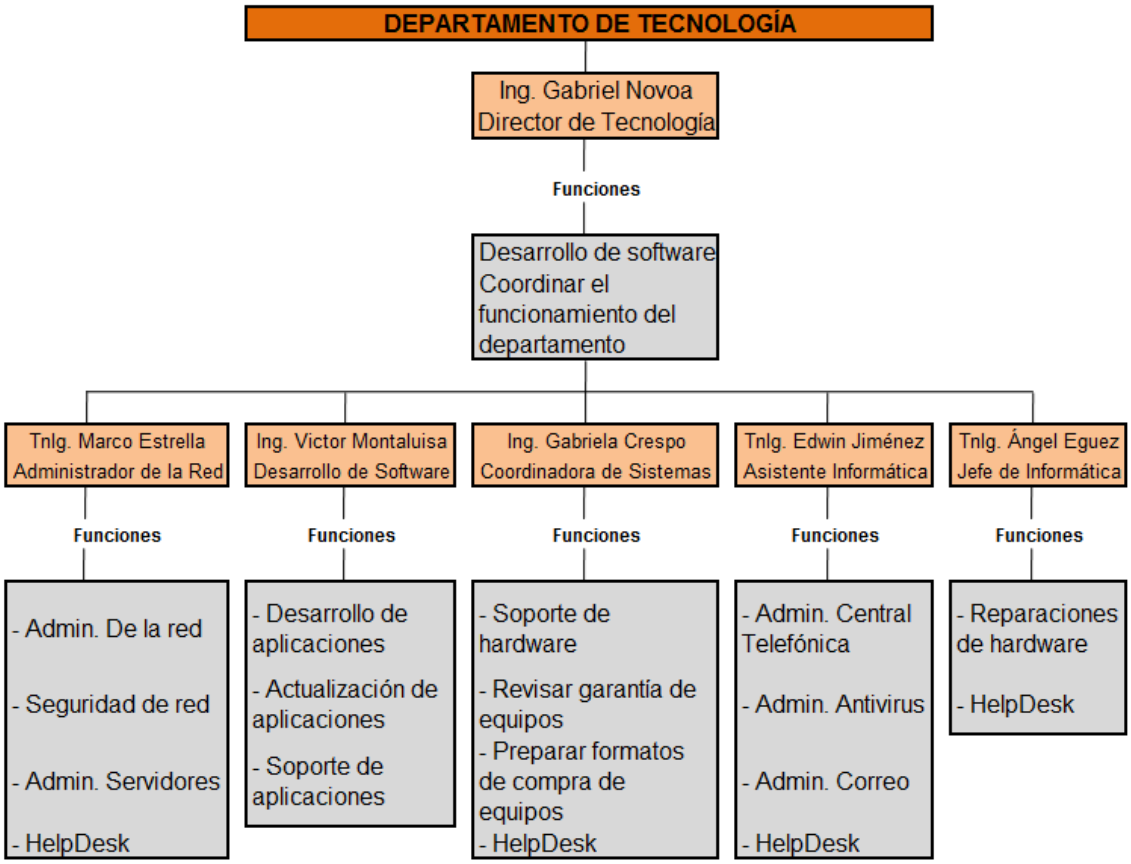


Figura 1.6: Organizacional Departamento de Tecnología
Autor: Departamento de Tecnología
Fuente: Departamento de Tecnología

Los objetivos del Departamento de Tecnología son:

1. Coordinar y monitorear el plan anual de tecnología;
2. Coordinar y monitorear los planes de mantenimientos preventivos y correctivos de la infraestructura tecnológica;
3. Coordinar y monitorear el soporte informático a nivel de hardware y software;
4. Coordinar y monitorear el desarrollo de software especializados;
5. Coordinar y monitorear los planes de auditorías informáticas;
6. Coordinar y monitorear los planes de respaldo y protección de la información de la Corte Constitucional.

Como parte de los Procesos y Servicios que brinda el Departamento de Tecnología, se tiene los siguientes:

1. Plan anual de desarrollo y actualización de tecnología y su aplicación;
2. Planes de mantenimientos preventivos/correctivos de la infraestructura tecnológica;
3. Soporte informático a nivel de hardware y software;
4. Desarrollo de software especializado;
5. Planes de auditorías informáticas y su aplicación;
6. Informe de administración de los servicios electrónicos, aplicaciones y bases de datos;
7. Plan de respaldo y protección de la información de la Corte Constitucional y su aplicación.

1.1.9 PROBLEMÁTICA DE LA CORTE CONSTITUCIONAL [6]

De acuerdo con el documento presentado a la Secretaría Nacional de Planificación y Desarrollo que hace referencia al proyecto de “Fortalecimiento de Infraestructura y Equipamiento de la Corte Constitucional” para el año 2012, se ha extraído las principales necesidades que tiene el Departamento de Tecnología a cargo del Ing. Gabriel Novoa, Director de Tecnología, de esta institución.

Este documento se desarrolló con el objetivo de hacer conocer las falencias y conseguir los recursos necesarios para mejorar la unidad de Tecnología de la Corte Constitucional en la Ciudad de Quito, con Dirección: Av. 12 de Octubre N16-114 y Pasaje Nicolás Jiménez.

Del análisis que se realizó en este documento se pudo identificar 5 problemas a resolverse lo más pronto posible, los mismos que serán detallados en la siguiente tabla:

#	Problema	Descripción
1	Servidores y almacenamiento	Plataforma insuficiente para soportar todos los procesos requeridos; equipos han superado su vida útil.
2	Licencias de equipos	No se cuenta con licencias para respaldar el trabajo de los equipos.
3	Página y servicios Web	Están soportados por un solo servidor, cuya capacidad de procesamiento ya es insuficiente.
4	Seguridad de la red de datos (LAN)	Los equipos que protegen actualmente la red LAN no son especializados para este cometido.
5	Almacenamiento de información	Actualmente la documentación de la Corte se maneja exclusivamente de forma física, lo que hace muy difícil realizar el seguimiento de un documento y confirmar su estatus.

Tabla 1.1: Problemas actuales de la Corte Constitucional
Autor: Departamento de Tecnología
Fuente: Departamento de Tecnología

En base a esta serie de problemas detectados y principalmente al numeral 4 que hace referencia a la Seguridad de la red de datos (LAN[18]), es por esto que se ha visto necesario realizar esta investigación sobre "Gestión de seguridad en la red de datos de la Corte Constitucional mediante el diseño de un CSIRT[19], (Equipo de respuesta a incidentes de seguridad)", por este motivo, es primordial implementar un sistema adecuado de aseguramiento de la información a nivel de red de datos interna, ya que debido a la demanda actual y al previsto crecimiento de información para los próximos años, es necesario migrar estos sistemas a aplicaciones dedicadas y robustas que permitan fortalecer la respuesta de la entidad ante ataques que pretendan vulnerar la integridad de la información residente en los servidores, pero sobre todo priorizar la capacitación del personal que va a estar a cargo de la seguridad de la información.

[18] **LAN (Local Area Network)**, Redes de Área Local. Es un sistema de comunicación entre computadoras que permite compartir información, obtenido en http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local.
[19] **CSIRT,** Computer Security Response Team, por sus siglas en inglés, disponible en www.csirt.org.

Por lo tanto y de acuerdo a su Proyecto de Fortalecimiento de Infraestructura y Equipamiento y de su Plan Operativo Anual propio del Departamento de Tecnología, es un requerimiento el garantizar el cuidado y manejo de la información, por esta razón es que se ha propuesto esta investigación sobre el diseño de un "Equipo de respuesta a incidentes de seguridad", ya que al no contar con un área especializada para dar seguridad a la red y a la información que fluye a través de la misma, es que se ha visto necesario diseñar un modelo de mejoramiento de seguridad, que ayudará a la nueva organización del Departamento de Tecnología, utilizando el mismo personal que ya labora dentro de él, pero con una nueva distribución de funciones.

La nueva tendencia de seguridad de la información necesita que tanto entidades de gobierno como del sector privado emprendan iniciativas para la protección de lo que se denomina "infraestructura crítica" dentro de cada empresa, por esta razón es que la gran mayoría de entidades que quieren implementar procesos de seguridad de la información se rigen a las recomendaciones de ISACA[20] (Information Systems Audit and Control Association), que es la Organización líder en Auditoria de Sistemas y Seguridad de los Activos de Información a nivel mundial, que según su publicación "Modelo del Negocio para Seguridad de la Información " realizada mediante su página web oficial, recomienda desarrollar un modelo de seguridad de acuerdo a los siguientes factores: organización, proceso, tecnología y el personal.

Para cubrir estas necesidades es que el tema de "Gestión de Seguridad de la Red de Datos Mediante el Diseño de un CSIRT" se ha planteado como una idea muy acorde a la seguridad que se merece la información de la Corte, sin embargo, hay que tener en cuenta que un CSIRT es un grupo de personas que trabajan coordinadamente en base a un proceso metodológico y una norma como lo recomienda ISACA.

[20] **ISACA,** Information Systems Audit and Control Association, Asociación de Control y Auditoría en Sistemas de la Información, Septiembre 2011. En www.isaca.org.

El desarrollo de este proyecto de tesis se enfoca en crear un Equipo de respuesta a incidentes de seguridad denominado CSIRT, que como su nombre lo indica servirá para dar un servicio de seguridad principalmente proactiva más que reactiva a la Corte Constitucional y que para su diseño necesitará de varios factores como, la norma ISO[21] 27002 dominio 9 que ayudará para guiar la gestión de incidentes y que también está aceptada dentro de la Subsecretaría de Informática del Ecuador; un modelo metodológico, que será evaluado entre el modelo que propone ISACA y el modelo propio del CSIRT para poder ver cuál de los dos beneficiará más al propósito de negocio de la institución, y por último, el diseño como tal, que se acoplará a las necesidades que se requieran en la Corte Constitucional.

1.2 LEYES Y REGLAMENTOS PARA SEGURIDAD ELECTRÓNICA DENTRO DEL SECTOR PÚBLICO

La Corte Constitucional por ser parte del sector público tiene que regirse a las leyes y normas de los organismos que regulan la seguridad electrónica a nivel nacional. Dentro de la Constitución de la República del Ecuador se encuentran todas las bases técnicas para implementar proyectos de tecnología dentro del sector público, y se encuentran detalladas dentro de la publicación del Registro Oficial[22] del año 2009. A parte de la Constitución existe también una entidad como es la Subsecretaría de Informática, que regula los proyectos de tecnología a nivel nacional.

1.2.1 Constitución de la República [7]

Publicada dentro del Registro Oficial del año 2009, separa todo un capítulo dedicado a “Tecnología de la Información” donde se encuentran varios puntos a ser tomados en cuenta antes de implementar o investigar un avance tecnológico,

[21] **ISO (International Organization for Standardization),** Organización Internacional para la Estandarización, por sus siglas en inglés. Organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Obtenido en, http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_para_la_Estandarizaci%C3%B3n.

[22] **Registro Oficial N° 87** del Lunes 14 de Diciembre del 2009. Pág. 48, Tecnología de la Información. Obtenido de, http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=17&Itemi

por esta razón, es que en esta sección se detallarán algunas de las normas que han sido revisadas y que se deben utilizar para implementar proyectos de tecnología, pero que sobre todo, servirán como pauta para el desarrollo del presente trabajo de investigación. Los tres principales puntos son:

1. Administración de proyectos tecnológicos

Sobre este punto la Constitución dice que:

"La Unidad de Tecnología de Información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad."[23]

Los aspectos a considerar dentro de este punto son:

- Describir los objetivos y alcance del proyecto, su relación con otros proyectos de la entidad y la aceptación de los usuarios interesados.
- Plantear un cronograma de actividades que facilite la ejecución y monitoreo del proyecto, con su respectiva descripción del talento humano requerido, tecnológico y financiero, sin olvidar las respectivas pruebas y capacitación al personal.
- En caso de que el proyecto considere una inversión para la institución, se deberá especificar todos los costos directos (Ej. Compra de equipos) e indirectos (Ej. Mantenimiento de equipos), sus beneficios para la inversión y la capacitación que se pueda incluir para el personal de soporte.
- Para la ejecución del proyecto se elegirá a una persona responsable con capacidad de decisión y autoridad para que dirija el desarrollo de la investigación.
- Se deberá monitorear y ejercer el control permanente de los avances del proyecto.

[23] **Constitución de la República,** Registro Oficial N° 87, Administración de proyectos tecnológicos, 2009. Pág. 50.

- La culminación formal del proyecto incluirá la aceptación, pruebas de calidad, cumplimiento de objetivos y beneficios obtenidos que fueron planteados desde un inicio.

2. Adquisición de infraestructura tecnológica

En caso de que dentro del estudio de vulnerabilidades en la Corte Constitucional se recomiende la adquisición de un equipo para mejorar la seguridad de la información, la Constitución dice lo siguiente:

"La Unidad de Tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:"[24]

- Para las adquisiciones tecnológicas deberán detallarse los objetivos de acuerdo a los lineamientos de la institución, principios de calidad de servicio y además deberá constar un plan de contrataciones aprobado por la autoridad pertinente, con previa justificación técnica presentada.
- La unidad de tecnología deberá planificar el incremento de capacidades, costos, vida útil del equipo y evaluará los riesgos tecnológicos de la inversión para futuras actualizaciones; además, incluir un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, esto será considerado para optimizar la inversión.
- Con respecto a la adquisición de hardware se tendrá que tomar en cuenta las ofertas respectivas que deberán incluir características técnicas de los componentes ofertados como. Marca, modelo, numero de serie, capacidades, unidades de entrada y salida, entre otros, así como también, la garantía ofrecida por el proveedor, todos estos datos para poder llegar a una fase precontractual y contractual con la institución.
- Los contratos con los proveedores deberán incluir especificaciones sobre acuerdo de nivel de servicio, teniendo en cuenta sobre todo la seguridad y

[24] **Constitución de la República,** Registro Oficial N° 87, Adquisición de infraestructura tecnológica, 2009. Pág. 51.

confidencialidad de la información además de los requisitos legales que sean aplicables. También se aclarará que los datos son propiedad de la institución contratante del servicio.

3. Seguridad de tecnología de información

Con respecto a la seguridad de la información la Constitución señala lo siguiente:

"La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:"[25]

- Se deberá dar una ubicación y un control de acceso adecuado al Departamento de Tecnología, en especial a las áreas sensibles como son: los servidores, desarrollo y biblioteca.
- El Departamento de Tecnología deberá encargarse de definir los procedimientos de obtención de respaldos de información en función de un cronograma previamente aprobado.
- Para lograr un buen soporte y actualización de tecnologías se priorizará la migración de la información a medios físicos externos que garanticen la perpetuidad y recuperación de los datos, siguiendo con los estándares necesarios para cumplir con este objetivo.
- Se tomará en cuenta como una alternativa, el almacenamiento externo de los respaldos de información sensible de la organización.
- La administración e implementación de seguridades a nivel de hardware[26] y software[27] se realizarán mediante un monitoreo y pruebas periódicas para poder detectar posibles vulnerabilidades o incidentes de seguridad, y así, tener la capacidad de tomar las acciones correctivas del caso.

---

[25] **Constitución de la República,** Registro Oficial N° 87, Seguridad de tecnología de información, 2009Pág.52

[26] **Hardware,** corresponde a todas las partes tangibles de un sistema informático sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Obtenido de, http://es.wikipedia.org/wiki/Hardware

[27] **Software,** al equipamiento lógico o soporte lógico de un sistema informático. Obtenido de, http://es.wikipedia.org/wiki/Software

- Las instalaciones físicas del data center o centro de datos del Departamento de tecnología deberá incluir dispositivos y equipo especializado para monitorear y extinguir fuego sin poner en riesgo la información, un ambiente controlado, una humedad relativa y aire acondicionado para mantener la temperatura estable en todos los equipos.
- Se deberá considerar y disponer de sitios de procesamiento alternativos.
- Habrá que definir procedimientos de seguridad por parte del personal que se turnará para trabajar por la noche o en fines de semana dentro de la organización.

1.2.2 Subsecretaría de Informática [8]

La Subsecretaría de Informática es un organismo público que regula los proyectos tecnológicos y promulga la utilización de software libre dentro de todas las entidades del estado, de esta manera se estandarizará los mismos procesos en beneficio de la ciudadanía.

La misión de la Subsecretaría de Informática es:

"Mejorar la gestión del gobierno mediante la estandarización, regulación, control, integración y ejecución de los proyectos informáticos de las entidades del gobierno central, y coordinar acciones en este campo en las demás instituciones del sector público."[28]

Sus responsabilidades y atribuciones son:

a) Coordinar el procesamiento de las políticas públicas de gestión tecnológica y su integración en el plan estratégico y planes operativos de la Subsecretaría;

b) Aprobar o rechazar la ejecución de proyectos informáticos de las instituciones que dependen de la Presidencia de la República;

c) Velar por el cumplimiento de leyes y reglamentos que favorezcan la utilización de software libre;

[28] **Misión Subsecretaría de Informática,** Página web oficial. Obtenido en, http://www.informatica.gob.ec/index.php/inicio/subsecretaria/base-legal.

d) Cuidar por el cumplimiento de leyes y reglamentos para la regulación, control, evaluación y seguimiento de los proyectos informáticos del sector público;

e) Difundir y hacer cumplir las normas y estándares para: la formulación y gestión de proyectos informáticos, el intercambio de información, el uso de buenas prácticas en la operación de sistemas informáticos, etc.

f) Integrar los sistemas y las bases de datos del sector público y facilitar el acceso a los mismos;

g) Gestionar, coordinar y ejecutar la capacitación y asistencia técnica, al personal e instituciones del sector público.

La Subsecretaría de Informática [8] dice que:

"Las entidades públicas velarán por fortalecer la seguridad en las redes de datos para evitar accesos no autorizados[29]"

Sus recomendaciones para la seguridad de información digital gubernamental dentro de los servicios de red de datos y comunicaciones son las siguientes:

- Restringir el acceso a usuarios no autorizados creando grupos de redes locales para despachos, autoridades, áreas, entre otras.
- Especialmente para el caso de autoridades ministeriales, implementar redes locales virtuales.
- Deshabilitar puntos de acceso a redes inalámbricas mientras no se utilicen.
- Para redes inalámbricas habilitar todo tipo de seguridades.
- Coordinar pruebas de hacking ético[30] o de vulnerabilidades a la infraestructura de rede institucional.
- Habilitar el acceso a la red alámbrica e inalámbrica mediante el registro de direcciones MAC[31].

[29] **Subsecretaría de Informática,** dentro de sus Recomendaciones para Seguridad de Información Digital Gubernamental. Disponible en, http://www.informatica.gob.ec/files/SIRecSegInfGub.pdf

[30] **Hacking Ético,** término utilizado para describir el desarrollo de técnicas para detectar vulnerabilidades en la red de una entidad u organización, con previa autorización y conocimiento de la empresa contratante. Obtenido en, http://tics.org.ar/index.php?option=com_content&view=article&id=97:conceptos-de-hacking-etico&catid=14:seguridad-informca&Itemid=31

Todas esta responsabilidades y atribuciones de la Subsecretaría de Informática han sido creadas para poder generar un marco de regulación, integración y control de todas las plataformas tecnológicas del estado, en donde se priorizará la utilización de software libre, el cual será de gran ayuda para la configuración y mantenimiento de la seguridad de la información, sin olvidar su costo reducido.

Con todo este marco legal previamente definido para las instituciones del sector público, se podrá generar el modelo de situación inicial propio del Capítulo 2 y a la postre poder crear el modelo de mejoramiento.

[31] **Dirección MAC (Media Access Control),** Control de Acceso al Medio por sus siglas en inglés, que es un identificador que corresponde de forma única a una tarjeta o dispositivo de red. Obtenido en, http://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC

CAPITULO 2

SITUACIÓN ACTUAL DE LA RED DE DATOS DE LA CORTE CONSTITUCIONAL

2.1 INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS

El objetivo de realizar el análisis a la red de datos será identificar, describir y diagnosticar los problemas que actualmente se presentan dentro de la Corte Constitucional, y cómo estos podrían afectar a futuro el flujo de información sensible para la institución. Para éste análisis de situación actual se utilizará el modelo TCP/IP[32], pero no se realizará el estudio capa por capa, en su lugar se dividirá de la siguiente manera:

- La capa de enlace y la capa de internet como Capa Física
- La capa transporte, como Capa de Red
- Y la Capa Aplicación de esta misma forma.

Para el análisis de la capa Física se usará la distribución de arquitectura modular de Cisco (Ver Anexo A), la cual permitirá dividir la red de la Corte en módulos funcionales para su análisis. Para el análisis de la Capa de Red se tomará en cuenta el direccionamiento, enrutamiento y gestión de configuración de los protocolos presentes en la red. En cuanto al análisis de la Capa de Aplicación, se estudiarán aplicaciones informáticas y servicios que se puedan encontrar dentro de la red de la Corte.

A continuación se detallará el análisis de cada una de estas tres capas para aclarar el estado de situación actual.

2.1.1 Capa Física

Para realizar el análisis actual de la red física de la Corte Constitucional, primero habrá que identificar sus principales componentes y luego organizarlos según la arquitectura modular de Cisco. De acuerdo a la arquitectura modular la Corte Constitucional está dividida en cinco módulos que son:

1. Módulo Central
2. Módulo distribución de edificios

[32] **Modelo TCP/IP,** es un modelo de descripción de protocolos de red creado en la década de 1970 por DARPA, una agencia del Departamento de Defensa de los Estados Unidos. Obtenido en, http://es.wikipedia.org/wiki/Modelo_TCP/IP.

3. Módulo servidores
4. Módulo edificio
5. Módulo edificio 2 y regionales.

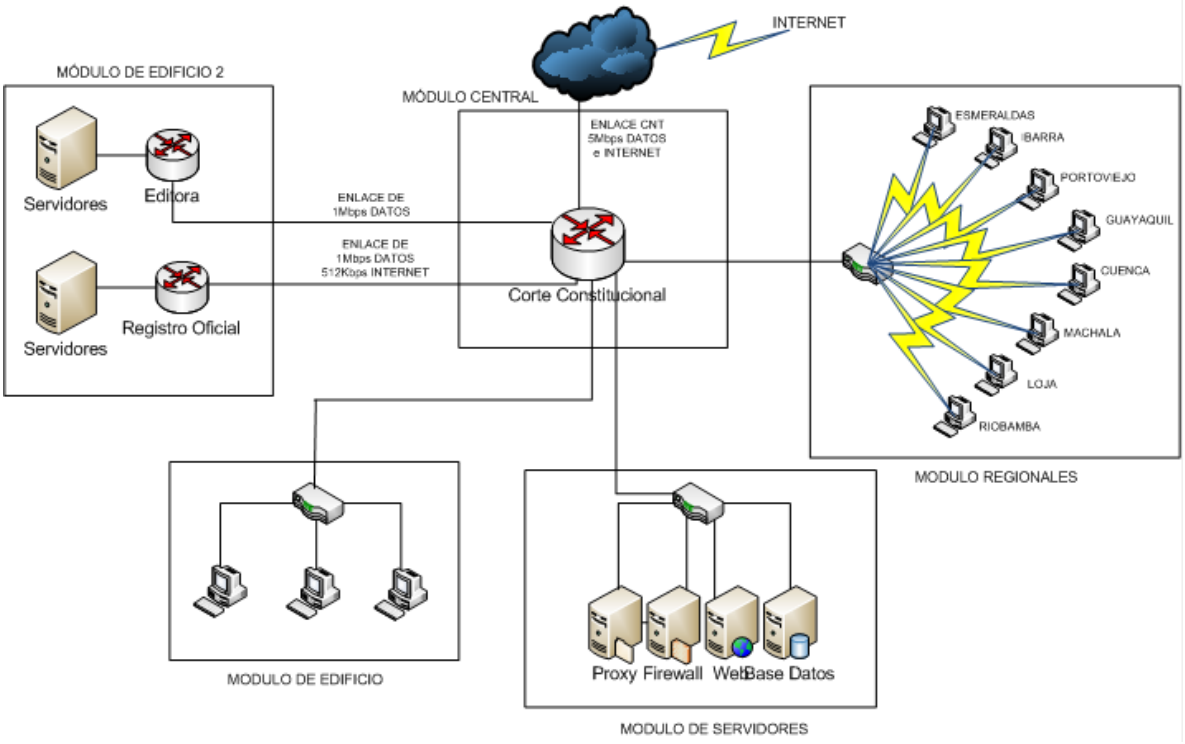


Figura 2.1: Situación Actual de la Red
Autor: Tesista
Fuente: Departamento de Tecnología

La información sobre cada uno de los módulos que se observan en la Figura 2.1 será ampliada a continuación.

2.1.1.1 Módulo Central

El módulo central de la Corte Constitucional está administrado por un Switch Core Capa 3 marca Cisco, modelo 3560G de 48 puertos, que se encarga de administrar las rutas y encaminar el tráfico tanto interno como externo de la forma más rápida a todas las áreas de la Corte. Este equipo está configurado para soportar el paso de 15 direcciones IP públicas[33] contratadas a la Corporación Nacional de

[33] **Dirección IP pública,** son la direcciones pagadas que usan los, servidores, routers y demás equipos que quieran verse a través de internet. Obtenido de, http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP.

Telecomunicaciones (CNT), las mismas que sirven para crear los enlaces a oficinas regionales, envío-recepción de información externa y video conferencias.

Por otra parte en el equipo se han generado 18 VLANs[34] que serán detalladas posteriormente dentro del enrutamiento de la red, estas direcciones se distribuyen hacia diferentes áreas y servicios de la Corte con el fin de balancear la carga de tráfico generado, y se encuentran divididas de la siguiente manera:

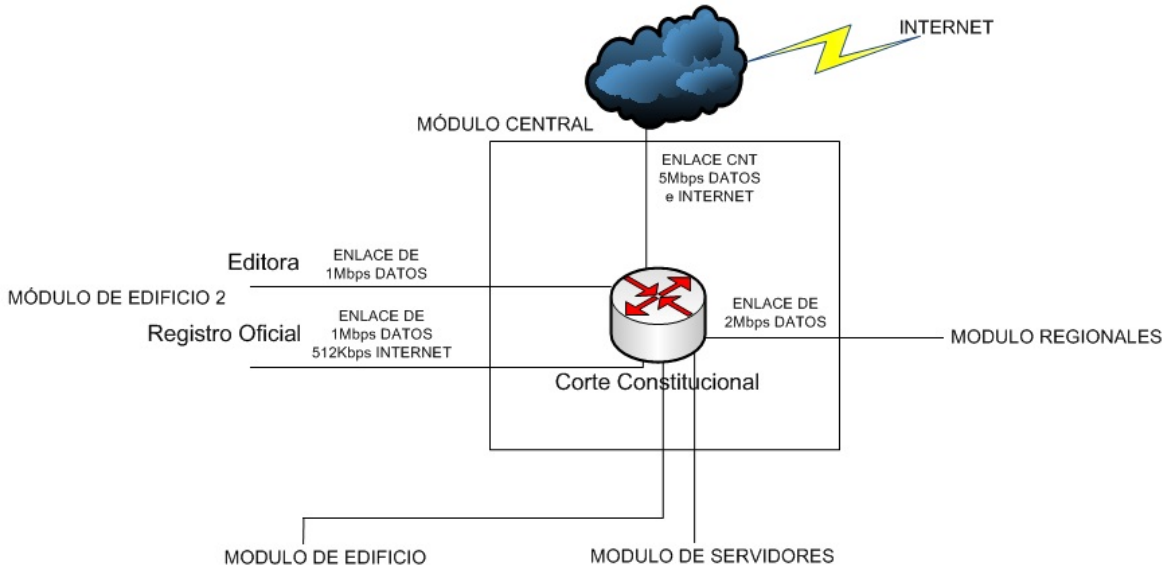


Figura 2.2: Módulo Central de la Red
Autor: Tesista
Fuente: Departamento de Tecnología

Este equipo provee a la Corte Constitucional una transmisión de paquetes con velocidades de hasta 32Gbps, razón por la cual, la tasa de rendimiento del equipo se encuentra por debajo del 8% de su capacidad máxima, principalmente debido a que todas las interfaces de red se encuentran configuradas a 100 Mbps y el Switch Core Capa 3 soporta velocidades de hasta 1000 Mbps, así que, no representa riesgo alguno de saturación o caída de servicios por sobrecarga de información. En lo que se refiere a la disponibilidad del servicio, no existe un equipo redundante para brindar respaldo a la red, lo que quiere decir, que si en caso fortuito el Switch Core Cisco 3560G llegara a quedarse sin servicio no habría

[34] **VLAN (Virtual LAN),** red de área local virtual, es un método de crear redes lógicamente independientes dentro de una misma red física. Obtenido en, http://es.wikipedia.org/wiki/VLAN.

ningún equipo alternativo para continuar con las funciones de las distintas áreas dentro de la Corte.

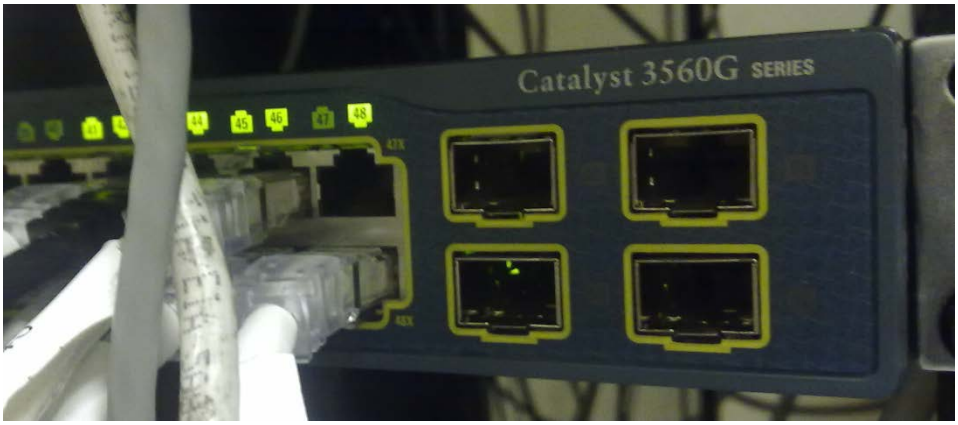


Figura 2.3: Switch Capa 3 Cisco 3560G
Autor: Tesista
Fuente: Data Center

Los aspectos de seguridad que posee este equipo dentro de sus características técnicas abarcan el nivel de capa 2 y capa 3, mediante el uso de reglas, que se encuentran divididas por: protocolos, red, dirección MAC y puertos.

2.1.1.2 Módulo de Distribución de Edificios

Para proteger la distribución de edificios de la Corte Constitucional se ha visto la necesidad de crear una DMZ[35], acrónimo que se utiliza para describir una zona desmilitarizada o red perimetral, con el objetivo de que la conexión desde la red interna de la Corte y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa. Los equipos dentro de la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna de la Corte en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquier intruso situado en la red externa y que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

[35] **DMZ (Demilitarized zone),** en seguridad informática una zona desmilitarizada o red perimetral, es una red local que se ubica entre la red interna de una organización y una red externa. Obtenido en, http://es.wikipedia.org/wiki/Zona_desmilitarizada_%28inform%C3%A1tica%29.

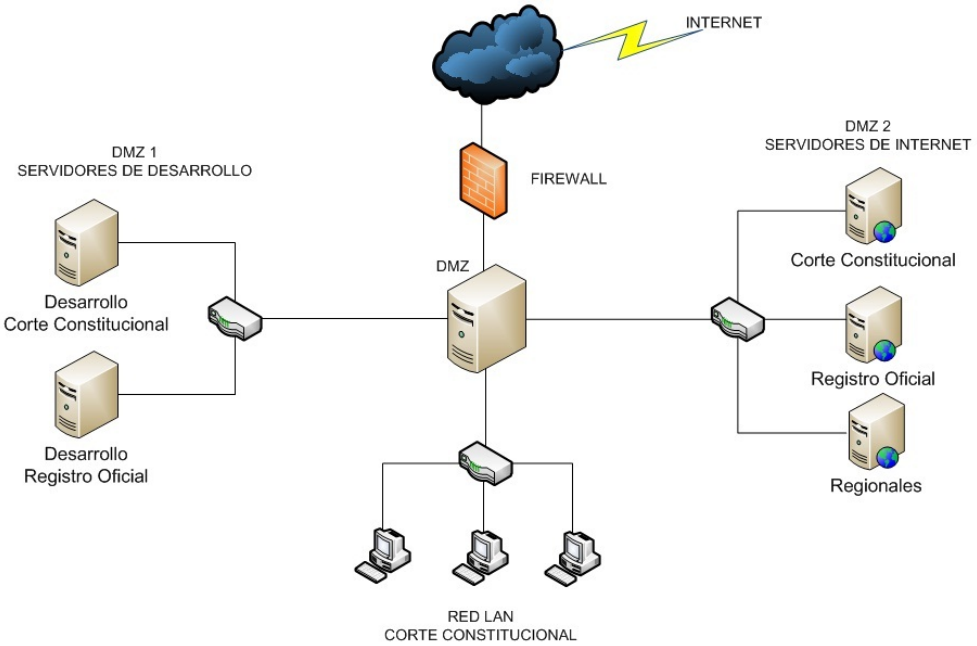


Figura 2.4: Segmento de Red DMZ
Autor: Tesista
Fuente: Departamento de Tecnología

La zona desmilitarizada de la Corte Constitucional protege dos segmentos de servidores muy sensibles, como son: los Servidores de Desarrollo y los Servidores de Internet.

Los Servidores de Desarrollo contienen todo el sistema de casos judiciales de la Corte siendo ésta información muy sensible; mientras que los Servidores de Internet ofrecen conectividad a usuarios externos, así que se debe cuidar este tipo de conexiones ya que podría haber intrusos que quieran filtrar la seguridad.

Por otra parte la red de la Corte Constitucional actualmente cuenta con un sistema de cableado estructurado certificado ANSI/EIA/TIA[36], y se encuentra dividido de la siguiente forma:

- Categoría 5e, para todo el cableado estructurado en cada uno de los pisos
- Categoría 6, para el enlace de cada uno de los pisos con el BackBone[37] principal.

[36] **ANSI/EIA/TIA,** representan los tres estándares oficiales para definir el cableado estructurado dentro de una organización. Obtenido en, http://es.wikipedia.org/wiki/TIA-568B.

La red interna también cuenta con los equipos apropiados para interconexión de información entre los distintos pisos y el BackBone principal de la Corte, este proceso se ha logrado mediante la implementación de Switchs de capa 2 marca Cisco, modelo 2960.

2.1.1.3 Módulo de Servidores

El módulo de servidores provee servicios y aplicaciones que son utilizados por usuarios finales de la red de la Corte Constitucional, los mismos que se encuentran distribuidos en las diferentes áreas y departamentos, conectados a cada segmento de la red local.

El Data Center se encuentra ubicado en el segundo piso del edificio de la Corte Constitucional dentro del Departamento de Tecnología, y cuenta con las siguientes características

- **Sistema de climatización para Data Center.-** este sistema posee un sensor de temperatura el cual se encarga de mantener la climatización del Data Center entre 18°C y 24°C; también tiene la capacidad de generar alertas cuando existen cortes de energía, cuando el equipo necesita mantenimiento o cuando está por terminarse el refrigerante.
- **Sistema de monitoreo.-** este sistema de monitoreo G4[38] incluye reportes sobre el desempeño del sensor de humedad, sensor de temperatura, sensor de inundación, sensor de humo, sensor de movimiento y sensor de apertura, las notificaciones de alerta se pueden recibir por medio de correo electrónico o servicio de mensajería celular al Administrador de la Red sobre el comportamiento del Data Center.
- **Control de acceso.-** el acceso se encuentra protegido en base a un sistema de clave biométrica, y las únicas personas que están autorizadas

---

[37] **BackBone (Columna vertebral),** en informática es el conducto principal que permite comunicar segmentos de red de área local entre sí, dentro de una organización. Obtenido en, http://www.alegsa.com.ar/Dic/backbone%20de%20red.php.

[38] **Monitoreo G4** es un dispositivo de monitoreo de red que garantiza el funcionamiento ininterrumpido del Data Center. Obtenido en, http://www.firmesa.com/web/conectividad-networking/gestion-y-monitoreo/gamatronic-g4

para ingresar son el Administrador de la Red y la Coordinadora de Sistemas.

- **Sistema de control y extinción de incendios.-** actualmente se cuenta con un sistema de detección de humo y fuego con sus respectivas alarmas, y el sistema de extinción de incendios es a base de gas ecológico ECARO 25 para controlar cualquier posible incendio.
- **Sistema de video vigilancia.-** se cuenta también con un sistema de cámaras, tanto en la parte exterior del edificio como en cada uno de los pisos para vigilancia de toda la entidad, esta función está a cargo de la Policía Nacional.
- **UPS[39].**- para proteger el equipamiento eléctrico se dispone de un UPS marca TripeLife de 10KVA[40] con sistema trifásico, que además de brindar soporte energético de 3 horas al Data Center sirve como regulador de voltaje para prevenir posibles descargas eléctricas.
- **Generador eléctrico.**- modelo trifásico que tiene una capacidad operativa de 30KVA, sin embargo, por el momento solo se están utilizando 8KVA para el soporte del Data Center, este generador utiliza diesel y se activa automáticamente cuando se interrumpe el fluido eléctrico se ubica en la parte exterior del edificio en el segundo piso.

Actualmente existen 27 servidores dentro del Data Center que serán especificados en la siguiente tabla:

#	SERVIDOR	Sistema Operativo
1	Servidor Antivirus Repositorio	Windows Server 2003
2	Servidor Administración Jurídica	Windows Server 2003
3	Servidor Administración Jurídica Backup	Windows Server 2003
4	Servidor Alfresco	Windows Server 2003
5	Servidor Antivirus Kaspersky	Windows Server 2003
6	Servidor Aplicaciones Pdf	Windows Server 2003

[39] **UPS (Uninterruptible Power Supply),** en español Sistema de Alimentación Ininterrumpida, que es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica. Obtenido en, http://www.alegsa.com.ar/Dic/ups.php.

[40] **KVA (Kilo Vatio Amperio),** es la unidad de la potencia aparente de un aparato eléctrico. Obtenido en, http://es.wikipedia.org/wiki/Voltiamperio.

7	Servidor Aplicativos	Windows Server 2003
8	Servidor Archivos Jurídicos	Windows Server 2003
9	Servidor BDD FIEL	Windows Server 2003
10	Servidor Desarrollo EQ1	Red Hat 6
11	Servidor Desarrollo EQ3	Red Hat 6
12	Servidor FIEL	Windows Server 2003
13	Servidor Impresión Finan	Windows Server 2003
14	Servidor Impresión Reg. Ofi.	Windows Server 2003
15	Servidor Open LDAP	Centos 5.7
16	Servidor Repositorio	Centos 5.7
17	Servidor Spool Win	Windows Server 2003
18	Servidor Web Alfresco	Centos 5.7
19	Servidor Web CCE	Centos 5.7
20	Servidor Web Proxy	Centos 5.7
21	Servidor Web Pruebas	Centos 5.7
22	Servidor Web Regionales	Centos 5.7
23	Servidor Web Test	Centos 5.7
24	Servidor Aplicaciones	Windows Server 2003
25	Servidor Web Red	Centos 5.7
26	Servidor Winsis	Windows Server 2003
27	Servidor Admin Finan	Windows Server 2003

Tabla 2.1: Servidores de la Corte Constitucional
Autor: Tesista
Fuente: Departamento de Tecnología

Estos 27 servidores que se detallaron anteriormente en la Tabla 2.2 se encuentran virtualizados con la ayuda de la herramienta VirtualBox y se encuentran dentro de distintas cuchillas en un Servidor Blade[41], este servidor es de marca HP, modelo C3000, este equipo es un chasis que sirve para interconectar cuchillas de diferentes características, esto incluirá, velocidad de procesamiento, capacidad de almacenamiento y memoria RAM[42] por cuchilla, estas especificaciones serán detalladas según los requerimientos de procesamiento necesarios para cada

[41] **Servidor Blade,** es un tipo de computadora para los centros de proceso de datos específicamente diseñada para aprovechar el espacio, reducir el consumo y simplificar su explotación. Obtenido en, http://es.wikipedia.org/wiki/Servidor_blade.
[42] **RAM (Random-Access Memory),** memoria de acceso aleatorio, es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados. Obtenido en, http://es.wikipedia.org/wiki/Memoria_ de_acceso_aleatorio.

servidor, con el objetivo de lograr el mejor rendimiento al momento de virtualizar cada servidor dentro de su respectiva cuchilla.

Figura 2.5: Servidor Blade C3000
Autor: Tesista
Fuente: Data Center

El Servidor Blade (Anexo B) de la Corte actualmente consta de las siguientes características:

- Capacidad máxima de expansión de 8 cuchillas
- 1 cuchilla se utiliza para la administración propia del Servidor Blade
- 1 cuchilla se utiliza para el Sistema de casos de la Corte Constitucional, con un procesadores Quad Core de 2.5Ghz y memoria RAM de 12Gb
- 2 cuchillas están siendo utilizadas para administrar la virtualización de los servidores, con procesadores Quad Core de 2.5Ghz y memoria RAM de 24Gb y 32Gb respectivamente
- 4 slots libres para cuchillas de expansión; estas cuchillas de expansión son de tipo BL460-G6 con una capacidad máxima para memoria RAM de 1 a 96Gb.

El almacenamiento de toda la información generada en las cuchillas del Servidor Blade se realiza a través de una red SAN[43], con una capacidad actual de 10 discos duros de 300Gb cada uno, con dos tipos de arreglos RAID[44] distribuidos de la siguiente forma:

- **RAID 1:** dos discos duros de 300Gb que funcionan como espejo para respaldar la información.
- **RAID 5:** arreglo de 3 / 5 discos de 300Gb que funcionan para almacenar información, pero perdiendo 300Gb de almacenamiento dentro del arreglo debido a la redundancia.
- Quedan aún 2 discos de 300Gb sin utilizar, y que podrían ser acoplados a cualquiera de las dos configuraciones RAID anteriormente mencionadas.

Figura 2.6: Arreglo de almacenamiento SAN
Autor: Tesista
Fuente: Data Center

Los respaldos de información de todos los servidores virtualizados se realizan una vez al mes y se los almacena en cintas magnéticas (CD, DVD).

A pesar de la virtualización todos los servidores brindan alta disponibilidad debido a las características de las cuchillas en donde están instalados los diferentes servicios.

La seguridad lógica de los servidores al momento se encuentra protegida por 5 servidores Firewall, distribuidos de la siguiente forma:

[43] **SAN (Storage Area Network),** en español una red de área de almacenamiento, es una red concebida para conectar servidores, matrices de discos y librerías de soporte. Obtenido en, http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_de_almacenamiento.
[44] **RAID (Redundant Array of Inexpensive Disks),** es un conjunto redundante de discos independientes que hace referencia a un sistema de almacenamiento que usa múltiples discos duros o SSD entre los que se distribuyen o replican los datos. Obtenido en, http://es.wikipedia.org/wiki/RAID.

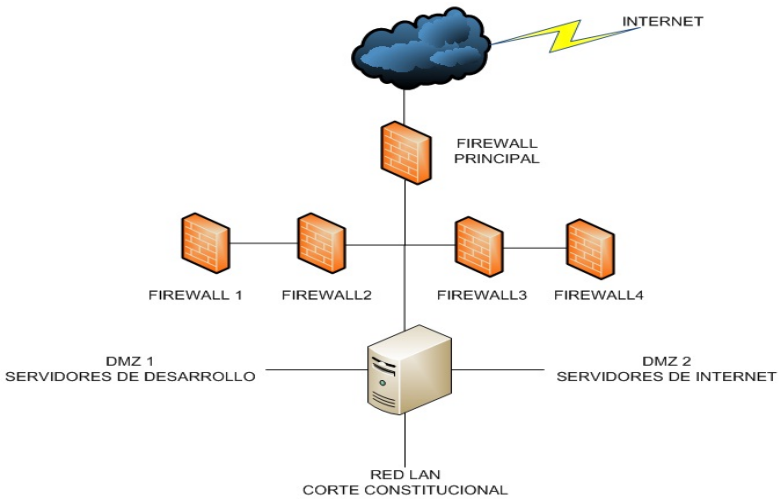


Figura 2.7: Distribución de Firewalls
Autor: Tesista
Fuente: Departamento de Tecnología

Como se puede observar en la Figura 2.7, el Firewall Principal es el que filtra y administra en base al Sistema Operativo Centos versión 5.7 todas las políticas del tráfico de entrada y salida de información para que cuando se direccione a los firewalls secundarios ya haya sido filtrada la mayor parte de tráfico indeseado, el único puerto que se encuentra habilitado en todos los firewalls es el número 80, el mismo que hace referencia a las conexiones web.

La seguridad que tiene al momento la red de datos de la Corte Constitucional es muy útil, pero se debería implementar una solución más robusta y que soporte ataques a la red como detección y prevención de intrusos, inyección SQL, prevención contra fuga de información, control de aplicaciones, filtrado URL, entre otros servicios que podrían ser necesarios para disminuir la vulnerabilidad de la red.

Existen dos appliance[45] externos dentro de los servidores, el primero ayuda como AntiSpam[46] de marca McAfee, que sirve para detectar y denegar el paso de correo basura al servidor de correo, y el segundo que se utiliza para brindar servicio de

[45] **Appliance,** palabra utilizada para denominar a un dispositivo de hardware independiente con su software integrado, diseñado especialmente para proporcionar un recurso informático específico. Obtenido en, http://en.wikipedia.org/wiki/Computer_appliance.
[46] **Antispam,** es lo que se conoce como método para prevenir el "correo basura". Obtenido en, www.symantec.com/anti-spam

video conferencia a través de un equipo marca Polycom, con un requerimiento de 2Mbps de ancho de banda para lograr una transferencia de información óptima.

Figura 2.8: Appliance McAfee y Appliance Polycom
Autor: Tesista
Fuente: Data Center

Por último, dentro del Data Center se encuentra la Central Telefónica de tipo análoga, que administra toda la comunicación telefónica de la Corte Constitucional, actualmente posee 43 líneas telefónicas contratadas a la empresa CNT, las mismas que se encuentran divididas en 93 extensiones; al momento ésta central telefónica se encuentra al 100% de su capacidad razón por la cual se requiere migrar a una central IP para economizar costos, ampliar el número de extensiones y mejorar a servicios digitales de comunicación.

2.1.1.4 Módulo de Edificios

Para la adquisición de equipos de tecnología dentro de la Corte Constitucional se deberá seguir un protocolo de compras públicas, el cual establece que se debe realizar un análisis y su respectiva planificación para luego poder ser implementado, todo esto de acuerdo a las necesidades de la entidad que son especificadas a principios de año en al Plan Operativo Anual[47].

[47] **POA (Plan Operativo Anual),** es un documento formal en el que se enumeran, por parte de los responsables de una entidad los objetivos a conseguir durante el presente ejercicio. Obtenido en, http://www.sinnexus.com/business_intelligence/plan_operativo_anual.aspx.

La adquisición e implementación de los equipos se realizará en base a las necesidades inmediatas de la Corte con los estándares necesarios para que se acople de la mejor manera a la red actual, sin descuidar la seguridad de la información.

Como se mencionó anteriormente el cableado estructurado en cada uno de los pisos se encuentra estandarizado con cable categoría 5e, para interconectar cada una de las estaciones de trabajo con el switch de capa 2 marca Cisco, modelo 2960, este equipo controla el paso de información hacia el BackBone principal de la entidad.

Figura 2.9: Switchs Cisco 2960
Autor: Tesista
Fuente: Corte Constitucional

La capacidad de cada switch según su número de puertos se encuentran ubicados dependiendo de las necesidades de cada piso y esta distribución se detalla en la siguiente tabla:

PISO	NÚMERO DE PUERTOS
Piso 1	Switch 48 puertos
Piso 2	Switch 24 puertos
Piso 3	Switch 24 puertos
Piso 4	Switch 24 puertos
Piso 5	Switch 24 puertos
Piso 6	Switch 24 puertos
Piso 7	Switch 24 puertos
Piso 8	Switch 48 puertos
Piso 9	Switch 24 puertos
Piso 10	Switch 24 puertos

Tabla 2.2: Ubicaciones de Switch 2960 en pisos de la Corte Constitucional
Autor: Tesista
Fuente: Departamento de Tecnología

Como se pudo apreciar anteriormente en la Tabla 2.2, a excepción del primer y octavo piso que utilizan Switch de 48 puertos debido a la cantidad de usuarios que poseen, los demás pisos utilizan tan solo switchs de 24 puertos para abastecer a todas las estaciones de trabajo.

Dentro de este módulo también se realizará un breve análisis del “Módulo de Edificio 2” y el “Módulo Regionales” que se pudo apreciar en la Figura 2.1, puesto que estos módulos utilizan los recursos de red de la Corte Constitucional.

2.1.1.4.1 Modulo de Edificio 2

La Corte Constitucional dentro de su Data Center brinda soporte de red al Registro Oficial, entidad del estado que trabajan con una de sus áreas de forma externa llamada Editora, para generar documentación necesaria para el estado como es el “Registro Oficial”, este documento se interpreta como el diario del Estado, en el que se publican todas las leyes, decretos, acuerdos, resoluciones y demás actos normativos emitidos por los organismos y entidades del Estado; además de las decisiones y resoluciones de los órganos de la Comunidad Andina, así como sentencias expedidas por la Corte Suprema de Justicia; resoluciones del Tribunal Constitucional, ordenanzas municipales y provinciales, y toda aquella normativa que dictamine la ley; y por otro lado la “Editora”, que contribuye con la impresión, distribución y repositorio para almacenar Registros Oficiales desde Enero del año 2000 hasta la presente fecha.

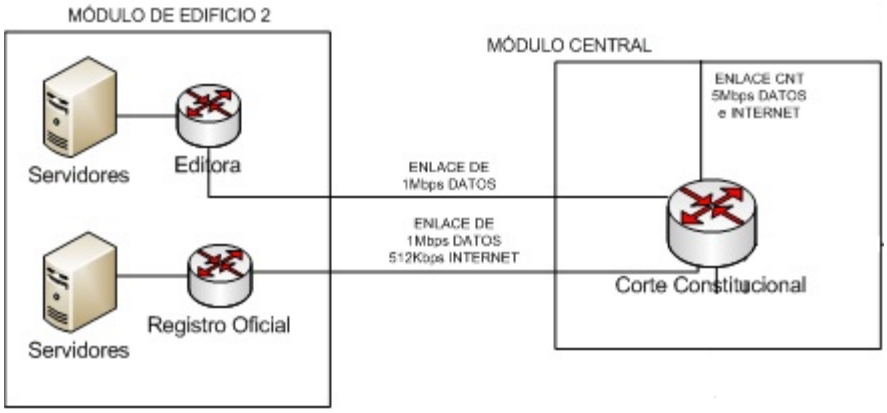


Figura 2.10: Enlace con el Registro Oficial y la Editora
Autor: Tesista
Fuente: Corte Constitucional

La conexión con el Registro Oficial y la Editora se realiza mediante una IP pública a través de un enlace de datos de 1Mbps, se debe tomar en cuenta que los servidores y servicios que presta el Registro Oficial se encuentran dentro del Data Center de la Corte, por esta razón es que utiliza el equipo de Core marca Cisco 3560G para conectarse con la Editora, que como se mencionó anteriormente es un departamento externo que utiliza un equipo Cisco 805SOH para establecer este enlace de información.

2.1.1.4.2 Módulo Regionales

El Data Center de la Corte Constitucional también brinda la conexión respectiva a las ocho oficinas regionales que se encuentran ubicadas en las siguientes ciudades:

- Esmeraldas
- Ibarra
- Portoviejo
- Guayaquil
- Cuenca
- Machala
- Loja y Riobamba.

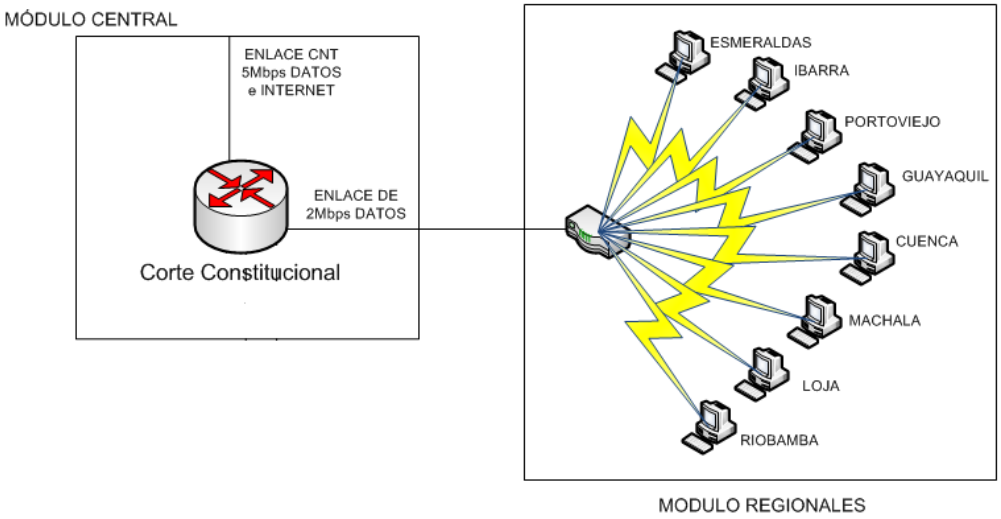


Figura 2.11: Enlace con las Regionales
Autor: Tesista
Fuente: Corte Constitucional

La conexión a estas ocho oficinas regionales se hace a través de dos equipos, el primero que es el Switch Core Cisco 3560G y el segundo un Switch Cisco 805SOH, equipo ubicado en cada una de las regionales para mantener conexión con la Corte, el enlace de datos se realiza utilizado una IP pública por medio de la cual fueron creadas 8 VLANs para poder conectar cada regional, las características de estos enlaces son:

- Canal de datos dedicado a base de Fibra Óptica
- Enlace de datos de 1Mbps para cada regional
- Enlace de internet 2Mbps compartido para todas las regionales
- Disponibilidad de servicio mayor o igual al 99,6% mensual
- Soporte 24horas x 7días x 1año.

Este enlace debe mantener un buen nivel de calidad de servicio (QoS[48]), puesto que, por lo general se necesita realizar enlaces de video conferencia para generar sentencias o dictaminar fallos desde la matriz principal ubicada en Quito hacia sus distintas oficinas regionales. Todas las estaciones de trabajo ubicadas en las oficinas regionales se encuentran agregadas dentro del Active Directory propio de la Corte para determinar sus privilegios dentro de la red.

2.1.1.5 Módulo de Internet

Este módulo facilita a los usuarios finales de la Corte Constitucional el acceso hacia Internet y a usuarios externos el acceso a la información de los servidores públicos que contienen la información necesaria como la página web. El equipo que actualmente integra este módulo es el Ruteador Cisco 1900 Series.

Figura 2.12: Equipo Cisco 1900 Series
Autor: Tesista
Fuente: Data Center

[48] **QoS (Quality of Service),** la Calidad de Servicio son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado. Obtenido en, http://es.wikipedia.org/wiki/Calidad_de_servicio.

Este ruteador Cisco 1900 Series es de propiedad de la Corporación Nacional de Telecomunicaciones (CNT), y se lo instaló cuando la Corte Constitucional contrató el servicio de Enlace de Datos e Internet, el Acuerdo de Nivel de Servicio[49] (Anexo C) goza de las siguientes características:

- Canal de datos dedicado a base de Fibra Óptica
- Enlace de datos e internet de 5Mbps
- Adquisición de 15 IPs públicas
- Disponibilidad de servicio mayor o igual al 99,6% mensual
- Soporte 24horas x 7días x 1año.

La seguridad del enlace y de este equipo se encuentra a cargo de la CNT, entidad responsable de bloquear puertos y todo lo necesario para garantizar una comunicación segura. El único problema que enfrenta actualmente la Corte Constitucional es que no posee un proveedor de Internet que brinde servicio de redundancia como soporte de conexión.

2.1.2 Protocolos

Continuando con el análisis de la red de datos de la Corte Constitucional en esta sección se estudiarán los protocolos de comunicación utilizados. Específicamente se enfocará en el estudio del protocolo TCP/IP[50] (Protocolo de control de transmisión/protocolo de Internet). Existen otros protocolos que por no estar estandarizados dentro de la red no se han tomado en cuenta.

Para realizar esta labor se ha visto necesario el dividir este estudio en tres partes: direccionamiento, enrutamiento y gestión de configuración actual del protocolo TCP/IP.

---

[49] **SLA (Service Level Agreement),** Un acuerdo de nivel de servicio es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. Obtenido en, http://es.wikipedia.org/wiki/Acuerdo_de_nivel_de_servicio

[50] **TCP/IP (Transmission Control Protocol/Internet Protocol)**, Protocolo de Control de Transmisión/Protocolo de Internet, es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras. Obtenido en, http://es.wikipedia.org/wiki/ Familia_de_protocolos_de_Internet.

2.1.2.1 Direccionamiento

Dentro de la red de datos de la Corte Constitucional se encuentra instalado como estándar de comunicación el protocolo TCP/IP, que cuenta con una red de clase C 192.168.0.0, a partir de esta dirección, se crean los segmentos de red necesarios según los requerimientos de expansión de la red y que para la distribución de direcciones IP a todas las estaciones de trabajo se lo hace mediante el uso de VLANs, que están generadas de la siguiente forma:

#	VLAN	DIRECCIÓN IP	MÁSCARA	# IPs Grupo
1	Administración	192.168.15.1	255.255.255.224	30
2	Secretaría General	192.168.7.1	255.255.255.224	30
3	Servidores	192.168.8.1	255.255.255.192	62
4	Impresoras	192.168.13.1	255.255.255.128	126
5	Jueces Corte Constitucional	192.168.10.1	255.255.255.240	14
6	DMZ	192.168.2.1	255.255.255.248	2
7	Secretaría Técnica	192.168.7.33	255.255.255.224	30
8	Secretaría Técnica Jurisdiccional	192.168.7.65	255.255.255.224	30
9	Presidencia Vicepresidencia	192.168.5.1	255.255.255.240	14
10	Centro de Estudios	192.168.6.1	255.255.255.192	62
11	Adm RRHH	192.168.14.1	255.255.255.224	30
12	Asesores	192.168.9.1	255.255.255.0	254
13	Jurídico	192.168.11.1	255.255.255.224	30
14	Sistemas Comunicaciones	192.168.12.1	255.255.255.224	30
15	Usuarios Externos	192.168.3.1	255.255.255.224	30
16	Público General	192.168.4.1	255.255.255.224	30
17	Vlan 160 Administración	192.168.16.1	255.255.255.192	62
18	Vlan 170 Administración	192.168.17.1	255.255.255.192	62

Tabla 2.3: Direccionamiento IP Corte Constitucional
Autor: Tesista
Fuente: Departamento de Tecnología

Todo el direccionamiento IP[51] de la red de datos se encuentra debidamente direccionado y dividido según el departamento o aplicación al que se quiera brindar servicio de conexión, de esta forma si un funcionario tiene que cambiarse de área por cualquier motivo se le tendrá que cambiar de VLAN dependiendo del área al que haya sido reasignado; de esta forma se puede mantener conocimiento necesario sobre los dispositivos que están utilizando una determinada dirección de red, así como a que VLAN pertenece y qué función está cumpliendo. La seguridad está dada según la dirección IP asignada y la dirección MAC de la máquina del usuario, así bien, si quiere conectarse a otro punto de red que no se encuentre dentro de su VLAN registrada, no obtendrá conexión alguna.

Adicionalmente la Corte posee 15 direcciones IP públicas para poder mantener los enlaces con sus oficinas regionales, para generar video conferencias y para conectarse con otras entidades; su distribución es la siguiente:

#	IP PÚBLICA
1	186.42.101.2
2	186.42.101.3
3	186.42.101.4
4	186.42.101.5
5	186.42.101.6
6	186.42.101.7
7	186.42.101.8
8	186.42.101.9
9	186.42.101.10
10	186.42.101.11
11	186.42.101.12
12	186.42.101.13
13	186.42.101.14
14	186.42.101.1
15	186.42.101.15

Tabla 2.4: Direccionamiento IP Público Corte Constitucional
Autor: Tesista
Fuente: Departamento de Tecnología

[51] **IP (Internet Protocol) el Protocolo de Internet,** es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados no fiable y de mejor entrega posible sin garantías. Obtenido en, http://es.wikipedia.org/wiki/Internet_Protocol.

Las primeras 13 direcciones de la Tabla 2.4 se utilizan generalmente para enlaces externos, y las direcciones que constan en la posición 14 y 15 son utilizadas para dar servicio de broadcast[52] a la red.

2.1.2.2 Enrutamiento

El enrutamiento propio de la Corte Constitucional se lo realiza de forma estática, esta ruta está conformada por el Switch de Core Cisco 3560G y de éste, tanto al ISP[53] como a la red interna de la entidad. El enrutamiento necesario entre segmentos de red lo realiza el Switch de Core Cisco 3560G, en el cual se encuentran creadas las tablas de ruteo para direccionar el tráfico a todas los segmentos de red. Cada segmento de la red ha sido creado en base a requerimientos o necesidades de cada departamento o servicio que se desee proporcionar a los usuarios, y por lo general se lo realiza con enrutamiento estático.

La gestión de enrutamiento para cada piso de la entidad se lo realiza con switchs de capa 2 Cisco 2960 que ayudan a encaminar los paquetes de datos hacia su destino final.

2.1.2.3 Sistema de Gestión

Todas las estaciones de trabajo de la Corte Constitucional son administradas y configuradas dentro del Active Directory[54], servicio que proporciona la opción de dividir los departamentos de la entidad en 28 unidades organizacionales que se encuentran dentro de un dominio en común llamado, cce.gob.ec, este proceso permite al Administrador de la red crear grupos de usuarios, permisos y asignación de recursos y políticas de acceso según la jerarquía del usuario dentro de cada departamento.

---

[52] **Broadcast,** difusión en español, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo. Obtenido en, http://es.wikipedia.org/wiki/Broadcast_(informática).

[53] **ISP (Internet Service Provider),** un proveedor de servicios de Internet es una empresa que brinda conexión a Internet a sus clientes. Obtenido en, http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet.

[54] **Active Directory,** es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Obtenido en, http://www.microsoft.com /latam/technet/productos/windows/windowsserver2003/admng.mspx.

A través del Active Directory se puede establecer políticas al dominio de la organización, a las unidades organizacionales, a los grupos de usuarios o a las estaciones de trabajo sin la necesidad de movilizarse por toda la entidad, también desplegar programas en muchos ordenadores y aplicar actualizaciones críticas. Con respecto a la seguridad, las claves asignadas dentro del Active Directory dependen de que la cuenta corresponda al administrador o a un usuario, de la siguiente manera:

Administrador.- existe solo un administrador del servicio que regula las políticas hacia toda la entidad y posee con una clave que necesita ser renovada cada 90 días por motivos de seguridad.

Usuarios.- la clave de cada usuario dentro del Active Directory caduca cada 60 días, a parte sus servicios de navegación y activación de cuenta dentro de la red se encuentran regulados al horario de 8am a 8pm de lunes a viernes, el ingreso que no sea dentro de estos horarios se encuentra restringido y solo se habilitará con previa solicitud y aprobación por el Director del Departamento de Tecnología.

Cabe detallar que todas las estaciones de trabajo dentro de la entidad se encuentran trabajando con sistema operativo Windows XP y Windows 7 como plataforma para los usuarios.

Por otra parte el inventario de software y hardware de todas las estaciones de trabajo dentro de la red de la Corte Constitucional se lo hace por medio del programa llamado OCSInventory, software libre que permite al Administrador de la Red administrar el inventario de todos los activos de tecnología, esta herramienta utiliza una estructura cliente servidor, el servidor recopila la información que le envía un software agente instalado en cada una de las estaciones de trabajo y la visualización de toda la información recabada se la hace por medio de una interfaz web.

Figura 2.13: Opciones OCS Inventory
Autor: Tesista
Fuente: Departamento de Tecnología

Entre las opciones del programa como se observa en la Figura 2.13 se podrá encontrar información sobre: procesador de la computadora, memoria, capacidad de disco duro, particiones de disco duro, tarjeta de sonido, tarjeta de video, puertos disponibles, adaptadores de red, impresoras conectadas, sistema operativo, actualizaciones instaladas, dominio al que pertenece la computadora, entre varias opciones más.

Con respecto al monitoreo del ancho de banda de la Corte Constitucional, actualmente se cuenta solo con el servicio que brinda la aplicación MRTG[55] de la CNT, la cual realiza un monitoreo continuo sobre la carga de tráfico que pasa a través de la red, sin embrago, se debería contar con una herramienta propia para mantener un análisis constante de todos los paquetes en la red.

Por último, el único segmento de la red en el que se utiliza direccionamiento dinámico DHCP[56] se encuentra en el Departamento de Tecnología, ya que posee un Acces Point marca Cisco para dar servicio de red inalámbrica al departamento, esta WLAN[57] se encuentra limitada a 10 conexiones simultaneas y protegida con su respectiva clave.

[55] **MRTG (Multi Router Traffic Grapher),** es una herramienta que se utiliza para supervisar la carga de tráfico de interfaces de red. Obtenido en, http://es.wikipedia.org/wiki/MRTG.
[56] **DHCP (Dynamic Host Configuration Protocol),** el protocolo de configuración dinámica de host, es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Obtenido en, http://es.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol.
[57] **WLAN (Wireless Local Area Network),** una red de área local inalámbrica, es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas. Obtenido en, www.gsmspain.com/glosario/?palabra=WLAN.

2.1.3 Aplicaciones y Servicios

Los servicios que presta la red de datos de la Corte Constitucional son: acceso a internet, correo electrónico y DNS interno. Por cuestión de seguridad de la información ningún otro servicio se encuentra permitido.

Por otra parte las aplicaciones que se encuentran corriendo a través de la red se encuentran especificadas en la siguiente tabla:

#	APLICACIONES
1	Sistema de Gestión de Acciones Constitucionales
2	Directorio telefónico
3	Registro de casos
4	Requerimiento de contratos
5	Secretaria técnica jurisdiccional
6	Seguimiento de proyectos centro de estudios
7	HelpDesk Incidentes
8	Gestión Social RRHH
9	Registro Oficial en la red
10	Facturación Registro Oficial
11	Antivirus
12	Correo Electrónico
13	Página Web
14	Servidor de archivos
15	Servidor de impresiones
16	Active Directory
17	Cámaras de Seguridad
18	Polycom video conferencia
19	Lexis (Consulta Jurídica Nacional)
20	Vlex (Consulta Jurídica Internacional)

Tabla 2.5: Aplicaciones de la Corte Constitucional
Autor: Tesista
Fuente: Departamento de Tecnología

Todos los servicios creados se los ha implementado en base a las necesidades del personal de la Corte para poder brindar disponibilidad, rendimiento y seguridad. Sin embargo, tomando en cuenta la confidencialidad de la información que fluye día a día, si sería recomendable incluir seguridad de red como: un sistema de detección de intrusos, un sistema que evite la fuga de información,

entre otros para garantizar la seguridad de la información. Por estas razones sería muy útil, planificar, organizar, coordinar, dirigir y controlar todas estas actividades por medio de un grupo especializado que se encargue de toda la seguridad de la red.

2.1.3.1 Acceso a Internet

El acceso a internet se lo obtiene por medio de la Corporación Nacional de Telecomunicaciones[58] que brinda un enlace de 5 Mbps para datos e Internet, este servicio es el más utilizado por todos los funcionarios de la Corte Constitucional para poder desempeñar sus labores diariamente, todas las políticas de seguridad sobre la salida a internet se encuentran reguladas por el Administrador de la Red, que ha denegado servicios como: uso de chat, descarga de videos, música e instalación de programas. Estas medidas se han tomado para mantener un buen rendimiento y disponibilidad de la red.

Como seguridad adicional a la que ya se tiene actualmente se debería agregar un sistema de filtrado de URLs o de control de aplicaciones para mantener un mejor control sobre las búsquedas y visitas de cada usuario a las páginas web.

2.1.3.2 Página Web Corte Constitucional

Dentro de las distintas publicaciones y actualizaciones de la página web el Departamento de Tecnología solo se encarga de controlar la seguridad y el buen funcionamiento del servidor, por estas razones solo se encuentra habilitado el puerto 80 para ingreso y salida de información con una capacidad de almacenamiento de 10GB, ya que la administración como tal del portal institucional se encuentra a cargo del Departamento de Comunicación Social, que está en la obligación de publicar información actualizada constantemente.

[58] **CNT,** Corporación Nacional de Telecomunicaciones, empresa estatal que brinda servicios de telefonía e internet. Obtenido en, www.cnt.gob.ec

2.1.3.3 Correo Electrónico

El servicio de correo electrónico de la Corte Constitucional se encuentra montado sobre un servidor SendMail de plataforma abierta que brinda todas las facilidades sobre políticas de gestión para sus usuarios como son:

- **Creación de cuentas.-** cada funcionario que sea parte de la entidad tendrá su cuenta de correo electrónico con su respectivo nombre de usuario y contraseña, a su vez, cada cuenta de usuario pertenecerá a un grupo, según el departamento de referencia, para que de esta manera se pueda facilitar el envío de correos en toda la entidad.
- **Creación de listas distribuidas.-** este sistema permite asociar un nombre de grupo a una serie de direcciones IP, de forma que al enviar un mensaje a ese grupo, automáticamente se está enviando el mensaje a todas las direcciones que tiene asociadas, eliminando el problema de que se detecten los correos como Spam[59] por enviarlos a los usuarios de forma masiva.
- **Capacidad de almacenamiento.-** el servidor de correo actualmente posee un almacenamiento de 30GB, sin embargo hay que detallar que ya se encuentra a un 90% de su capacidad, por este motivo se piensa en posibilidades de migración a otro servidor con mejores prestaciones.
- **Seguridad física.-** como parte de seguridad del servidor se encuentran habilitados solo los puertos 25 y 110 que hacen referencia a los protocolos SMTP y POP3 respectivamente, todos los demás puertos se encuentran cerrados.
- **Seguridad lógica.-** el servicio de correo se encuentra protegido por tres herramientas: un AntiSpam de McAfee, un antivirus propio del servicio de correo llamado ClamAV y un escáner de correos llamado MailScanner, todo esto para evitar tanto el correo basura como para evitar infecciones por virus a través de envio de información.

[59] **SPAM correo basura o mensaje basura,** así se denomina a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. Obtenido en, http://es.wikipedia.org/wiki/Spam.

Todos estos servicios permiten a los funcionarios la comunicación interna y externa mediante el protocolo SMTP[60] (Protocolo de Transferencia Simple de Mensajes) para el envío de mensajes y el protocolo POP3[61] (Protocolo de Oficina de Correo) para la descarga de mensajes en las diferentes estaciones de trabajo de la Corte.

La única herramienta que podría integrarse para mejorar la seguridad a través de correo electrónico, es implementar un sistema anti fuga de información, teniendo en cuenta la documentación que se maneja a diario en la Corte.

2.1.3.4 Configuración DNS

Primeramente cabe detallar que un DNS o Servicio de Nombres de Dominio es un sistema de nomenclatura para computadores que ayuda a traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP), que es la forma en la que las máquinas pueden encontrarse a través de Internet.

En la red de la Corte Constitucional existen dos servicios de DNS el primero se encuentra instalador dentro de de un servidor Squid[62], que es un programa de software libre que implementa un servidor proxy configurado en el puerto 3128 para salida a internet y un dominio para almacenamiento de páginas web, de esta manera se puede acelerar las búsquedas en la web por medio de las peticiones a DNS repetidas, además de añadir seguridad filtrando el tráfico. Y el segundo DNS se encuentra dentro del Active Directory el cual ayuda a resolver los nombres de funcionarios en direcciones IP para poder tener constancia de su localización y autentificación en el dominio de la red para poder tener los respectivos privilegios.

---

[60] **SMTP (Simple Mail Transfer Protocol),** se utiliza para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos. Obtenido en, http://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol.

[61] **POP3 (Post Office Protocol),** se utiliza en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Obtenido en, www.alegsa.com.ar/Dic/pop3.php.

[62] **Squid,** es un programa que ayuda a implementa un servidor proxy y utiliza un dominio para caché de páginas web. Obtenido en, http://es.wikipedia.org/wiki/Squid_%28programa%29.

El dominio de la Corte Constitucional es:

- @cce.gov.ec
- El DNS principal es 192.168.17.14
- El DNS secundario es 192.168.17.22

Con esta configuración el DNS del Active Directory resuelve los nombres de funcionarios dentro de la red para estabilizar conectividad.

2.1.4 Trafico de Red

En esta sección se analizará el tráfico de red que generan los usuarios al utilizar los tres principales servicios de la Corte Constitucional que son:

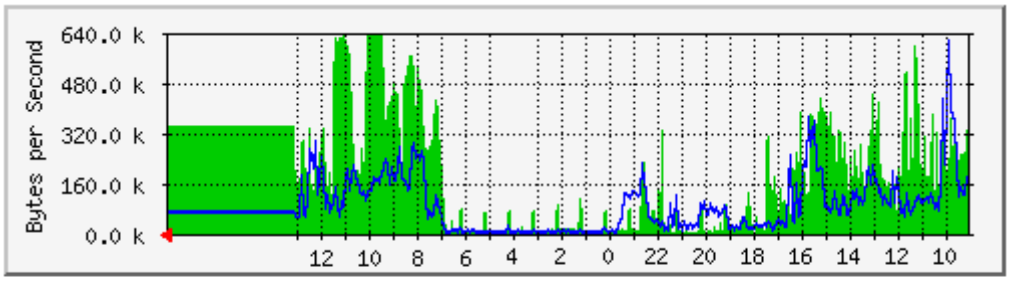
- Carga de tráfico sobre la red
- Carga de tráfico del servicio web
- Carga de tráfico del correo electrónico

A continuación se desglosa la información de cada uno de estos servicios.

2.1.4.1 Carga de tráfico sobre la red

Para tener la capacidad de medir el tráfico de red se utilizó la herramienta MRTG[63], configurada para que analice todo el tráfico que pasa a través del Switch Core Capa 3 de la Corte Constitucional, con este direccionamiento se podrá obtener mediciones sobre el nivel de utilización y carga de información que posee actualmente la red de datos. De esta medición realizada, se obtuvo un informe sobre los últimos 10 días de análisis con los siguientes resultados como muestra la Figura 2.14:

[63] **MRTG (Multi Router Traffic Grapher),** es una herramienta que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera informes en formato HTML con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo. Obtenido en, http://es.wikipedia.org/wiki/MRTG.



	Max	Average	Current
In	631.5 kB/s (5.1%)	206.5 kB/s (1.7%)	345.5 kB/s (2.8%)
Out	613.4 kB/s (4.9%)	84.7 kB/s (0.7%)	65.4 kB/s (0.5%)

Figura 2.14: Carga de tráfico Semanal
Autor: Tesista
Fuente: Departamento de Tecnología

Como se puede observar la carga de tráfico de red que se genera diariamente y estos valores se encuentran representados en Kilobytes/segundo. De acuerdo a estos valores el promedio de salida de información sobre la red representa una tasa de transmisión de 84,7 Kb/s, mientras que el promedio diario de ingreso de información es de 206,5 Kb/s. De igual forma la cantidad máxima de Kbps que ingresa a la red es de 631,5 Kb/s, y la cantidad máxima que sale de este es de 613,4 Kb/s. Estos valores reflejan una mayor cantidad de tráfico a partir de las 7:00 hasta las 12:00 horas del medio día y en horas de la tarde disminuye gradualmente desde las 13:00 hasta las 18:00 horas que los funcionarios de la Corte Constitucional terminan sus respectivas labores. Es importante notar que entre las 21:00 y 23:00 horas existen conexiones de acceso remoto, actualizaciones o respaldos que ocupan cierta carga de recursos en la red.

2.1.4.2 Carga de tráfico del servicio web

De la misma forma se realizó el análisis estadístico sobre el número de visitas que posee el sitio Web de la Corte Constitucional, www.corteconstitucional.gob.ec, para este proceso se utilizó la herramienta AWStats[64], que nos brinda un completo informe sobre el número de visitas que se realizo a diario, el tráfico generado, entre otras opciones que se muestran a continuación en la Figura 2.15:

[64] **AWStats,** es una herramienta open source de informes sobre análisis de datos de servicios de Internet como un web, streaming, mail y FTP. AWstats analiza los archivos de log del servidor, y con base a ellos produce informes HTML. Obtenido en, http://es.wikipedia.org/wiki/Awstats.

Día	Número de visitas	Páginas	Solicitudes	Tráfico
01 Abr 2012	137	660	7,774	135.50 MB
02 Abr 2012	432	2,942	29,703	384.39 MB
03 Abr 2012	411	2,867	27,886	328.67 MB
04 Abr 2012	385	3,472	28,142	368.54 MB
05 Abr 2012	130	1,031	10,487	116.62 MB
06 Abr 2012	0	0	0	0
07 Abr 2012	0	0	0	0
08 Abr 2012	0	0	0	0
09 Abr 2012	422	2,695	28,448	387.15 MB
10 Abr 2012	472	3,054	33,290	435.91 MB
11 Abr 2012	55	352	4,231	46.13 MB

Figura 2.15: Carga de tráfico del servicio Web
Autor: Tesista
Fuente: Departamento de Tecnología

Como se puede observar se ha obtenido el reporte de los últimos 10 días de visitas a la página web de la Corte, con un promedio de 306 visitas diarias al portal web institucional, y la carga de tráfico que se generó diariamente en la red. El resumen sobre los distintos visitantes, el número de visitas, las páginas visitadas, las solicitudes realizadas y el tráfico generado se muestra en la Figura 2.16 a continuación:

Visitantes distintos	Número de visitas	Páginas	Solicitudes	Tráfico
1,501	**2,444** (1.62 visitas/visitante)	**17,073** (6.98 Páginas/Visita)	**169,961** (69.54 Solicitudes/Visita)	**2.15 GB** (922.99 KB/Visita)

Figura 2.16: Resumen sobre la carga de tráfico del servicio Web
Autor: Tesista
Fuente: Departamento de Tecnología

En la figura anterior se pudo observar que las visitas al portal web institucional generaron un tráfico de 2,15 Gb en los últimos 10 días, con un número total de visitas que asciende a 2444 personas, atendiendo 169,961 solicitudes a través del sitio web.

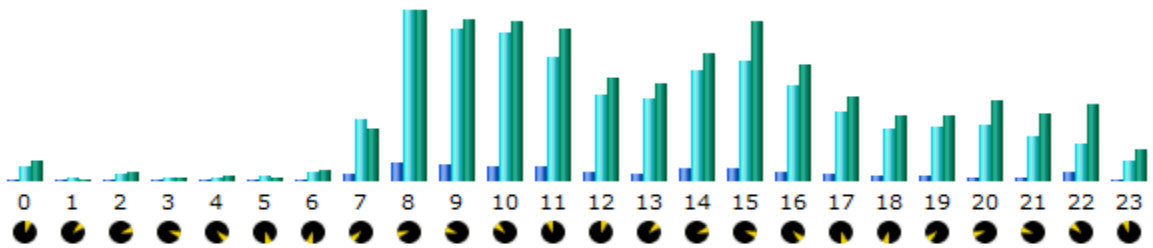


Figura 2.17: Uso diario del servicio Web
Autor: Tesista
Fuente: Departamento de Tecnología

Por otra parte en la Figura 2.17 se puede apreciar que las horas pico en que los usuarios acceden al sitio Web están entre las 8:00 y 11:00 horas en la mañana y en la tarde entre 14:00 y 15:00 horas.

2.1.4.3 Carga de tráfico correo electrónico

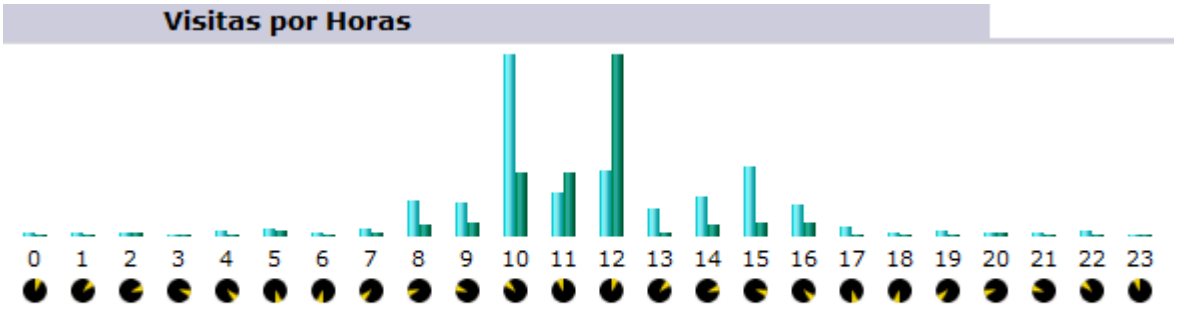
Para analizar la cantidad de mensajes enviados y recibidos, se estudiarán los logs que generó el servidor de SendMail durante los últimos días, mediante la utilización de la herramienta AWStats, la misma que ayudará a generar reportes del servicio de correo y de esta manera poder visualizar los promedios de utilización de este servicio tanto de entrada como de salida, como se muestra en la Figura 2.18:

Visitantes distintos	Correos	Tamaño
Correos electrónicos enviados con éxito	**3,017**	**1.16 GB** (404.74 KB/Correos)
Correos electrónicos incorrectos o rechazados	**489**	**1.88 MB**

Figura 2.18: Estadística de Correo Electrónico
Autor: Tesista
Fuente: Departamento de Tecnología

De este análisis se pudo obtener que el servidor SendMail dejó un total de 3,017 correos electrónicos enviados con éxito, representando una carga de tráfico sobre la red de 1,16 Gb y que en promedio de resultaría un tamaño de 404,74 Kb por correo enviado satisfactoriamente. Los correos electrónicos incorrectos o rechazados son considerados por el sistema como Spam, por esta razón es que 489 fueron descartados con una tasa de transferencia sobre la red de 1,88 Mb.

Mediante este proceso también se pudo observar que tanto para el envío como para la recepción de correo electrónico el servicio es más utilizado en días laborables que en fines de semana, como se muestra a continuación en la Figura 2.19:



Visitas por Horas	Correos	Tamaño	Visitas por Horas	Correos	Tamaño
00	13	140.03 KB	12	338	550.06 MB
01	13	905.95 KB	13	136	10.70 MB
02	16	7.88 MB	14	202	31.30 MB
03	8	1.00 MB	15	355	39.77 MB
04	27	342.39 KB	16	163	42.41 MB
05	32	13.41 MB	17	46	6.00 MB
06	17	190.45 KB	18	15	2.14 MB
07	32	7.78 MB	19	23	1.38 MB
08	178	36.60 MB	20	20	10.91 MB
09	167	42.51 MB	21	20	2.46 MB
10	938	190.69 MB	22	24	3.04 MB
11	227	190.85 MB	23	7	78.94 KB

Figura 2.19: Horario de tráfico de Correo Electrónico
Autor: Tesista
Fuente: Departamento de Tecnología

Como se puede observar en el gráfico anterior las horas pico en que los funcionarios utilizan el servicio de correo electrónico están entre las 10:00 y 12:00 horas en la mañana y en la tarde a las 15:00 horas, horarios que representan las tasas de transferencias más altas que se registran a diario sobre la red.

Después de haber analizado toda la situación inicial de la infraestructura tecnológica de la Corte Constitucional, en el siguiente capítulo se analizará los posibles riesgos y vulnerabilidades de la red de datos.

CAPITULO 3

ANÁLISIS DE RIESGOS Y VULNERABILIDADES DE LA RED DE DATOS DE LA CORTE CONSTITUCIONAL

3.1 RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN

3.1.1 Definición de Riesgo

Según ISACA[65] un riesgo dentro de las Tecnologías de la Información se considera como: un factor identificado que podría afectar la consecución de un objetivo.

Y un riesgo a la seguridad de la información según ISACA es un "acontecimiento adverso que materializa una amenaza cuando una vulnerabilidad se explota, afectando uno o más activos de información, el cual es reflejado en cualquiera de las siguientes características de la información":

- Confidencialidad
- Integridad
- Disponibilidad.

La ISO (Organización Internacional de Estándares) por su parte define que: "El riesgo es la posibilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes en un activo o grupos de activos, generándose así, perdidas o daños a la infraestructura de la institución".

En resumen un Riesgo para la Corte Constitucional puede considerarse como: la posibilidad de sufrir daño de infraestructura o pérdida de información; se debe comprender y analizar su potencial para asumir las consecuencias negativas de un evento. El riesgo refiere a una situación en la cual una persona puede generar un evento indeseable o un acontecimiento natural puede causar un resultado indeseado de vulnerabilidad, teniendo un impacto negativo dentro de la entidad.

[65] **ISACA (Information Systems Audit and Control Association),** organización líder en establecer pautas para los profesionales sobre el gobierno, control, seguridad y auditoría de tecnologías de la información. Obtenido en, http://www.isaca.org/About-ISACA/History/Espanol/Pages/default.aspx

3.1.2 Componentes del Riesgo

3.1.2.1 Procesos y Activos

Son todos y cada uno de los componentes sobre los cuales se gestiona el normal funcionamiento de una empresa o institución. Se incluye en estos todos los activos, tanto físicos como de información. Se compone de los siguientes elementos:

Activos físicos: son aquellos elementos tangibles dentro de la estructura de una institución y que sirven como soporte para el desarrollo de la misma como por ejemplo: el edificio de la Corte Constitucional, su infraestructura interna, los elementos tecnológicos y las distintas estaciones de trabajo para cada uno de los funcionarios.

Activos de información: son aquellos elementos no tangibles que ayudan a controlar tanto aplicaciones como infraestructura tecnológica y de esta manera poder mantener una comunicación confiable a través de toda la entidad, estas aplicaciones pueden ser: bases de datos, aplicaciones, sistemas de gestión, sistemas de monitoreo, archivos de datos y sistemas operativos.

3.1.2.2 Impacto del riesgo

El impacto que pueda producir un riesgo es la consecuencia que se tendría dentro de los activos de la Corte Constitucional tanto físicos como de información, si es que llega a producirse un posible daño eventual ligado a la probabilidad de ocurrencia del riesgo, en donde éste se convertiría en un caso real.

Por ejemplo, el impacto de una brusca variación de voltaje en la Corte Constitucional se valoraría utilizando una escala de acuerdo a la prioridad, valor y funcionalidad que tienen los activos afectados dentro de la institución.

3.1.2.3 Probabilidad

Es la combinación entre la frecuencia de ocurrencia de la amenaza y el impacto que podría producir si se repite constantemente dentro de la Corte Constitucional, es decir, con qué periodicidad ocurre la amenaza dentro de la institución y el grado de impacto que esta u otra actividad podría dejar a su paso después de ocasionar un riesgo físico o lógico.

3.1.3 Riesgos en Tecnologías de la Información

Según el "Marco de Riesgos de Tecnologías de Información[66]" que realiza ISACA, los riesgos se encuentran ligados a la exposición de los activos que conforman la unidad de TI[67] de la Corte Constitucional, a una actividad que represente una amenaza para los mismos. Dentro de este ambiente se podría catalogar las siguientes categorías para TI:

- **Riesgos asociados a catástrofes.-** aquellos eventos asociados a fuerzas naturales de destrucción, por ejemplo, terremotos, maremotos, inundaciones entre otros.
- **Riesgos por variaciones y pérdida del flujo eléctrico.-** son los eventos ligados al suministro eléctrico del que la institución dispone a través de un servicio público o privado.
- **Riesgos por mal uso o mala configuración de equipos.-** son los que tienen que ver con una errónea manipulación o uso de los equipos que forman parte de los activos de la información, por ejemplo una configuración descuidada de un equipo o borrado de registros de una base de datos por un mal uso de las aplicaciones.
- **Riesgos de pérdida de la información.-** son aquellos asociados al desvanecimiento de la información almacenada en medios magnéticos debido

[66] **ISACA Risk IT,** análisis y administración de riesgos en tecnologías de información. Obtenido en, http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx.
[67] **TI (Tecnologías de la Información),** agrupan los elementos y las técnicas usadas en el tratamiento y la transmisión de las informaciones. Obtenido en, es.wikipedia.org/wiki/Tecnologías_de_la_información_y_la_comunicación.

a daños de las fuentes de almacenamiento o incursión deliberada de process que generen actividades de supresión de registros y/o archivos.

- **Riesgos por caídas del sistema.-** son los que involucran pérdidas tanto de datos como económicas por el deceso o fallo de los sistemas de información que soporten los distintos procesos considerados como críticos para la Corte Constitucional.
- **Riesgos por vandalismo.-** son aquellos que están ligados a la destrucción física o lógica de la integridad de los equipos, de los cuales depende el funcionamiento de las aplicaciones y servicios que ofrece el Departamento de Tecnología de la Corte Constitucional.
- **Riesgos por pérdida de equipos o partes.-** estos están vinculados al hurto o pérdida involuntaria de equipos o partes de los mismos, como consecuencia de delitos o accidentes.
- **Riesgos de pérdida de confidencialidad de la información.-** esta clase de riesgos están vinculados netamente al robo de la información de la institución para su posterior divulgación a terceras personas que no deberían obtener tales datos. En este punto tiene que ver mucho sobre el robo o filtración tanto por agentes internos como externos de la institución.
- **Riesgos de autenticación.-** están ligados a la violación del sistema de autenticación que posee la Corte Constitucional para dar acceso a los usuarios autorizados a cierta información o roles administrativos inherentes al cargo que este funcionario ocupa en la institución. También están relacionados con la posibilidad de suplantar la identidad electrónica de un usuario a través del Active Directory de la institución, de modo que se logre un acceso supuestamente autorizado dentro de la red a una persona que simula ser un funcionario permitido para manipular o hurtar archivos sensibles.
- **Riesgos de violación de la integridad.-** Estos están vinculados a la posibilidad de alteración de los datos de un archivo o una base de datos, modificándolos voluntaria o involuntariamente en una situación inesperada, de modo que se añada, suprima o actualice información de manera deliberada o

accidental dentro de las fuentes que contienen dichas referencias, poniendo en peligro la confiabilidad de la información almacenada.

- **Riesgos de pérdida de prestigio institucional.-** están relacionados directamente a la perdida de confiabilidad, prestigio o veracidad de la Corte Constitucional ante los usuarios. Esta clase de riesgo podría representar un altísimo impacto ya que se ofrece un servicio de jurisprudencia a nivel nacional.

En base a esta introducción teórica sobre el riesgo y al análisis que se realizó en el Capítulo 2 sobre la "Situación actual de la red de datos de la Corte Constitucional", a continuación, se detallará el nivel de riesgo de la infraestructura tecnológica de la entidad (Anexo D), con una valoración de 0 a 1 para la probabilidad de riesgo y de 1 a 5 para el nivel de impacto, siendo 1 y 5 los valores más significativos respectivamente, como lo muestra la Tabla 3.1:

Procesos y Activos	Probabilidad del riesgo	Impacto del riesgo
Módulo Central	0.2	3
Módulo Distribución de Edificios	0.2	2
Módulo Servidores	0.2	4
Módulo Edificio	0.5	3
Módulo Edificio 2 y Regionales	0.3	2
Aplicaciones y Servicios	0.4	3
Página Web Corte Constitucional	0.3	5
Correo Electrónico	0.3	3

Tabla 3.1: Análisis de riesgos de la infraestructura tecnológica
Autor: Tesista
Fuente: Tesista

De acuerdo a la tabla anterior, los servidores y la página web de la Corte Constitucional representan el mayor riesgo dentro de la infraestructura, motivo por el cual se realizará el debido análisis de riesgos y vulnerabilidades de estos servicios.

3.2 VULNERABILIDADES EN LAS TECNOLOGÍAS DE INFORMACIÓN

3.2.1 Definición de Vulnerabilidad

Para ISACA una vulnerabilidad representa:

"Una deficiencia en el diseño, la implementación, la operación o la ausencia de los controles internos en un proceso, que podría explotarse para violar la seguridad del sistema."[68]

El término vulnerabilidad caracteriza la ausencia o riesgo de permitir que una amenaza ocurra con mayor frecuencia, gran impacto o cualquiera de los dos. Estas pueden ser explotadas por una amenaza que puede causar daño a todo el sistema de TI o a los objetivos del negocio de la Corte Constitucional.

Hay que tener en cuenta que una vulnerabilidad no causa daño por sí sola; las vulnerabilidades se incluyen en un sistema como debilidades que pueden ser explotadas y pueden conducir a consecuencias indeseables.

Estas se representan como oportunidades que pueden permitir a una amenaza causar daño, como por ejemplo, el no tener instalados los parches necesarios en estaciones de trabajo con sistema operativo Windows o no disponer de un sistema de autentificación de usuarios, son vulnerabilidades que podrían permitir la amenaza de una intrusión y por tanto generarse una pérdida de información o daño de la infraestructura.

3.2.2 Clasificación de las vulnerabilidades

En vista de los diversos tipos de vulnerabilidades que se puede encontrar se los clasificará en los siguientes grupos:

---

[68] **ISACA, An Approach to Vulnerability Management,** apartado sobre aprovechamiento y administración de vulnerabilidades. Obtenido en, http://www.isaca.org/Journal/Past-Issues/2005/Volume-5/Pages/JOnline-An-Approach-to-Vulnerability-Management1.aspx.

- **Vulnerabilidades de diseño.-** es una debilidad inherente dentro del diseño o especificación de hardware o software por medio de la cual hasta una instalación perfecta podría resultar siendo una vulnerabilidad.

  Esta clase de vulnerabilidades representan el mal diseño de aplicaciones de software, bases de datos, modelos relacionales, arquitecturas de red, infraestructura física y sistemas de seguridad, que harán que se tenga que rediseñar todo para que se logren mitigar las amenazas que podrían suscitarse en determinado momento por la ocurrencia del riesgo que representa el tener una vulnerabilidad de ese tipo.

- **Vulnerabilidades de configuración.-** son aquellas vulnerabilidades que resultan de un error en la configuración y administración de un componente de sistema. Generalmente estas vulnerabilidades aparecen como consecuencia de un error humano, como olvidos, omisiones, malas configuraciones de fábrica o por defecto.

- **Vulnerabilidades de implementación.-** son aquellas que están asociadas a actividades de programación errónea de sistemas, implementación incorrecta de hardware o software en ambientes de producción o errores de programación dentro de sistemas. Estas resultan de una implementación de un diseño que parecía satisfactorio, pero termina representando una vulnerabilidad.

- **Vulnerabilidades organizacionales.-** estas se encuentran asociadas a las políticas organizacionales o prácticas que pueden resultar en la ocurrencia de acciones no autorizadas. Las vulnerabilidades son indicaciones de prácticas de seguridad omitidas, erróneas o inadecuadas. Generalmente aparecen cuando no existe la documentación pertinente a las políticas y prácticas de seguridad dentro de la organización, o estas no son debidamente explicadas y fundamentadas para su concreta aplicación.

- **Vulnerabilidades tecnológicas.-** son aquellas que se encuentran dentro de los sistemas que podrían dirigir directamente acciones no autorizadas. Este tipo de vulnerabilidades están presentes dentro y aplican a servicios de red, arquitectura, sistemas operativos y aplicaciones. Los tipos de vulnerabilidades de tecnología incluyen las vulnerabilidades de diseño, implementación y configuración explicadas anteriormente.

- **Vulnerabilidades físicas.-** están asociadas a la infraestructura física con la que cuenta la institución para asegurar un desempeño aceptable de todos los procesos que maneje a través de máquinas o la red.

- **Vulnerabilidades de control.-** son aquellas que se expresan como parte de un control mal desarrollado o implementado dentro de la institución. Pueden dar inicio a situaciones donde se presenten otro tipo de vulnerabilidades.
  El no disponer de un control específico bien desarrollado para las actividades o activos críticos del negocio o institución pueden limitar la capacidad de este para lograr sus objetivos o lograrlos pero obteniendo beneficios más bajos de los esperados.

- **Vulnerabilidades geográficas.-** son aquellas asociadas a la ubicación geográfica de la institución. La localización de la misma puede determinar que existan cierto tipo de vulnerabilidades en lo que respecte a acontecimientos de catástrofes naturales como terremotos, inundaciones, maremotos, entre otros.

3.3 ANÁLISIS DE VULNERABILIDADES EN LA RED DE DATOS DE LA CORTE CONSTITUCIONAL

Para el análisis previo sobre la gestión de seguridad en la red de datos de la Corte Constitucional se utilizará el sistema operativo BackTrack 5, que es una

distribución GNU/Linux[69] basada en Ubuntu y diseñada para realizar auditorías en seguridad informática.

BackTrack 5 se deriva de la unión de dos distribuciones orientadas a la auditoría y seguridad de la información, como son el sistema operativo denominado “Auditor Security Collection” y Knoppix respectivamente, por esta razón es que BackTrack incluye una larga lista de herramientas de seguridad que vienen pre instaladas, entre las que destacan numerosos escáner de puertos y vulnerabilidades, archivos de exploits[70], sniffers[71], herramientas de análisis forense y herramientas para la auditoría de redes inalámbricas.

Para comenzar con el análisis de la red en la Corte Constitucional se utilizará la siguiente herramienta:

AutoScan Network 1.5

Este programa es un escáner de red que viene previamente instalado en BackTrack 5, el cual tiene la capacidad de proveer datos sobre todos los equipos que están conectados a la red de la Corte. A través de esta herramienta se recolectará información relevante que incluye, sistema operativo que usan las estaciones de trabajo, direcciones mac de los equipos, puertos abiertos y servicios que brindan a la red, además de, impresoras, routers y switches conectados, entre otras.

Para obtener los primeros datos con esta herramienta se la ha direccionado a la IP 192.168.0.121 dentro del asistente de configuración del programa, dirección que corresponde al segmento de red más crítico de la Corte Constitucional, como muestra la Figura 3.1:

---

[69] **GNU/Linux,** término utilizado para referirse a la combinación entre software libre/distribución propia de Linux. Obtenido en, http://es.wikipedia.org/wiki/GNU/Linux.

[70] **Exploit (explotar o aprovechar),** es una secuencia de comandos con el fin de causar un error o un fallo en alguna aplicación, con el objetivo de causar un comportamiento no deseado en software o hardware. Obtenido en, http://es.wikipedia.org/wiki/Exploit.

[71] **Sniffer,** es el nombre que se le da a un programa analizador de paquetes, es decir captura las tramas de una red de computadoras para ser analizadas. Obtenido en, http://es.wikipedia.org/wiki/Sniffer.

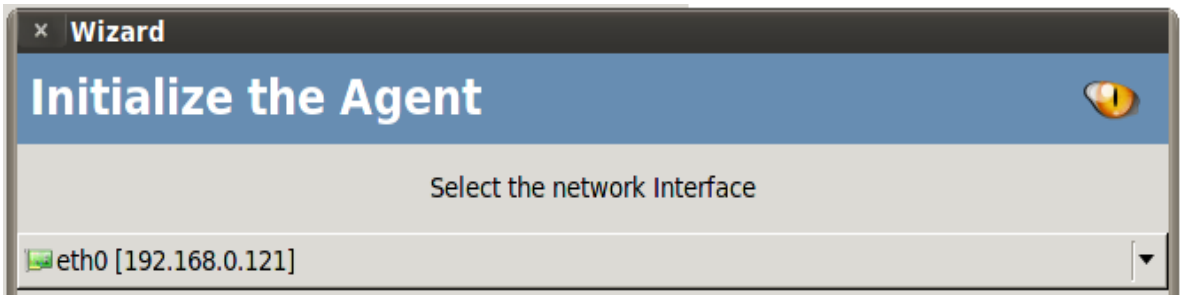


Figura 3.1: Configuración de dirección IP
Autor: Tesista
Fuente: AutoScan Network

Luego de esperar unos minutos hasta que el programa termine de escanear todos los dispositivos conectados a la red se visualizará la siguiente pantalla, como se muestra en la Figura 3.2:

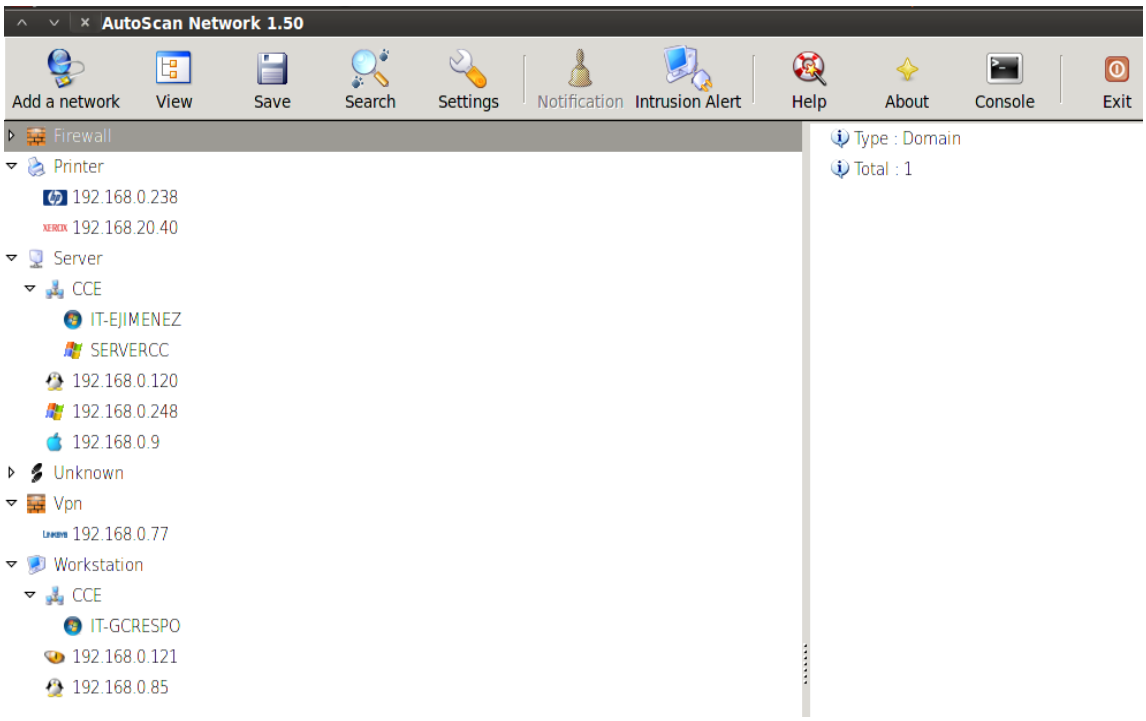


Figura 3.2: Dispositivos conectados a la red
Autor: Tesista
Fuente: AutoScan Network

Como se puede observar en la figura anterior, esta es la imagen resultante después de correr la herramienta, se presenta un resumen sobre los firewall, impresoras, servidores y algunas estaciones de trabajo propias del Departamento de Tecnología asociadas a ese segmento de red.

Después de haber obtenido toda esta información se tomarán cinco direcciones IP como un muestreo estadístico sobre la vulnerabilidad de la red, las direcciones seleccionadas se han considerado como sensibles y servirán para realizar este proceso analítico; se pueden observar en la Tabla 3.2 a continuación:

#	Dirección IP	Descripción
1	192.168.0.248	Repositorio de servidores virtualizados
2	192.168.0.150	Servidor del Active Directory
3	186.42.101.3	IP pública del servidor de desarrollo Alfresco
4	192.168.13.10	IP de un host[72] de impresiones
5	192.168.0.115	IP del servidor Web de pruebas

Tabla 3.2: Direcciones IP para el muestreo de vulnerabilidades
Autor: Tesista
Fuente: Tesista

Posterior al estudio de estas cinco direcciones, se seleccionarán tres de ellas para realizar las respectivas pruebas de aprovechamiento de las vulnerabilidades detectadas o más comúnmente conocido este proceso como, hacking ético[73] a los servidores de la Corte Constitucional, para de esta manera establecer una investigación completa sobre las debilidades encontradas y a continuación poder tomar los correctivos necesarios.

Para comenzar con el análisis de las direcciones IP escogidas, primeramente habrá que dar click sobre la IP 192.168.0.248 que se desplegó anteriormente en el informe de la herramienta AutoScan, se podrá observar información adicional como muestra la Figura 3.3:

[72] **Host,** término usado en informática para referirse a las computadoras o impresoras conectadas a una red, que proveen y utilizan servicios de ella. Obtenido en, http://es.wikipedia.org/wiki/Host.
[73] **Hacking Ético**, consiste en una penetración controlada en los sistemas informáticos de una empresa, de la misma forma que lo haría un hacker o pirata informático pero de forma ética, con previa autorización. Obtenido en, http://www.esa-security.com/web/servicios/hacking.htm.

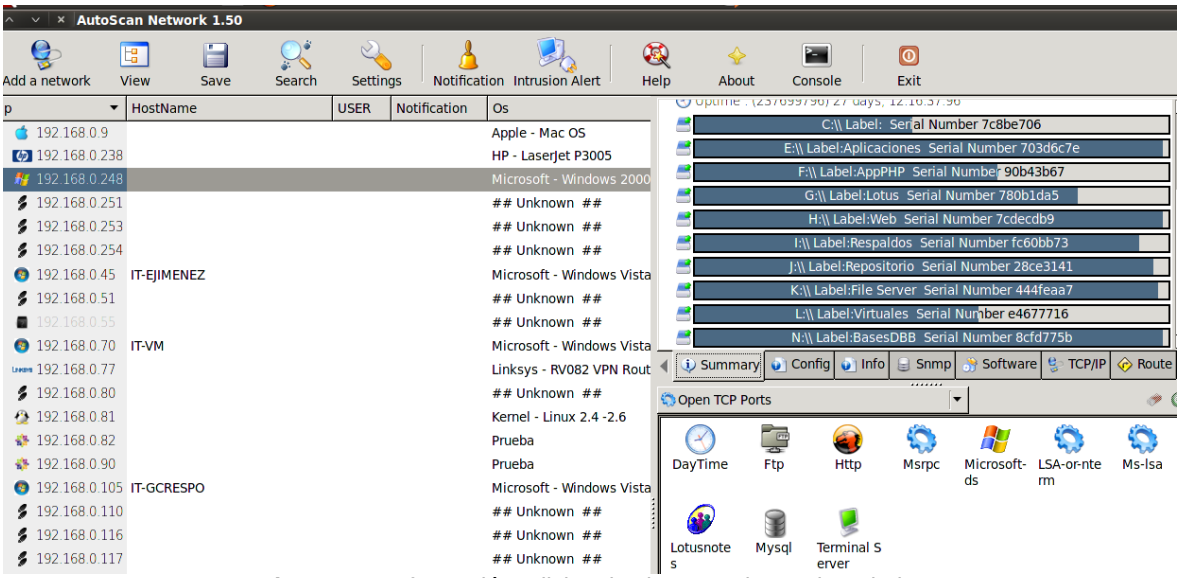


Figura 3.3: Información adicional sobre estaciones de trabajo
Autor: Tesista
Fuente: AutoScan Network

La Figura 3.3 muestra las distintas distribuciones de los servidores virtuales instalados en este repositorio, se pueden observar los siguientes: servidor de aplicaciones, servidor PHP[74], servidor Lotus, servidor web, servidor de respaldos, servidor de Base de Datos y un file server[75], además, se podrá encontrar información adicional en la parte derecha de la pantalla, que incluye la dirección mac del equipo, el sistema operativo que utiliza y su configuración de dispositivos. Este mismo proceso se realizará con la herramienta AutoScan Network para las cuatro direcciones IP restantes que se seleccionaron de los diferentes servidores.

Para el posterior análisis de vulnerabilidad sobre este repositorio de servidores virtuales se utilizará la siguiente herramienta:

Nessus

Este programa es uno de los más utilizados a nivel mundial para poder realizar escaneos o auditorías sobre vulnerabilidades de red, esta herramienta es capaz de presentar los puertos habilitados y de ejecutar 4 tipos de análisis diferentes que

[74] **PHP**, es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas. Obtenido en, www.php.net/
[75] **File Server o Servidor de Archivos,** es un tipo de servidor en una red de ordenadores cuya función es la de permitir el acceso remoto a archivos almacenados en él o directamente accesibles por este. Obtenido en, http://es.wikipedia.org/wiki/Servidor_de_archivos.

son: escaneo interno de la red, escaneo externo de la red, escaneo de preparación para auditorías y escaneo de aplicaciones Web, cualquiera de estas opciones serán escogidas según los requerimientos del Departamento de Tecnología; para continuar con el proceso se deberá seleccionar la opción “Scan” en la pantalla principal de esta herramienta como muestra la siguiente Figura 3.4:

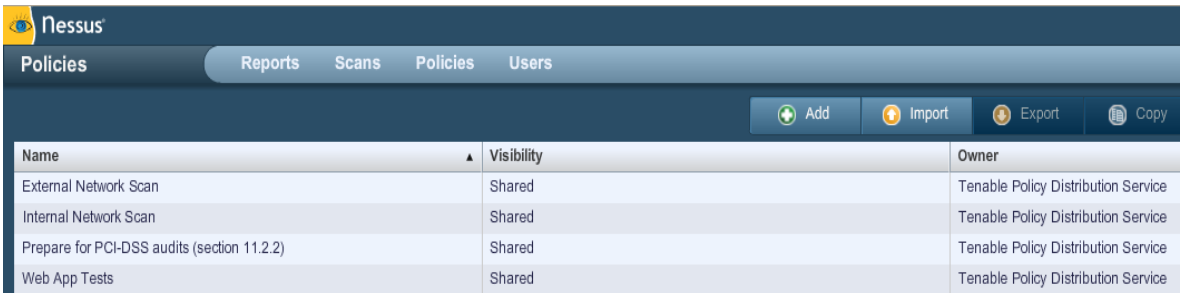


Figura 3.4: Pantalla principal herramienta Nessus
Autor: Tesista
Fuente: Analizador Nessus

Luego de haber realizado el paso anterior se desplegará una nueva pantalla en la que se deberá ingresar los datos necesarios para poder realizar el escaneo de vulnerabilidades, como se muestra en la Figura 3.5 a continuación:

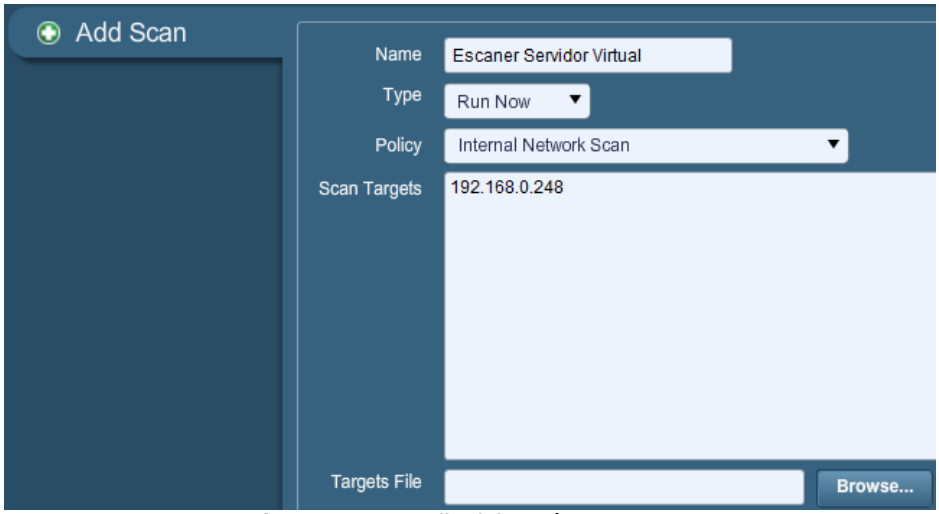
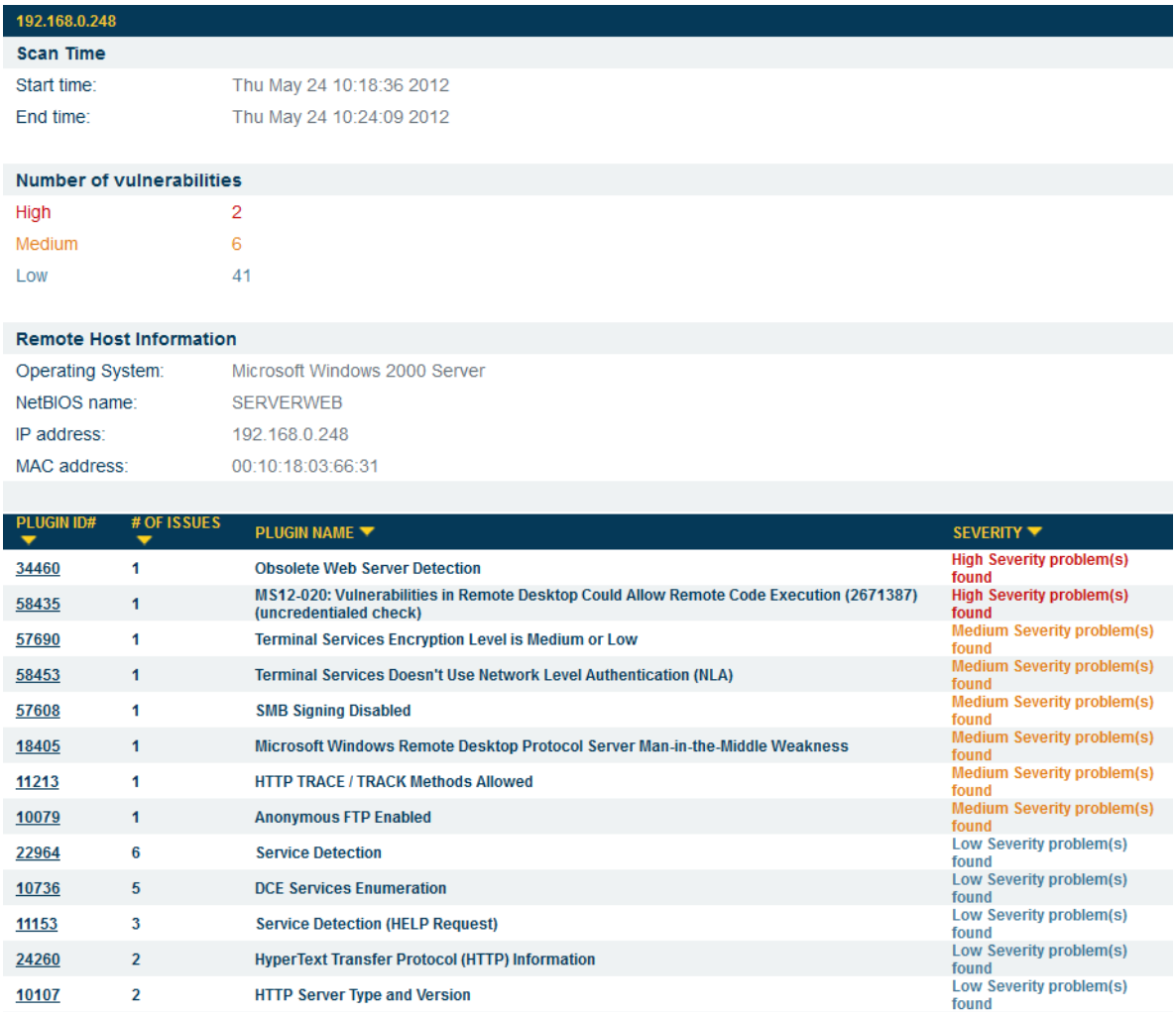


Figura 3.5: Pantalla del Escáner Nessus
Autor: Tesista
Fuente: Analizador Nessus

Como se puede observar en la imagen, habrá que darle un nombre de referencia al análisis que se va a realizar, en este caso se le ha puesto “Escáner Servidor Virtual”, además de seleccionar un tipo, que será el pre establecido por la

herramienta como “Run Now[76]”, la política del análisis que será un escaneo interno de la red y la dirección IP objetivo del estudio, que es la **192.168.0.248**. Luego de esperar varios minutos, la herramienta nos presentará un informe resultante sobre las vulnerabilidades encontradas actualmente en el servidor, como muestra la Figura 3.6 en la página a continuación:



192.168.0.248

Scan Time

Start time:	Thu May 24 10:18:36 2012
End time:	Thu May 24 10:24:09 2012

Number of vulnerabilities

High	2
Medium	6
Low	41

Remote Host Information

Operating System:	Microsoft Windows 2000 Server
NetBIOS name:	SERVERWEB
IP address:	192.168.0.248
MAC address:	00:10:18:03:66:31

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
34460	1	Obsolete Web Server Detection	High Severity problem(s) found
58435	1	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High Severity problem(s) found
57690	1	Terminal Services Encryption Level is Medium or Low	Medium Severity problem(s) found
58453	1	Terminal Services Doesn't Use Network Level Authentication (NLA)	Medium Severity problem(s) found
57608	1	SMB Signing Disabled	Medium Severity problem(s) found
18405	1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium Severity problem(s) found
11213	1	HTTP TRACE / TRACK Methods Allowed	Medium Severity problem(s) found
10079	1	Anonymous FTP Enabled	Medium Severity problem(s) found
22964	6	Service Detection	Low Severity problem(s) found
10736	5	DCE Services Enumeration	Low Severity problem(s) found
11153	3	Service Detection (HELP Request)	Low Severity problem(s) found
24260	2	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
10107	2	HTTP Server Type and Version	Low Severity problem(s) found

Figura 3.6: Resultado del análisis
Autor: Tesista
Fuente: Analizador Nessus

Como resultado de este análisis con la herramienta Nessus se podrá encontrar en su reporte información relevante como, la fecha y hora en que inició con el proceso, así como también cuando lo terminó, pero la parte más importante del

[76] **Run Now,** opción utilizada por el programa Nessus para especificar el escaneo se realizará en ese momento.

reporte hace referencia a los resultados sobre el número de vulnerabilidades encontradas, que en el caso de este servidor es de:

- 2 vulnerabilidades con severidad alta, marcadas con color rojo
- 6 vulnerabilidades con severidad media, marcadas con color naranja
- 41 vulnerabilidades con severidad baja, marcadas con color azul.

Todo el reporte generado por esta herramienta se lo puede ver de forma detallada como muestra la Figura 3.6 presentada anteriormente, que incluye el "Plugin[77] ID" que hace referencia al identificador del plugin utilizado por Nessus para detectar la vulnerabilidad, así como también, el "# Of Issues" que se refiere al número de incidencias detectadas, el "Plugin Name" o nombre de plugin con el que se identificó a la incidencia detectada y por supuesto su severidad.

Además se puede obtener el detalle de los 18 puertos abiertos que se encontraron en el respectivo análisis, incluyendo el protocolo y el nombre del servicio que lo está utilizando, como muestra la Figura 3.7:

Scans Policies Users

Virtual 192.168.0.248

Port ▲	Protocol	SVC Name
0	udp	general
0	tcp	general
0	icmp	general
7	tcp	echo
9	tcp	discard
13	tcp	daytime
17	tcp	qotd
19	tcp	chargen
21	tcp	ftp
80	tcp	www
135	tcp	epmap
211	tcp	914c/g?
445	tcp	cifs
1026	tcp	dce-rpc
1029	tcp	dce-rpc
1030	tcp	dce-rpc
1352	tcp	notes
2283	tcp	dce-rpc
3306	tcp	mysql
3389	tcp	msrdp
8090	tcp	www

Figura 3.7: Puertos habilitados del servidor
Autor: Tesista
Fuente: Analizador Nessus

[77] **Plugin o Plug-in,** es un módulo de hardware o software que añade una característica o un servicio específico a un sistema más grande. Obtenido en, en.wikipedia.org/wiki/Plug-in_(computing).

Siguiendo con el mismo proceso antes detallado con la dirección 192.168.0.248 del repositorio de servidores virtuales, a continuación se presentarán los informes que generó Nessus al analizar las 4 direcciones IP restantes.

La dirección **192.168.0.150** que hace referencia al Active Directory de la Corte Constitucional generó el siguiente informe de vulnerabilidades encontradas, como muestra la Figura 3.8:

192.168.0.150

Scan Time

Start time:	Thu May 24 10:08:44 2012
End time:	Thu May 24 10:10:27 2012

Number of vulnerabilities

High	5
Medium	7
Low	69

Remote Host Information

Operating System:	Microsoft Windows 2000 Service Pack 4
NetBIOS name:	SERVERCC
IP address:	192.168.0.150
MAC address:	00:06:29:55:85:53

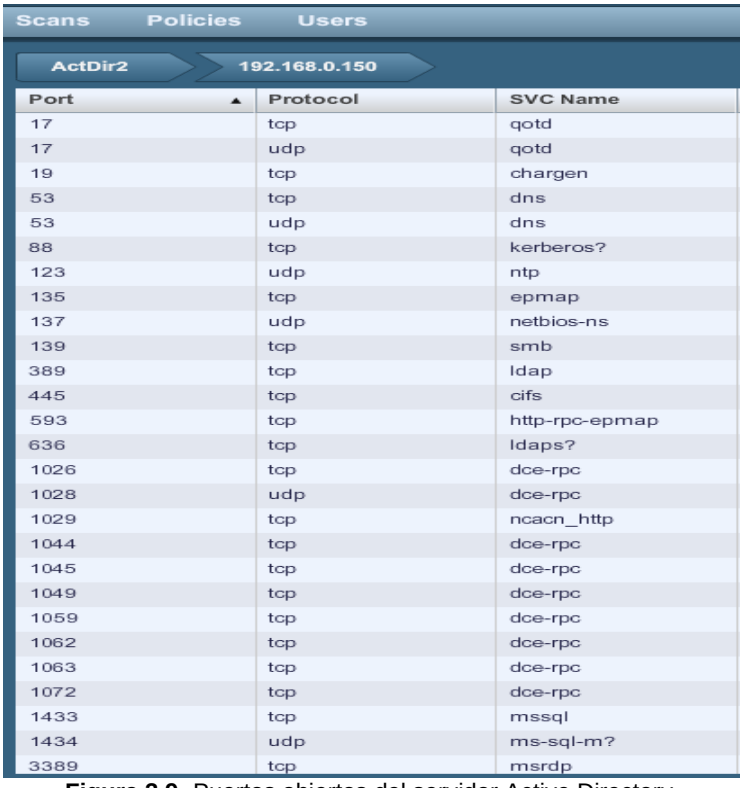
PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
58435	1	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High Severity problem(s) found
11214	1	MS02-061: Microsoft SQL Server Multiple Vulnerabilities (uncredentialed check)	High Severity problem(s) found
10907	1	Microsoft Windows Guest Account Belongs to a Group	High Severity problem(s) found
47709	1	Microsoft Windows 2000 Unsupported Installation Detection	High Severity problem(s) found
10862	1	Microsoft SQL Server Default Credentials	High Severity problem(s) found
57690	1	Terminal Services Encryption Level is Medium or Low	Medium Severity problem(s) found
58453	1	Terminal Services Doesn't Use Network Level Authentication (NLA)	Medium Severity problem(s) found
56211	1	SMB Use Host SID to Enumerate Local Users Without Credentials	Medium Severity problem(s) found
26920	1	Microsoft Windows SMB NULL Session Authentication	Medium Severity problem(s) found
56210	1	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials	Medium Severity problem(s) found
10595	1	DNS Server Zone Transfer Information Disclosure (AXFR)	Medium Severity problem(s) found
10043	1	Chargen UDP Service Remote DoS	Medium Severity problem(s) found
10736	11	DCE Services Enumeration	Low Severity problem(s) found
22964	5	Service Detection	Low Severity problem(s) found
11153	2	Service Detection (HELP Request)	Low Severity problem(s) found
10198	2	Quote of the Day (QOTD) Service Detection	Low Severity problem(s) found
11011	2	Microsoft Windows SMB Service Detection	Low Severity problem(s) found
10061	2	Echo Service Detection	Low Severity problem(s) found
11002	2	DNS Server Detection	Low Severity problem(s) found

Figura 3.8: Análisis del servidor Active Directory
Autor: Tesista
Fuente: Analizador Nessus

Como resultado del estudio a este servidor se puede verificar en su reporte información sobre el número de vulnerabilidades encontradas, que en el caso de éste es de:

- 5 vulnerabilidades con severidad alta, marcadas con color rojo
- 7 vulnerabilidades con severidad media, marcadas con color naranja
- 69 vulnerabilidades con severidad baja, marcadas con color azul.

A su vez, en la Figura 3.8 también se puede observar información detallada sobre el tipo de incidencia detectada; además, se tiene la posibilidad de revisar el informe sobre los 25 puertos establecidos como abiertos dentro de la configuración de este servidor en la Figura 3.9 a continuación, con su respectiva información del protocolo y servicio al que hace referencia, para de esta manera, investigar sobre las posibles soluciones y actuar de forma proactiva antes de que un usuario intente explotar alguna de estas vulnerabilidades.



Port	Protocol	SVC Name
17	tcp	qotd
17	udp	qotd
19	tcp	chargen
53	tcp	dns
53	udp	dns
88	tcp	kerberos?
123	udp	ntp
135	tcp	epmap
137	udp	netbios-ns
139	tcp	smb
389	tcp	ldap
445	tcp	cifs
593	tcp	http-rpc-epmap
636	tcp	ldaps?
1026	tcp	dce-rpc
1028	udp	dce-rpc
1029	tcp	ncacn_http
1044	tcp	dce-rpc
1045	tcp	dce-rpc
1049	tcp	dce-rpc
1059	tcp	dce-rpc
1062	tcp	dce-rpc
1063	tcp	dce-rpc
1072	tcp	dce-rpc
1433	tcp	mssql
1434	udp	ms-sql-m?
3389	tcp	msrdp

Figura 3.9: Puertos abiertos del servidor Active Directory
Autor: Tesista
Fuente: Analizador Nessus

Para los dos servidores antes analizados, el presente estudio quedará hasta allí, ya que por la sensibilidad de los servicios que brindan sería contraproducente realizar un ataque, por esta razón es que se deberán tomar los correctivos necesarios para mejorar directamente las vulnerabilidades detectadas de los servidores antes analizados.

A partir de las siguientes direcciones IP que corresponden al "Servidor Alfresco", "IP de un Host de Impresiones" y "Servidor Web", sí se realizarán pruebas de acceso diferentes para cada uno de ellos, con la autorización y supervisión del Administrador de la Red de la Corte Constitucional.

3.3.1 Análisis de Vulnerabilidades y pruebas de ataque

A partir de este momento se utilizarán las tres direcciones IP para realizar las respectivas pruebas de ataque, como se muestra a continuación:

3.3.1.1 Dirección IP Pública Servidor Alfresco

Se empezará con este proceso seleccionando la dirección IP pública 186.42.101.3 escogida y que pertenece a un servidor de desarrollo con sistema Alfresco[78], al proceder con el respectivo análisis con la herramienta Nessus se detectó las siguientes anomalías de seguridad como lo muestra la Figura 3.10 a continuación:

Scan Time	
Start time:	Wed May 23 12:55:25 2012
End time:	Wed May 23 13:02:11 2012
Number of vulnerabilities	
High	2
Medium	4
Low	26
Remote Host Information	
Operating System:	Microsoft Windows 2000
IP address:	186.42.101.3

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
10166	1	Windows NT FTP 'guest' Account Present	High Severity problem(s) found
58435	1	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High Severity problem(s) found
57690	1	Terminal Services Encryption Level is Medium or Low	Medium Severity problem(s) found
58453	1	Terminal Services Doesn't Use Network Level Authentication (NLA)	Medium Severity problem(s) found

Figura 3.10: Análisis del servidor de desarrollo Alfresco
Autor: Tesista
Fuente: Analizador Nessus

[78] **Alfresco,** es un sistema de administración de contenidos libre, basado en estándares abiertos y de escala empresarial para sistemas operativos tipo Unix y Otros. Obtenido en, http://es.wikipedia.org/wiki/Alfresco.

Cabe mencionar que este proceso de análisis y ataque se lo realizó en un servidor que fue creado como réplica del original, para no causar daño a los servicios que brinda, por esta razón a continuación se encuentra la información sobre el número de vulnerabilidades detectadas, que en este caso fueron de:

- 2 vulnerabilidades con severidad alta, marcadas con color rojo
- 4 vulnerabilidades con severidad media, marcadas con color naranja
- 26 vulnerabilidades con severidad baja, marcadas con color azul.

Para comenzar con las pruebas de ataque, en este caso se tomará especial referencia a una de las dos vulnerabilidades detectadas con severidad alta del análisis anterior, que hace referencia al nombre: “MS12-020” como se aprecia en la Figura 3.11 a continuación:

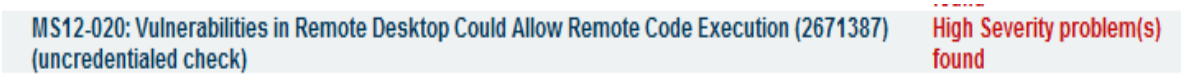


Figura 3.11: Vulnerabilidad MS12-020
Autor: Tesista
Fuente: Analizador Nessus

Esta incidencia detectada con el nombre “MS12-020” se la considera como crítica dentro de los sistemas Windows, ya que representa una “vulnerabilidad en los escritorios remotos que podría permitir ejecución remota de código”, este tipo de vulnerabilidad podría permitir la ejecución remota de código, puesto que, si un atacante envía una secuencia de paquetes RDP[79] a un sistema afectado este podría generar un error del sistema muy grave.

Para explotar este error crítico de Windows se utilizará la herramienta “Metasploit” de BackTrack 5, luego de haber abierto esta aplicación dentro del sistema aparecerá una “Terminal” donde se procederá a escribir la siguiente línea de comando:

use auxiliary/dos/Windows/rdp/ms12_020_maxchannelids

[79] **RDP (Remote Desktop Protocol),** es un protocolo propietario y desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal y un servidor Windows. Obtenido en, http://es.wikipedia.org/wiki/Remote_Desktop_Protocol.

Como se observa en la Figura 3.12 a continuación y presionar “Enter”:

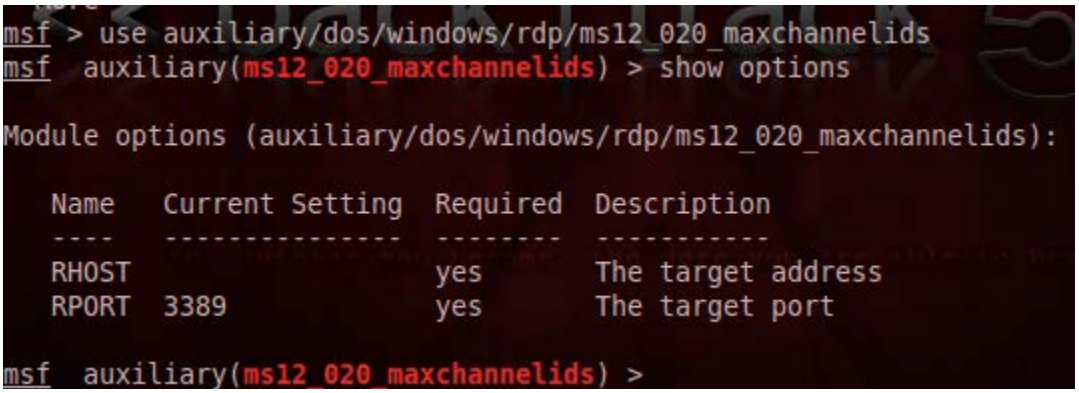


Figura 3.12: Explotar vulnerabilidad MS12-020 con Metasploit
Autor: Tesista
Fuente: Metasploit

El comando “use” de la Figura 3.12 ayuda a utilizar las librerías almacenadas en la herramienta, mientras que el comando “show options”, muestra las diferentes opciones que se pueden utilizar para realizar el ataque, siendo éstas, por conexión a la dirección IP “The target address” y mediante el puerto habilitado (3389) “The target port”; en este caso se realizará el ataque utilizando la conexión mediante dirección IP, introduciendo la siguiente línea de comando:

set RHOST 186.42.101.3

Como se muestra en la siguiente Figura 3.13:

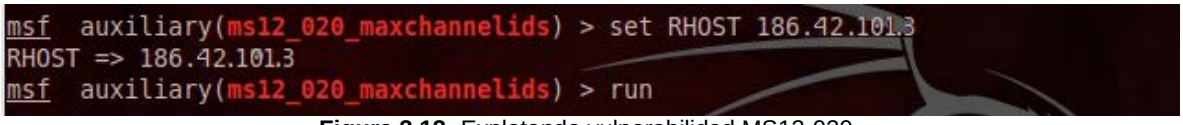


Figura 3.13: Explotando vulnerabilidad MS12-020
Autor: Tesista
Fuente: Metasploit

Luego de haber incluido esta línea de código se observará el resultado en el servidor atacado con una pantalla similar a la que se muestra a continuación en la Figura 3.14:

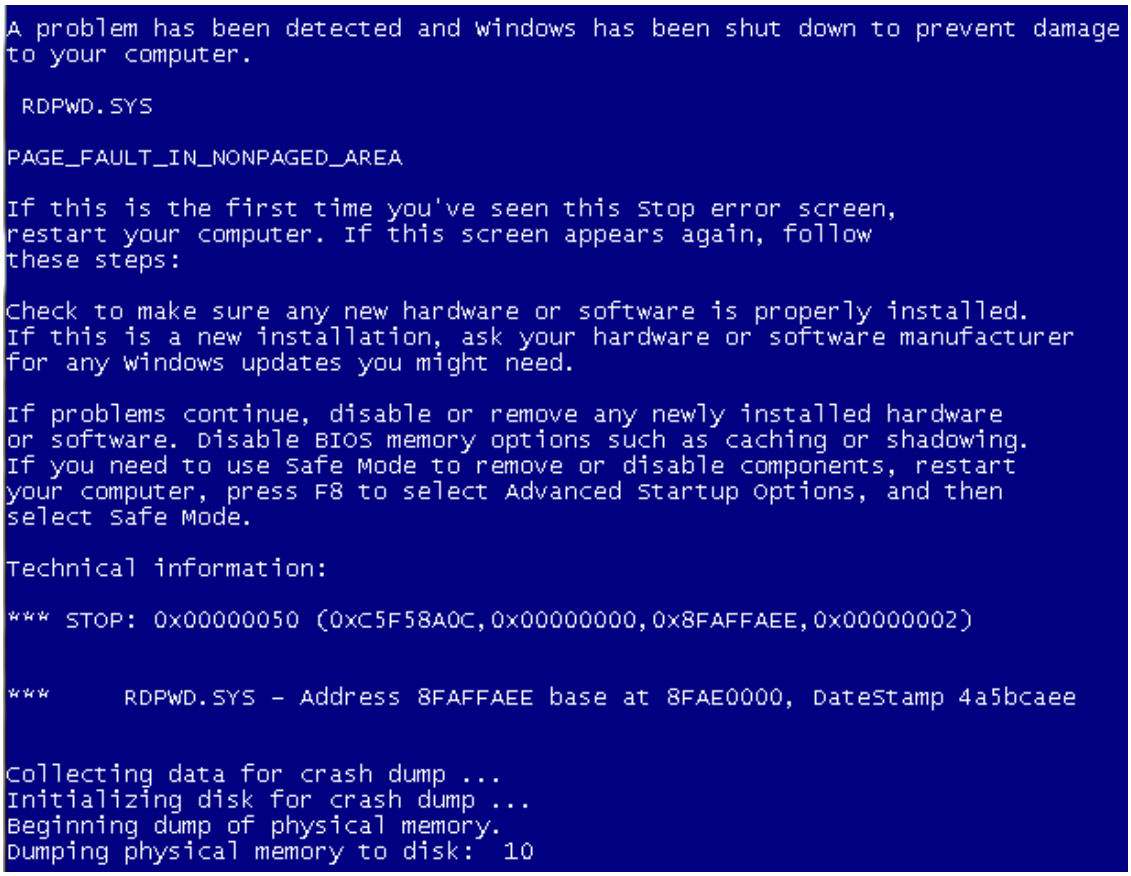


Figura 3.14: Resultado de explotar la vulnerabilidad MS12-020
Autor: Tesista
Fuente: Servidor Alfresco Afectado

En la figura anterior se puede observar un grave error de DoS al servidor con la realización de un volcado de memoria, la descripción del error se encuentra en la parte superior izquierda de la imagen con el nombre de “RDPWD.SYS”, este es un driver[80] propietario del sistema Windows y es el que resulta atacado, produciendo esta falla operativa y dejando sin servicio al servidor.

Luego de haber logrando explotar y comprobar esta vulnerabilidad del sistema Windows, la solución será descargar e instalar lo más pronto posible el parche que ya se encuentra disponible en la página oficial de Microsoft para poder corregir esta incidencia.

[80] **Driver o controlador de dispositivo,** es un programa informático que permite al sistema operativo interactuar con un periférico, haciendo posible el uso de las distintas interfaces. Obtenido en, http://es.wikipedia.org/wiki/Controlador_de_dispositivo.

3.3.1.2 Dirección IP Host Impresora

Continuando con el proceso de investigación de vulnerabilidades es el turno de la dirección 192.168.13.10 que pertenece a una impresora conectada a la red; cuando se realizó el análisis con la herramienta Nessus nos generó el siguiente resultado como muestra la Figura 3.15:

192.168.13.10

Scan Time	
Start time:	
End time:	Thu May 24 09:35:06 2012

Number of vulnerabilities	
High	0
Medium	0
Low	2

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
19506	1	Nessus Scan Information	Low Severity problem(s) found
11933	1	Do not scan printers	Low Severity problem(s) found

Figura 3.15: Análisis del host de impresión
Autor: Tesista
Fuente: Herramienta Nessus

Tal como se puede observar en la imagen anterior, el análisis podría dejar un resultado satisfactorio para el usuario ya que el reporte solo despliego:

- 2 vulnerabilidades con severidad baja, marcadas con color azul.

Y además, no se detectó ningún puerto habilitado en el host remoto de impresión, por estas razones tal vez pasaría como desapercibido del análisis, pero en este caso no es así, ya que se quiso realizar un estudio más profundo con una herramienta especializada para detectar puertos habilitados de cualquier dispositivo conectado a la red, el nombre de esta herramienta es ZenMap, otra aplicación propia de Back Track 5 que permite escanear los puertos accesibles de una determinada dirección IP.

El proceso de utilización de esta herramienta es el siguiente, al abrir la herramienta encontraremos una pantalla donde se deberá ingresar la información del análisis que se desea hacer como muestra la Figura 3.16:

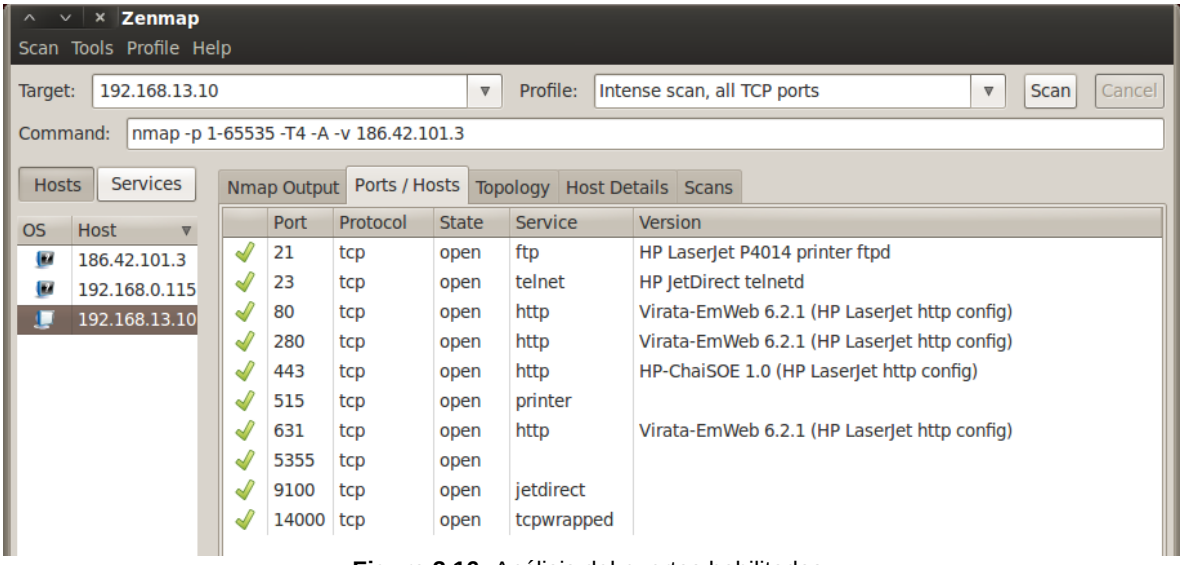


Figura 3.16: Análisis del puertos habilitados
Autor: Tesista
Fuente: Herramienta ZenMap

Como se detalla en la imagen, en el recuadro llamado “Target” se especifica la dirección IP a la que se desea realizar el análisis, que en este caso será la 192.168.13.10 y en el recuadro “Profile”, el tipo de escaneo que se desea realizar, que será, un escaneo intensivo de todos los puertos TCP[81]; después de realizada esta tarea se pueden observar los 10 puertos que se encuentran habilitados, al contrario de lo que mencionaba la herramienta Nessus que no encontró ninguno.

Para realizar los ataques se procederá a utilizar el puerto 23 Telnet[82] y el puerto 80 Http[83], los mismos que permitirán generar las siguientes acciones:

Primeramente se intentará acceder vía conexión Telnet a través del puerto 23 con la impresora, para lo cual se utilizará una pantalla de la terminal de Back Track 5 y se procederá a poner la siguiente línea de código:

telnet 192.168.13.10 9100

[81] **TCP (Transmission Control Protocol),** sirve para crear conexiones entre computadores garantizando que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. Obtenido en, http://es.wikipedia.org/wiki/Transmission_Control_Protocol.
[82] **Telnet (TELecommunication NETwork)**, es el nombre de un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. Obtenido en, http://es.wikipedia.org/wiki/Telnet.
[83] **HTTP (Hypertext Transfer Protocol)**, o en español protocolo de transferencia de hipertexto, es el protocolo usado en cada transacción que se realiza al inernet a través de un explorador Web. Obtenido en, http://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol.

La palabra Telnet hace referencia al servicio que se va a utilizar, luego la dirección IP a la que se quiere realizar la conexión y por último el puerto de conexión de la impresora “HP Laser Jet” que en este caso es el 9100, a continuación de realizado este proceso se podrá observar la siguiente Figura 3.17 de acceso a los privilegios de configuración de la impresora:

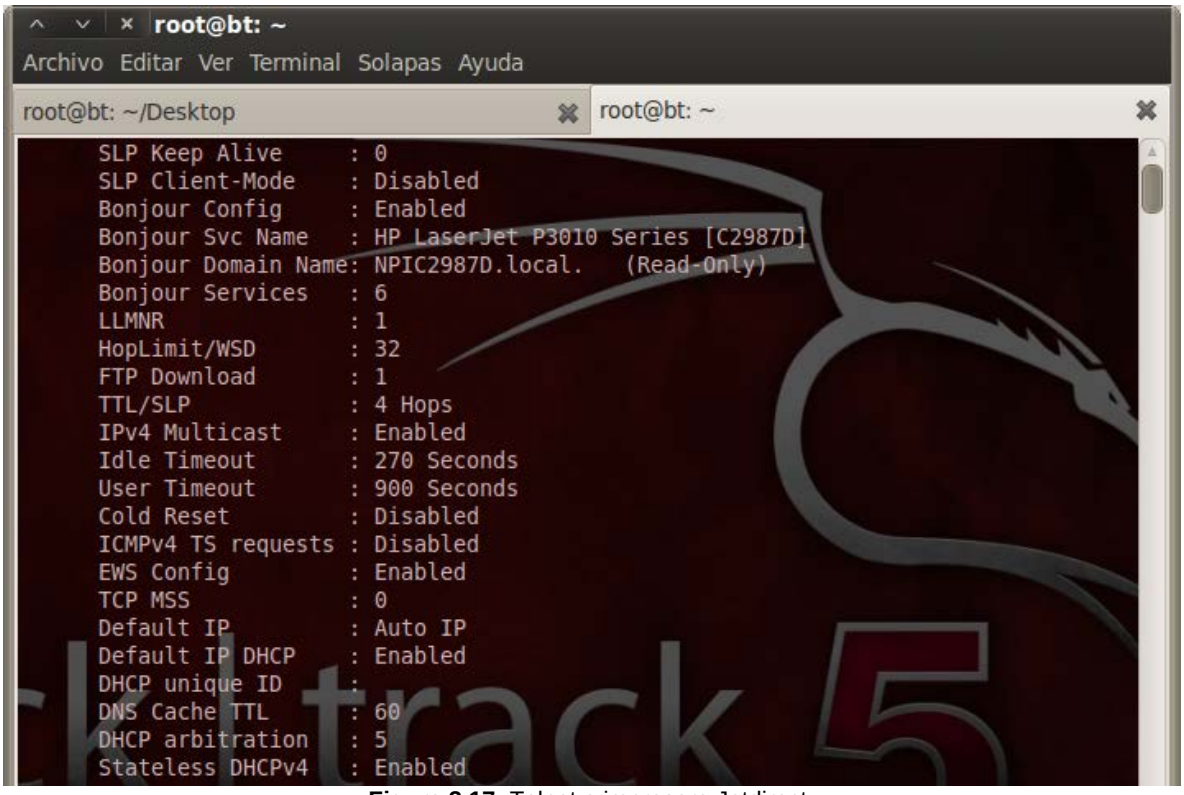


Figura 3.17: Telnet a impresora Jetdirect
Autor: Tesista
Fuente: Terminal Back Track 5

Como se pudo apreciar en la figura anterior, por medio de esta conexión se puede obtener información sin ningún tipo de restricción, por ejemplo, el modelo “HP Laser Jet P3010 Series”, el nombre del dominio, los servicios y datos adicionales, pero por si eso fuera poco, también hay la opción de utilizar el comando “help” el cual nos mostrará como cambiar la configuración de la impresora como especifica la Figura 3.18 en la página a continuación:

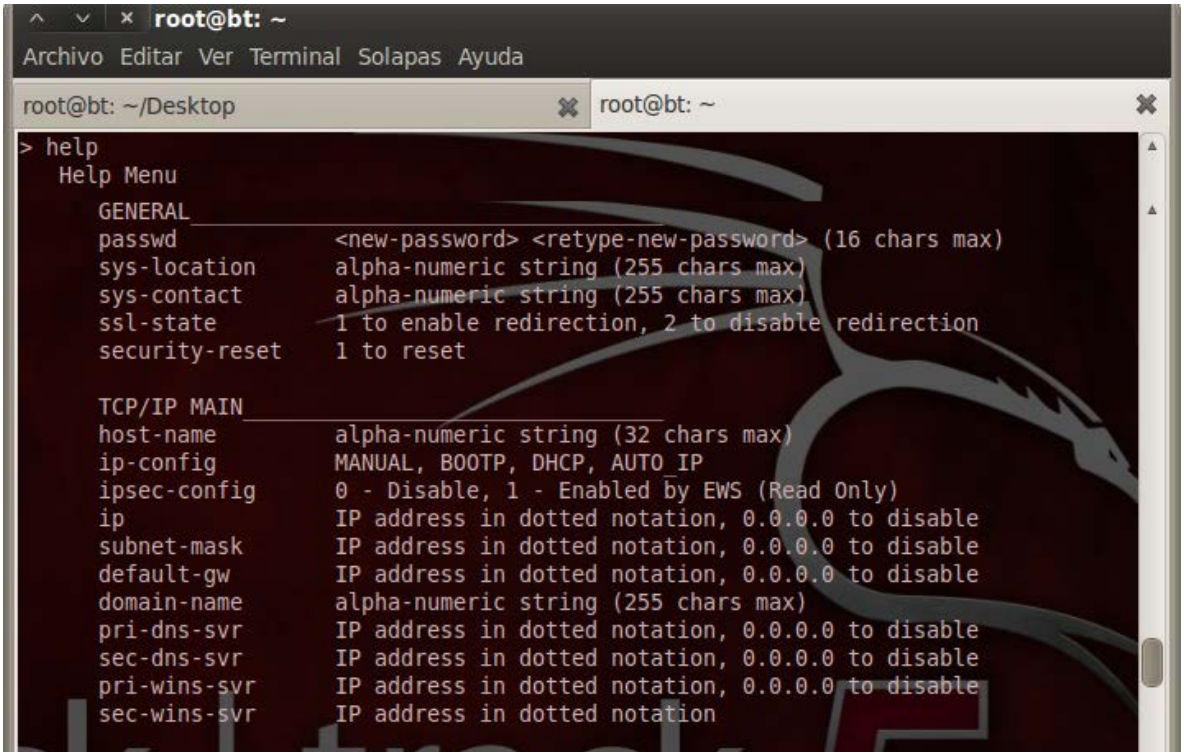


Figura 3.18: Configuración de impresora Jetdirect
Autor: Tesista
Fuente: Terminal Back Track 5

Al observar la figura anterior sobre la pantalla desplegada con el comando "help" podemos asimilar el poder que se tiene sobre dicha impresora, ya que se podría ponerle una clave utilizando la línea de comando **"passwd <nueva clave> <repetir nueva clave>"** con la única restricción que la clave debe tener un máximo de 16 caracteres, quedando de esta forma inaccesible para el departamento técnico si se llegara a presentar algún problema, o también se podría cambiar su dirección IP con el comando **"ip-config MANUAL < nueva dirección IP>"** y dejar a todo el departamento sin conexión por tiempo ilimitado reduciendo su productividad.

Estos son algunos de los posibles ataques que se podrían realizar mediante una conexión Telnet, sin embargo, existe la posibilidad de atacar de una forma distinta a través de un navegador Web como Internet Explorer o Mozilla, como se observó anteriormente en la Figura 3.15 en el escaneo de puertos con ZenMap también se encontraba habilitado el puerto 80, que deja abierta la posibilidad de intentar una intrusión vía Web.

Para comprobar este tipo de procedimiento se deberá abrir un navegador y probar introduciendo en la parte superior la dirección IP 192.168.13.10 y observar si se logra una conexión satisfactoria:

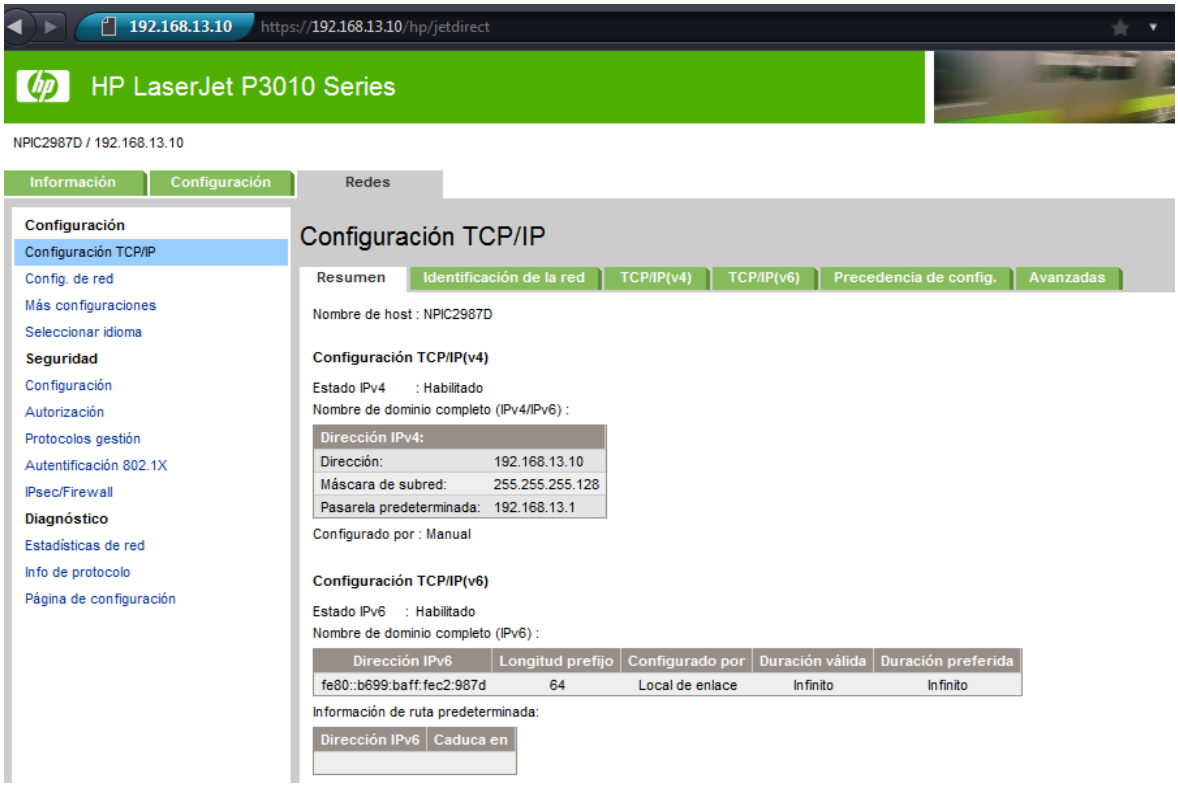


Figura 3.19: Conexión via Web con impresora Jetdirect
Autor: Tesista
Fuente: Mozilla Fire Fox

Al parecer se logró el resultado esperado, como se muestra en la Figura 3.19 la conexión fue exitosa y no fue necesario el ingreso de ninguna clave para acceder a la configuración de la impresora, para este caso solo basta dar click en el cuadro de texto y modificar toda la información que se desee, ocasionando así un incidente de seguridad y un retraso en la impresión de documentación.

En base a este estudio se ha logrado comprobar que las impresoras también pueden ser víctimas de ataques y representar una brecha en la seguridad de la red, considerando esto, será necesario incluir contraseñas para prevenir la manipulación de personal no autorizado.

3.3.1.3 Servidor Web de pruebas

Para concluir con las pruebas de vulnerabilidad se intentará acceder al Servidor Web de la Corte Constitucional, este proceso se lo realizará generando una copia del Servidor Web que se encuentra virtualizado, de esta manera no se generará ningún riesgo a la página oficial de la institución que se encuentra en producción.

Gracias a la virtualización es posible respaldar el servidor y utilizarlo para estas pruebas, la copia se la generó con las siguientes características:

- **Programa de virtualización:** Virtual Box
- **Sistema Operativo:** Centos 5.8
- **Servicio:** Servidor Web Tester
- **Almacenamiento:** 10Gb
- **Memoria:** 512Mb

Para realizar este estudio, al servidor de pruebas se lo ha configurado de la misma forma que al original, con el fin de que la simulación pueda atentar en contra de su seguridad, ya que el servidor web principal se encuentra en producción. Se comenzará el proceso de intento de acceso revisando las vulnerabilidades con el programa Nessus, en donde su reporte se puede apreciar en la Figura 3.20:

Scan Time	
Start time:	Fri May 18 11:22:20 2012
End time:	Fri May 18 11:27:38 2012
Number of vulnerabilities	
High	0
Medium	4
Low	37
Remote Host Information	
Operating System:	Linux Kernel 2.6 on CentOS release 5
IP address:	192.168.0.115
MAC address:	08:00:27:29:fb:8b

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
51192	2	SSL Certificate Cannot Be Trusted	Medium Severity problem(s) found
12218	1	mDNS Detection	Medium Severity problem(s) found
11213	1	HTTP TRACE / TRACK Methods Allowed	Medium Severity problem(s) found
22964	6	Service Detection	Low Severity problem(s) found
11111	4	RPC Services Enumeration	Low Severity problem(s) found

Figura 3.20: Escaneo de vulnerabilidades Servidor Web
Autor: Tesista
Fuente: Herramienta Nessus

El resultado del análisis como muestra la imagen anterior ha dejado la siguiente información para poder ser estudiada:

- 0 vulnerabilidades con severidad alta, marcadas con color rojo
- 4 vulnerabilidades con severidad media, marcadas con color naranja
- 37 vulnerabilidades con severidad baja, marcadas con color azul.

Del reporte obtenido habrá que estudiar las 4 vulnerabilidades detectadas con severidad media para generar una posible intrusión, ya que en este caso no se ha observado incidencias con severidad alta debido a la seguridad que le ha dado el Administrador de Red a este servidor.

A su vez, también se realizará el escaneo de los puertos habilitados con la herramienta ZenMap, para de esta manera poder determinar de forma segura cuales podrían ser las vías adicionales de acceso para lograr la intrusión al Servidor Web; para cumplir con este proceso se deberá configurar la herramienta con la dirección IP 192.168.0.115, obteniendo la Figura 3.21 como resultado del escaneo:

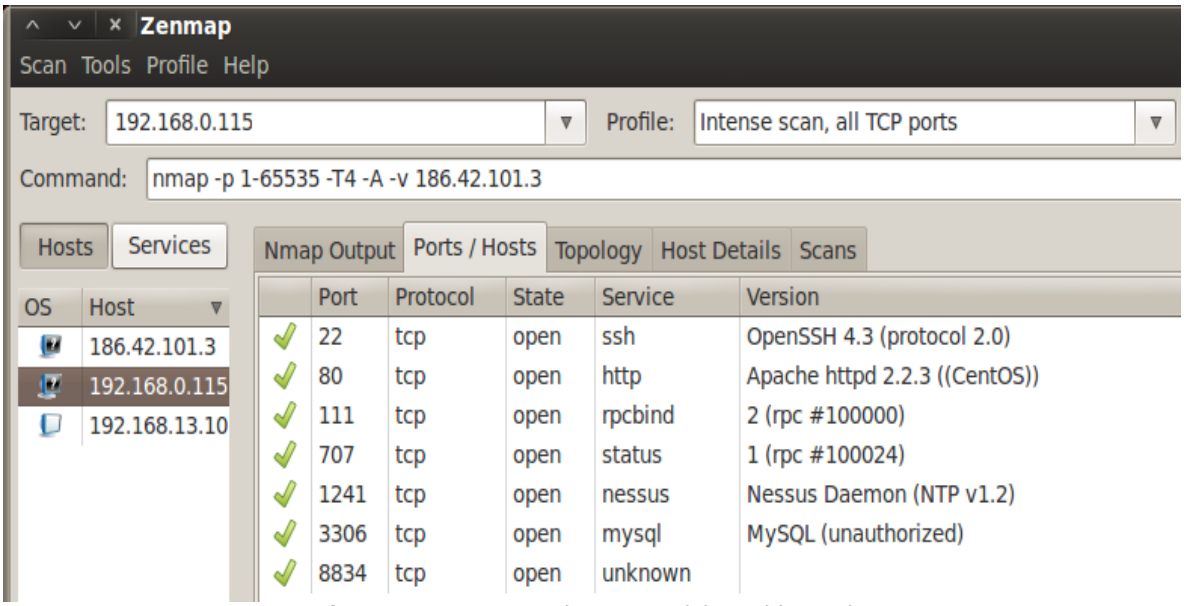


Figura 3.21: Escaneo de puertos del Servidor Web
Autor: Tesista
Fuente: Herramienta Nessus

Luego de obtener toda la información posible sobre las vulnerabilidades detectadas y puertos habilitados, se comenzará con el intento de intrusión al Servidor Web, como se pudo observar en la Figura 3.20 se encuentra abierto el puerto 3306 que hace referencia al servicio de MySQL[84], que es la herramienta que almacena información de los usuarios con sus respectivos privilegios dentro de una base de datos, además, la página de la Corte Constitucional se encuentra administrada por el programa Joomla[85], que es la aplicación que se utiliza para integrar, añadir o editar el contenido del sitio web de la institución.

Al ser estos dos programas las herramientas para manipular la administración de la página oficial, se intentará utilizar el programa Metasploit de Back Track 5 para intentar explotar alguna vulnerabilidad a través del puerto 3306, como alternativa para realizar este proceso se intentará generar un ataque de fuerza bruta de tipo diccionario, con la intención de coincidir con alguna clave registrada en el sistema para lograr la intrusión.

Un ataque de diccionario es un método que se usa para acceder a un computador, servidor o aplicación protegida por claves; la generación de los diccionarios no obedece a ninguna metodología en especial, al contrario, las claves se seleccionan dependiendo del objetivo que se va a atacar, por esta razón es que para su creación simplemente se pueden utilizar las palabras del diccionario, números, letras, caracteres, palabras por defecto de las aplicaciones y hasta scripsts[86], que se analizarán de forma sistemática para lograr su objetivo.

En referencia a lo anterior y para comenzar con este proceso, se crearán dos archivos de texto plano con los nombres de usuarios y contraseñas más comunes para la protección de servidores, aplicaciones o sistemas operativos, las palabras que se seleccionaron se detallan en la Tabla 3.3 a continuación:

---

[84] **MySQL,** es un sistema de gestión de bases de datos que pueden ser de tipo relacional, multihilo y multiusuario. Obtenido en, http://es.wikipedia.org/wiki/MySQL.

[85] **Joomla,** es un sistema de gestión de contenidos y entre sus principales virtudes está la de permitir integrar, añadir o editar el contenido de un sitio web de manera sencilla. Obtenido en, http://es.wikipedia.org/wiki/Joomla!.

[86] **Script o archivo de órdenes,** es un programa que por lo regular se almacena en un archivo de texto plano y se lo utiliza para realizar un proceso dentro de una aplicación. Obtenido en, http://es.wikipedia.org/wiki/Script

#	Nombres de Usuario	Contraseñas
1	root	root
2	toor	toor
3	administrador	administrador
4	user	user
5	usuario	usuario
6	admin	admin
7	administrator	administrator
8	mestrella	mestrella
9	corteweb	corteweb
10	servidorweb	servidorweb

Tabla 3.3: Nombres de usuarios y claves para ataque diccionario
Autor: Tesista
Fuente: Tesista

Luego de haber creado los dos archivos con los usuarios y claves respectivamente, se utilizará la consola de Metasploit para explotar el diccionario dentro del ataque al servidor web, como muestra la Figura 3.22:

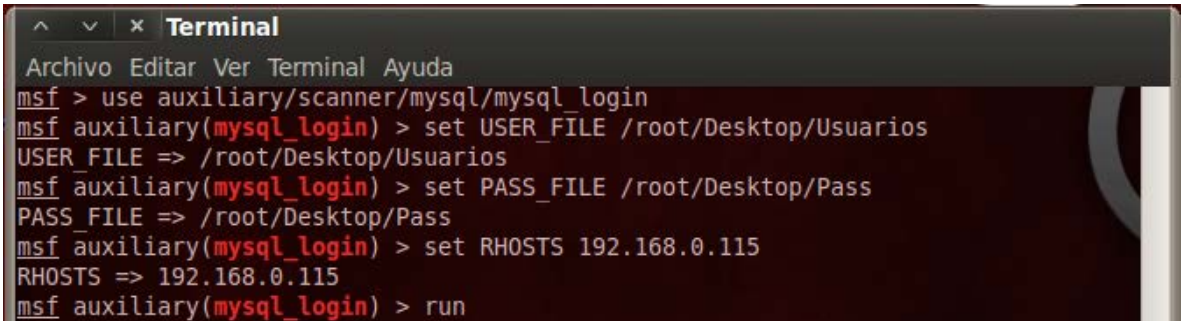


Figura 3.22: Generando el ataque de diccionario
Autor: Tesista
Fuente: Metasploit

Los comandos que se utilizaron para este proceso son:

- ***use auxiliary/scanner/mysql/mysql_login****,* este comando se utiliza para acceder a la librería de Metasploit que analizará secuencialmente los usuarios con las claves.
- **set USER_FILE /root/Desktop/Usuarios,** comando para seleccionar la ruta del archivo plano que contiene los nombres de usuario que se utilizarán para el ataque.

- **set PASS_FILE /root/Desktop/Pass,** comando para seleccionar la ruta del archivo plano que contiene las claves que se utilizarán para el ataque.
- **set RHOSTS 192.168.0.115,** comando para seleccionar la dirección ip del servidor objetivo del ataque y **run,** comando que ejecutará todo el proceso.

En este caso el resultado del ataque de diccionario ha sido exitoso mostrando un mensaje de “SUCCESSFUL LOGIN” como muestra la Figura 3.23 a continuación:

Figura 3.23: Clave detectada exitosamente
Autor: Tesista
Fuente: Metasploit

Lo primero que se puede deducir de esta intrusión, es que los administradores de la página web dejaron el nombre de usuario y la contraseña por defecto de Joomla para el ingreso a la administración, un error muy común pero que representa una vulnerabilidad muy sensible del servidor, principalmente considerando que para la creación del servidor secundario no se modificó dato alguno como el usuario o clave que constan como “admin”, “admin” y que fueron encontrados para la administración de la página de la Corte Constitucional.

A continuación de haber conseguido el usuario y la clave de acceso se intentará utilizarla en el administrador de Joomla, ya que esta herramienta realiza su autenticación directamente a la base de datos de MySQL, de esta forma se deberá abrir una ventana del explorador web y escribir la dirección 192.168.0115/administrador como muestra la Figura 3.24:

Figura 3.24: Utilizar clave en el administrador Joomla
Autor: Tesista
Fuente: Joomla

Dentro del formulario de acceso que nos presentará el administrador de Joomla, se deberá introducir el nombre de usuario ‘admin’ y contraseña ‘admin’ obtenidas anteriormente para autenticar el acceso al servidor.

A continuación en la Figura 3.25 se podrá observar la validación de usuario y clave con los que se logró el ingreso al gestor de contenido de Joomla:

Figura 3.25: Autenticación exitosa en el administrador
Autor: Tesista
Fuente: Joomla

Después de ingresar al gestor de administración se podrá realizar cualquier cambio para tomar el control de la página de la Corte Constitucional, para esta demostración, se comenzará cambiando la clave de ingreso a la aplicación, con el objetivo de retrasar las labores de actualización de la página por parte de los administradores, así bien, para cumplir con este objetivo habrá que ingresar en el link de Super User de la parte superior derecha como se observó en la figura anterior y luego editar el perfil principal como muestra la siguiente Figura 3.26:

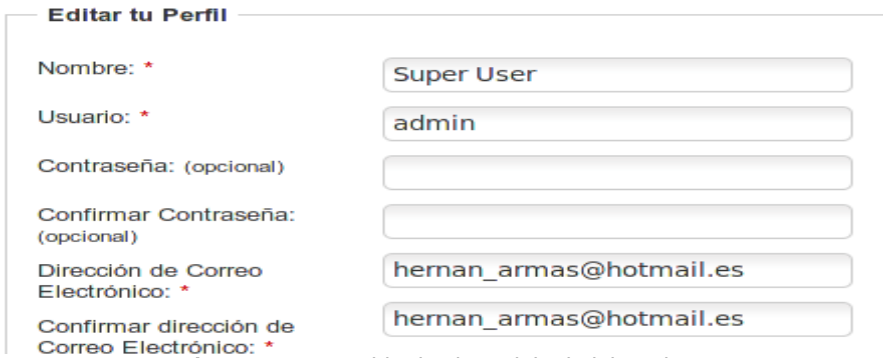


Figura 3.26: Cambio de clave del administrador
Autor: Tesista
Fuente: Joomla

Como se pudo observar existe la posibilidad de cambiar la siguiente información: nombre por defecto, usuario por defecto, contraseña y dirección de correo electrónico, por esta razón, se procederá a introducir una nueva clave de administración, una nueva dirección de correo para recibir notificaciones sobre los cambios realizados en la página y se dejará el nombre y usuario por defecto, luego de haber realizado este proceso el perfil de Super User quedará de la siguiente forma como muestra la Figura 3.27 a continuación:

Figura 3.27: Comprobación cambio de perfil
Autor: Tesista
Fuente: Joomla

Luego de haber obtenido acceso y control total de la administración del portal web a través de Joomla, se podrá ingresar al gestor de plantillas para alterar la página de la Corte Constitucional, realizando un cambio en una de las imágenes, quedando como pantalla resultante la Figura 3.28 a continuación:

Figura 3.28: Imagen antes y después del cambio de la vulneración
Autor: Tesista
Fuente: Joomla

Para poder realizar este proceso de modificación de la página web se utilizó una de las imágenes de muestra que contiene Joomla y se la publicó como si fuera parte original del portal, de esta forma terminaría la comprobación sobre la vulnerabilidad detectada en la administración del servidor web a través de Joomla; sin embargo, con el propósito de ampliar la búsqueda de debilidades en un servicio tan sensible como este, se intentará realizar un segundo tipo de ataque con una técnica diferente a la anterior, para este caso se realizará un ataque de "inyección SQL[87]" a la página web de la Corte Constitucional.

- **Intento de ataque de inyección SQL**

Este tipo de ataque se ocupa de insertar código SQL[88] intruso a las consultas que una página web realiza a su base de datos, y de esta forma poder conseguir información confidencial y lograr acceder al servidor; debido a que este tipo de ataques es muy utilizado actualmente se hará una demostración de este tipo de intrusiones con el servidor de la Corte Constitucional.

Para empezar se deberá intentar agregar parte de código SQL a la solicitud que realiza la página web de la Corte Constitucional a la base de datos, este proceso de inserción se lo realiza a continuación de la dirección IP que apunta al servidor, como muestra la siguiente línea:

*http://192.168.0.115/administrator/index.php?option=com_productshowcase&Itemid=S@BUN&action=details&id=-99999/**/union/**/select/**/0,concat(username, 0x3a,password),concat(username,0x3a,password),0,0,0,0,0,1,1,1,1,2,3,4,5/**/from/**/jos_users/**

Esta línea de código fue extraída de una publicación de vulnerabilidades encontradas en la aplicación Joomla a principios de este año, razón por la cual se la ha querido implementar a ver las consecuencias del mismo, obteniendo como

[87] **Inyección SQL,** es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos. Obtenido en, http://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL.

[88] **SQL (Structured Query Language),** es un lenguaje de manipulación y acceso a bases de datos relacionales permitiendo especificar diversos tipos de operaciones en estas. Obtenido en, http://es.wikipedia.org/wiki/SQL

resultado un error en la base de datos como muestra la Figura 3.29 a continuación:

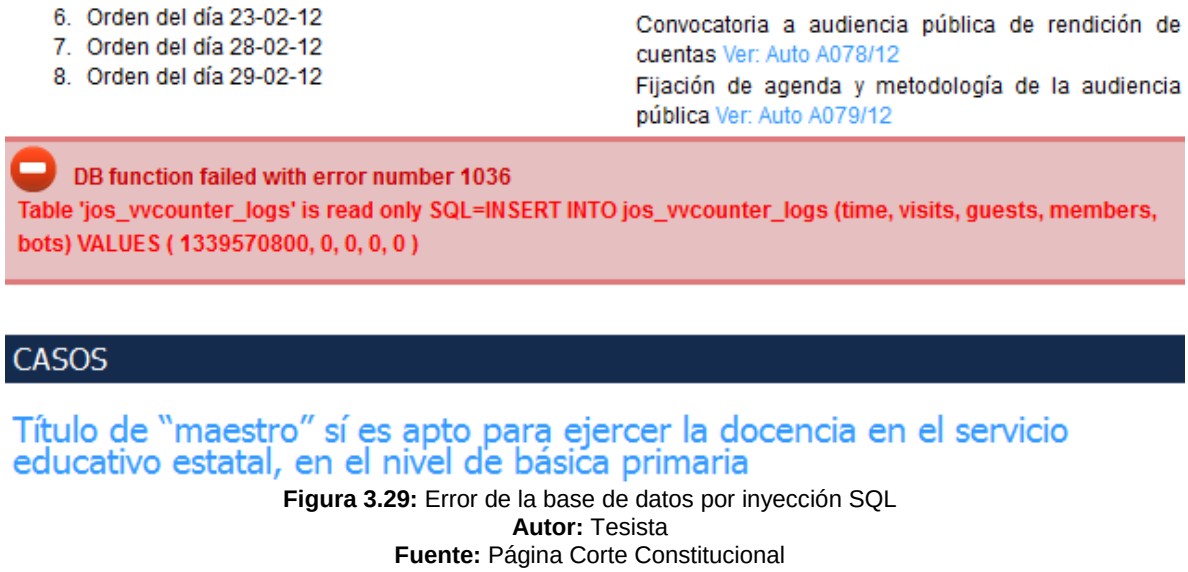


Figura 3.29: Error de la base de datos por inyección SQL
Autor: Tesista
Fuente: Página Corte Constitucional

A pesar de que esta línea de código fue creada para una versión anterior de Joomla igual generó un error a la base de datos, esta línea tiene como objetivo extraer los nombres de usuarios y las direcciones de correo electrónico autorizadas para el ingreso o recuperación de la clave del gestor de administración de la página web, como se puede observar en la figura anterior la base de datos no permite insertar información ni realizar las consultas que desea ejecutar la línea de código, debido a que la versión utilizada se encuentra actualizada. Pero no por esto quiere decir que no sea vulnerable, así que se ingresará otra línea de código SQL como la que se encuentra a continuación, para intentar cambiar la clave de administración a pesar de que no existe ningún enlace relacionado con este procedimiento:

http://192.168.0.115/index.php?option=com_user&view=reset&=confirm

La inyección SQL con la línea de código anterior dejo el siguiente resultado como muestra la Figura 3.30 a continuación:

Figura 3.30: Solicitud de correo electrónico de administración
Autor: Tesista
Fuente: Página Corte Constitucional

Como se pudo observar en la imagen anterior, se insertó un mail por defecto del administrador Joomla para que nos autentifique el registro de renovación de clave, luego de enviar los datos requeridos en el formulario nos aparecerá una nueva pantalla solicitando el ingreso de la clave que fue enviada al mail de administración, sin embargo, no será necesario abrir el mail para verificar la contraseña enviada, puesto que si se abre el código fuente de la página podremos visualizar la clave en MD5[89] enviada al correo de administración, esta codificación es de tipo hexadecimal y cuenta con 32 dígitos para cifrar la información, como muestra a continuación la Figura 3.31:

```
el for="email" class="hasTip" title="Dirección de e-mail::Introducir la dire
ut id="email" name="email" type="text" class="required validate-email" />
/>
 class="readon-wrap1"><div class="readon1-l"></div><a class="readon-main"><s
ut type="hidden" name="24e33a5437feceb08f0cfe1c95652718" value="1" /></form>
```

Figura 3.31: Verificación de clave MD5 a través del código fuente
Autor: Tesista
Fuente: Página Corte Constitucional

Como se aprecia anteriormente en la figura se encuentra el código MD5 de la siguiente forma.

name=”24e33a5437feceb08f0cfe1c95652718”

[89] **MD5 (Message-Digest Algorithm 5),** el algoritmo de resumen del mensaje 5, es una secuencia de código de reducción criptográfica de 128 bits ampliamente usado para encriptar claves de administración de distintas aplicaciones. Obtenido en, http://es.wikipedia.org/wiki/MD5.

A continuación habrá que insertar la siguiente línea de código SQL en la barra del navegador para que nos proporcione la pantalla de ingreso de la clave MD5:

http://192.168.0.115/index.php?option=com_user&view=reset&layout=confirm

Al copiar este código e ingresarlo dentro del formulario que nos solicita la clave de registro enviada al correo electrónico, de la siguiente manera como muestra la Figura 3.32:

Figura 3.32: Ingreso de clave MD5
Autor: Tesista
Fuente: Página Corte Constitucional

Por último, luego de haber autenticado el ingreso mediante la dirección de correo electrónico por defecto y la clave a través del visor de código fuente, se accede a la ventana final para restablecer la contraseña de administración del aplicativo Joomla, que contiene la página web de la Corte Constitucional como se muestra en la siguiente Figura 3.33:

Figura 3.33: Restablecimiento de contraseña
Autor: Tesista
Fuente: Página Corte Constitucional

En la figura antes detallada se puede ingresar la nueva información sobre las credenciales de verificación de Joomla, como son: la contraseña y su respectiva verificación. A continuación se ingresará al administrador del aplicativo para probar los cambios realizados como muestra la Figura 3.34:

Figura 3.34: Utilizar clave modificada en el administrador Joomla
Autor: Tesista
Fuente: Joomla

Con la utilización del usuario “admin” y la clave modificada anteriormente como “corteadmin” se obtiene el acceso exitoso a la pantalla de administración de Joomla, teniendo la posibilidad de modificar cualquier segmento de la página que se presenta a los usuarios, como por ejemplo se puede observar la Figura 3.35 a continuación:

Figura 3.35: Imagen antes y después de la intrusión
Autor: Tesista
Fuente: Joomla

De esta forma se ha comprobado que existe otro tipo de vulnerabilidad a través de pequeños fragmentos de inyección SQL que solicitan información que no se encuentra disponible en el sistema, obteniendo como resultado una intrusión exitosa al servidor web.

Con todos los antecedentes antes descritos culmina la parte de pruebas y ataques de intrusión a los distintos servicios de la Corte Constitucional; a continuación se plantearán las posibles vías de mitigación y solución que se debe tomar para corregir las incidencias detectadas.

3.3.2 Propuesta de mitigación y solución a vulnerabilidades

Para solucionar las vulnerabilidades encontradas en análisis precedentes, a continuación se propondrá las soluciones más convenientes que se puede tomar.

3.3.2.1 Dirección IP pública del servidor de desarrollo Alfresco

Este servidor con dirección IP 186.42.101.3, presentó una debilidad de sistema operativo llamada MS12-020, que se considera como una vulnerabilidad en el escritorio remoto, mediante el cual se podría permitir la ejecución de código remotamente, y actualmente esta falla de actualización está considerada como crítica. Por esta razón es que se propondrá la forma de mitigar y la solución a la vulnerabilidad detectada en el sistema.

Mitigación.- tiene que ver con la deshabilitación del protocolo de escritorio remoto (RDP), esto quiere decir, que se bloquearían todas las conexiones remotas hacia el servidor y en caso de que se necesitara realizar cualquier cambio o modificación, se debería estar presentes en él, sin embargo, habría que tomar en cuenta que al realizar este proceso se solucionaría gran parte de la debilidad detectada, pero se limitaría la capacidad de conexión remota continua para controlar el desempeño del servidor en caso de que el administrador de red no pueda acudir en ese instante a solucionar el problema.

Solución.- la vía más óptima para solucionar este inconveniente es actualizar la versión del sistema operativo de la KB2570222 por la KB2621440, para eliminar la

vulnerabilidad detectada, para realizar este proceso habrá que ingresar a la página web oficial de Microsoft[90] y descargar la actualización llamada “Windows Server 2003 Service Pack 2”, que corrige la ejecución remota de código y de esta forma poder eliminar cualquier posibilidad de ataque al servidor.

3.3.2.2 Host de Impresión

Para el análisis de las posibles vulnerabilidades se tomó la dirección IP 192.168.13.10, que corresponde a una impresora conectada dentro de la red y se realizó pruebas de conexión mediante los puertos habilitados, obteniendo como resultado enlaces exitosos para manipular la configuración y afectar el desempeño de la impresora.

La única protección con la que se cuenta actualmente, es que las impresoras están divididas de acuerdo a unidades organizacionales dentro de la entidad, esto quiere decir, que si un funcionario del Departamento Financiero desea conectarse a una impresora del departamento de Tecnología se le pedirá una clave para realizar la conexión, pero si intenta conectarse a otra impresora dentro del mismo departamento la configuración resulta exitosa, por estos motivos se propondrá dos posibles soluciones para corregir las falencias detectadas.

Mitigación.- del análisis efectuado se obtuvo como resultado, que se encuentran abiertos los puertos 23 y 80, que corresponden a los servicios de Telnet y Http respectivamente, a través de los cuales se puede realizar la conexión a cualquier impresora y cambiar su configuración sin ningún tipo de restricción, debido a esto, es que se recomienda el bloqueo de éstos puertos para disminuir los posibles intentos de conexión y manipulación de las impresoras conectadas a la red, sin embargo, habrá que tomar en cuenta que este proceso de bloqueo de puertos se tendrá que hacer en las casi 200 impresoras que posee la institución, representando un tiempo de configuración muy alto por cada una de ellas, y además, si se realiza este procedimiento no se podrá configurar las impresoras desde una misma ubicación a través de conexiones remotas, ya que será

[90] **Microsoft,** TechCenter de seguridad, Boletín de seguridad de Microsoft MS12-020 – Crítica. Obtenido en, http://technet.microsoft.com/es-ec/security/bulletin/ms12-020.

necesario acudir a cada una de ellas si se presenta un error, aumentando los tiempos de atención al usuario.

Solución.- se recomienda implementar contraseñas a todas las impresoras de red, ya que si se bloquean los puertos de administración como se mencionó anteriormente, siempre sería necesario estar presente para la manipulación de una impresora, por esta razón es que resulta más conveniente implementar una clave de administración, ya que de esta forma existe la posibilidad de poder manipular la configuración de todas las impresoras desde un mismo punto, y además, obtener la protección de una clave de seguridad para que no se puedan conectar personas no autorizadas. Hay que tener en cuenta que para la creación de claves se deben tomar en cuenta los siguientes parámetros:

Persona responsable.- se refiere a la designación de un integrante del Departamento de Tecnología, como encargado de administrar las claves que se van a asignar a todas las impresoras de la entidad.

Tipo de clave de implementación.- la seguridad que se deberá implementar según el Libro Naranja será de tipo “C2-Protección de acceso controlado”[91] en el cual menciona que la clave tendrá que ser definida por la persona responsable, teniendo en cuenta para esta labor, puntos importantes como por ejemplo: que las claves deberán tener al menos 8 caracteres alfanuméricos, así como también, poseer como mínimo una letra mayúscula, número o carácter especial y por último, que las claves tendrán que ser renovadas cada cierto tiempo, para más información sobre el Libro Naranja ver Anexo E.

Registro de las claves por departamentos.- de la misma forma la persona encargada será responsable de llevar un registro de las claves de todas las impresoras, para documentar los motivos para el cambio o actualización de una contraseña, sin olvidar el cuidado que deberá brindar a este documento.

---

[91] **Libro Naranja** del Departamento de Defensa de Estados Unidos, indica algunos de los niveles de seguridad para proteger la infraestructura tecnológica de un ataque al hardware, software y a la información guardada.

3.3.2.3 Servidor Web

En el caso del servidor web se utilizó un respaldo del la página y se la ubicó en una máquina virtual con la dirección IP 192.168.0.115, a la que se realizó los dos tipos de ataques. A continuación se explicarán los procesos de mitigación y solución para mantener segura la página de la Corte Constitucional.

- **Ataque de Diccionario**

Como primer proceso se realizó un ataque de tipo diccionario al servidor con el objetivo de descubrir la clave de administración de la página, luego de haber concluido con el ataque se descubrió que se mantenía el usuario y contraseña por defecto del gestor Joomla, que es el programa que contiene la página oficial de la entidad, debido a esto se propondrá las posibles mejoras para disminuir la posibilidad de un ataque de este tipo.

Mitigación.- lo primero que se recomienda hacer es modificar de forma inmediata la información actual del administrador de la página web, tanto usuario como contraseña, ya que de esta manera se obtendrá una disminución considerable en los posibles ataques que se puedan presentar.

Solución.- para cubrir con todos los parámetros de seguridad que se deben implementar en un servidor con información tan sensible, también será necesario utilizar el Libro Naranja de seguridad para incluir una política de creación de claves de seguridad para la administración de la página web, que en este caso será de Tipo, “A-Protección Verificada”, y que contemplará los siguientes parámetros:

1. Se deberá utilizar al menos 8 caracteres alfanuméricos para la creación de la nueva clave.
2. Se deberá utilizar dígitos, letras y caracteres especiales para la clave.
3. Se recomienda que las letras alternen aleatoriamente entre mayúsculas y minúsculas.
4. La contraseña tendrá que ser cambiada con una regularidad de al menos una vez cada 2 meses de tiempo. Y, a la vez, habrá que procurar no

generar reglas secuenciales de cambio, por ejemplo: pasar de “AdminServer2011” a “AdminServer2012”.

5. La utilización de signos de puntuación dentro de la contraseña si el sistema lo permite, para incrementar los niveles de complejidad.

Estas son algunas recomendaciones para generar una buena política sobre la creación y cambio de contraseñas para mantener protegidos los sistemas críticos de una empresa.

- **Ataque de inyección SQL**

Por último y con respecto a los posibles intentos de ataque por medio de inyección SQL que se puedan generar en contra de la página web institucional se propondrán las maneras más recomendables de mitigación y solución a los problemas detectados anteriormente.

Mitigación.- para disminuir el impacto de este tipo de amenazas a través de inyección SQL es necesario eliminar las cuentas por defecto que contiene el sistema, como el mail “operador@miempresa.com”, con el objetivo de denegar la conexión en caso de no registrar un mail autorizado dentro del servidor, o a su vez, se puede ingresar al administrador de Joomla en: Panel de control > configuración global > servidor, y en el formulario de “Configuración de correo” desactivar el servicio de sendmail que se encuentra habilitado.

Solución.- en caso de que se desee tomar medidas efectivas frente a este tipo de incidencias, existen dos formas de resolver estos ataques al servicio web que son:

La primera forma, es desactivando completamente el servicio de mensajería de correo sendmail que tiene el servidor, herramienta que utiliza la aplicación Joomla para poder enviar el mail de restablecimiento de contraseñas, para deshabilitar este servicio se debe hacer lo siguiente:

Detener el servicio: service sendmail stop
Ingresar al fichero **/etc/rc.conf** y modificar la siguiente línea:
sendmail_enable="NONE"

Ese es todo el procedimiento para que el servicio de mensajería quede deshabilitado y no pueda establecer ningún tipo de conexión con el servidor, ocasionando que la clave no sea autorizada por el sistema para ingresar y modificar los datos de administrador del aplicativo Joomla.

La segunda forma, es mantener el aplicativo Joomla siempre actualizado para evitar posibles intrusiones, gracias a la instalación continua de parches del sistema se logrará solucionar cualquier tipo de error de programación de la herramienta, que podría ser utilizado para acceder de forma no autorizada al sistema. Para realizar este proceso habrá que ingresar a la página oficial del gestor de contenido Joomla, http://joomlacode.org/gf/project/spanish/frs/?action=index, y buscar las actualizaciones pertinentes según la versión del aplicativo, en este caso se deberá descargar e instalar la actualización: “Joomla_1.7.2_a_1.7.5-Spanish-Parche_Pack.tar.gz”, para fortalecer la configuración del sistema, de esta manera se tendrá una administración más segura con el respaldo del servicio técnico del proveedor de la solución.

Con esto culmina el estudio de vulnerabilidades de los servicios de la Corte Constitucional; en el siguiente capítulo se detallarán los procesos pertinentes para crear un Equipo de respuesta ante incidentes de seguridad CSIRT, que ayudará con soluciones proactivas ante los incidentes que se puedan presentar.

CAPITULO 4

CSIRT INNOVACIÓN EN SEGURIDAD PROACTIVA

4.1 ANTECEDENTES

Como antecedente principal dentro del presente trabajo de tesis, será indispensable comenzar despejando las dudas sobre el significado del término CSIRT, que no es más que un Equipo de Respuesta a Incidentes de Seguridad Informática (por sus siglas en inglés: Computer Security Incident Response Team).

Las abreviaturas habituales que hacen referencia al mismo tipo de equipos son:

- **CERT o CERT/CC.-** Equipo de respuesta a emergencias informáticas / Centro de Coordinación (Computer Emergency Response Team). Término registrado en Estados Unidos y sus objetivos son trabajar junto a la comunidad de Internet para facilitar su respuesta a problemas de seguridad informática que afecten a los sistemas centrales de Internet, dar pasos proactivos para elevar la conciencia colectiva sobre temas de seguridad informática y llevar a cabo tareas de investigación que tengan como finalidad mejorar la seguridad de los sistemas existentes.
- **IRT.-** Equipo de respuesta a incidentes (Incident Response Team), es un grupo de personas que debe prepararse y responder a cualquier incidente de emergencia, tales como un desastre natural o una interrupción de las operaciones comerciales. Los equipos de respuesta a incidentes son comunes en las empresas, así como en organizaciones de servicio público. Este equipo se compone generalmente de determinados miembros designados antes de que ocurra un incidente, aunque en determinadas circunstancias, el equipo puede ser un grupo de voluntarios.
- **CIRT.-** Equipo de respuesta a incidentes informáticos (Computer Incident Response Team), es un grupo de personas cuidadosamente seleccionadas y bien capacitadas cuyo objetivo es manejar ágil y correctamente un incidente de manera que pueda ser rápidamente contenido, investigado, y recuperado.
- **SERT.-** Equipo de respuesta a emergencias de seguridad (Security Emergency Response Team), es un grupo de personas capacitadas que se encarga de la seguridad de las personas afectadas por los incidentes.

La aparición del término y del primer organismo CERT se difunde a finales del año de 1988, cuando el 2 de noviembre del mismo año Robert Morris, estudiante de la universidad de Cornell, desarrolla un "Worm[92]", un programa que lanzado desde un computador, generaba copias de sí mismo y se auto-enviaba a otras estaciones de trabajo, en cuestión de horas este “Worm” había infectado cerca de 6000 computadoras incluyendo equipos del Gobierno Federal, la NASA y la Fuerza Aérea.

A partir de este acontecimiento, el Gobierno de Estados Unidos y la Agencia de Investigación de Proyectos Avanzados de Defensa, DARPA[93], deciden crear el primer Equipo de respuesta a Emergencias informáticas CERT.

El CERT/CC se encuentra ubicado en la Universidad de Carnegie Mellon, en Pitsburgh (Pensilvania) y se encarga de enfrentar emergencias de seguridad y trabajar en la prevención de futuros incidentes, además de convertirse en un grupo que también brindará asesoramiento en la formación de equipos similares a nivel mundial.

Hay que aclarar que en Estados Unidos la abreviatura CERT/CC se encuentra registrada en la oficina de marcas y patentes, motivo por el cual, en varios países se necesita pagar para poder hacer uso de este término en proyectos de seguridad de la información, y es la razón principal para que se utilice la abreviatura CSIRT, ya que es un término de libre uso y que especifica las necesidades de la Corte Constitucional.

4.2 DEFINICIÓN

Un CSIRT, es un grupo de personas que velarán por la seguridad de las Tecnologías de la Información (TI) y cuya principal tarea es responder a los incidentes de seguridad informática. El CSIRT presta servicios de identificación y

---

[92] **Worm o gusano,** es código malicioso que tiene la propiedad de duplicarse a sí mismo. Obtenido en, http://es.wikipedia.org/wiki/Gusano_inform%C3%A1tico.

[93] **DARPA (Defense Advanced Research Projects Agency),** es una agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar. Obtenido en, http://es.wikipedia.org/wiki/Defense_Advanced_Research_Projects_Agency.

solución a las diferentes amenazas[94] y vulnerabilidades que se presentan en los sistemas de información de una organización.

Para mitigar los riesgos y minimizar el número de respuestas necesarias, la mayor parte de los CSIRT se encargan de reforzar y proteger la seguridad, brindan respuestas y elaboran planes y estrategias para responder ante cualquier amenaza, vulnerabilidad o ataque de terceros.

Este tipo de equipos se encargan de publicar avisos sobre las vulnerabilidades del software y el hardware en uso, e informan a los usuarios sobre los programas maliciosos y virus que se aprovechan de estas deficiencias. De este modo, la organización podrá corregir y actualizar rápidamente sus sistemas.

Las ventajas de contar con un CSIRT son:

- Disponer de una coordinación centralizada para la seguridad de las TI dentro de la Corte Constitucional.
- Reaccionar a los incidentes relacionados con las TI y tratarlos de un modo centralizado y especializado.
- Tener al alcance de la mano los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad.
- Realizar un seguimiento de los progresos conseguidos en el ámbito de la seguridad.
- Fomentar la cooperación en la seguridad de las TI entre los usuarios y el grupo de seguridad.

4.3 BENEFICIOS DE UN CSIRT

Los beneficios de un CSIRT ganarán valor dependiendo de los servicios que brinde a la Corte Constitucional, siempre tomando en cuenta la misión, visión y

[94] **Amenaza,** es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, serían los Elementos de Información. Obtenido en, http://protejete.wordpress.com/gdr_principal/amenazas_ vulnerabilidades/

área de cobertura donde se va a desempeñar, no hay que olvidar que el principal objetivo de este grupo de personas es trabajar para proveer un servicio y manejo de incidencias. Los servicios de un CSIRT pueden agruparse en tres categorías:

- Servicios Reactivos
- Servicios Proactivos
- Servicios de gestión de calidad de la seguridad

4.3.1 Servicios Reactivos

Hay que tener en cuenta que los servicios reactivos son acciones posteriores a los ataques, por esta razón estos servicios se inician ante un evento o pedido del usuario afectado. Este tipo de eventualidades podrían incluir diseminación de código malicioso[95], vulnerabilidad de software, virus o cualquier otra amenaza que fuera identificada por un sistema de detección de intrusos o un sistema de registro de eventos como riesgo para la red.

Los servicios reactivos son el componente central del trabajo de un CSIRT, y serán distribuidos como muestra la Tabla 4.1 a continuación:

SERVICIOS REACTIVOS

Alertas y Advertencias	Generación de alertas y advertencias
Riesgos	Manejo de incidentes
	Análisis de incidentes
	Respuesta al incidente en el lugar
	Coordinación de respuesta a incidentes
Vulnerabilidades	Manejo de vulnerabilidades
	Análisis de vulnerabilidades
	Respuesta a vulnerabilidades
	Coordinación de respuesta a vulnerabilidades

Tabla 4.1: Servicios Reactivos de un CSIRT
Autor: Tesista
Fuente: www.enisa.europa.eu/act/cert/support/guide/csirt/fullReport

[95] **Código malicioso o Artifacts,** se trata de código encontrado en un sistema, pueden incluir virus a computadoras, troyanos, gusanos, y herramientas de software o hardware. Obtenido en, http://es.wikipedia.org/wiki/Malware.

4.3.1.1 Alertas y Advertencias

4.3.1.1.1 Generación de Alertas y Advertencias

La generación de alertas y advertencias se deberá realizar desde el mismo CSIRT hacia todo el personal, esta labor consistirá en generar reportes donde se incluirá las distintas vulnerabilidades, intentos de intrusión, código malicioso o virus detectados últimamente en la red de datos de la entidad.

El equipo de respuesta a incidentes de seguridad se encargará de buscar la forma más adecuada para poder mitigar estas amenazas, ya sea con la compra de equipos o la suscripción a empresas externas que brinden este tipo de servicios, con el fin de precautelar la seguridad de la información.

En la actualidad se encuentran a diario actualizaciones sobre las posibles vulnerabilidades, virus e intrusiones más comunes y el equipo de respuesta tendrá que estar al tanto de todo esto para poder buscar la mejor solución.

4.3.1.2 Riesgos

4.3.1.2.1 Manejo de Incidencias

Esta parte comprende el análisis, clasificación y respuesta a las alertas y advertencias generadas anteriormente sobre los incidentes de vulnerabilidad generados. El manejo de incidentes comprende las siguientes actividades:

- Proteger la red y los sistemas afectados por la intrusión de un atacante.
- Brindar estrategias de mitigación ante posibles intrusiones
- Filtrar el tráfico de la red según usuario y privilegios.
- Desarrollar alertas y advertencias para evitar que se repitan las intrusiones detectadas.

Dentro del proceso de creación de un CSIRT el manejo de incidentes se clasifica en:

4.3.1.2.2 Análisis de Incidentes

Este análisis se encargará de recolectar toda la información generada últimamente sobre los incidentes presentados en la red de datos, con esta información se podrá realizar la evaluación del daño que cada una de las intrusiones presentó, para luego empezar con la mitigación y restauración de lo afectado, teniendo en cuenta que esta labor debe realizarse en el menor tiempo posible para reducir los efectos del ataque.

Los procesos para la recolección de información a utilizar en este tipo de análisis serán:

- **Rastreo.-** o seguimiento consiste en obtener la información necesaria sobre la intrusión detectada, como podría ser el acceso al sistema, hora de ingreso, dirección IP[96] y si fuera posible la o las herramientas que se utilizaron para lograr este cometido.

- **Recolección de evidencia.-** consiste en recolectar la documentación existente y realizar el estudio de la red y programas informáticos, con la finalidad de determinar cambios no autorizados en el sistema para reconstruir los eventos que han ocurrido.
  Esto podrá incluir copias de disco que hayan sido afectados, la búsqueda de cambios en el sistema, la instalación de nuevos programas, modificación de archivos, entre otras características.

4.3.1.2.3 Respuesta a Incidentes

Este tipo de respuesta se encargará de revisar y analizar físicamente los sistemas afectados por una determinada incidencia, brindando asistencia de forma directa a las personas involucradas, esta actividad de realizará para alcanzar una pronta reparación y recuperación de los sistemas.

---

[96] **Dirección IP,** es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz de un dispositivo dentro de una red. Obtenido en, http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP.

4.3.1.2.4 Coordinar a incidentes

El CSIRT coordina las tareas de respuesta entre las partes involucradas en el incidente, estas incluyen a la a la persona objeto del ataque, los sitios relacionados con el ataque, además, podría incluir a las partes que proporcionan apoyo de tecnologías de la víctima, como pueden ser proveedores de servicios de internet, administradores de sistemas y de redes.

El trabajo de coordinación consiste en reunir información del funcionario, área o departamento que se vio involucrado en el incidente con la finalidad de intercambiar información con la gente afectada y de esta manera buscar una solución

4.3.1.3 Vulnerabilidades

4.3.1.3.1 Manejo de Vulnerabilidades

Involucra la recepción de información y reportes acerca de las vulnerabilidades de software y hardware que se encontraron en el análisis previo, además, se deberá realizar un análisis de las causas y efectos que éstas podrían tener sobre los sistemas y en base a esto se desarrolla estrategias para reparar las mismas.

Las falencias detectadas en los sistemas tecnológicos analizados deberán ser atendidas de manera rápida, sin olvidar la instalación de herramientas que contribuyan a la detección y manejo continuo de brechas de seguridad.

4.3.1.3.2 Análisis a Vulnerabilidades

Consiste en buscar en donde se pueden encontrar posibles vulnerabilidades y como pueden ser explotadas, para esto se realizan estudios técnicos tanto del hardware como del software para determinar en donde se encuentran ubicadas las debilidades y cómo pueden ser explotadas por un agente externo o interno y de esta manera poder disminuir las probabilidades de un nuevo ataque.

Este tipo de estudios se los puede realizar con sistemas de prueba que ayuden analizando los puertos habilitados tanto en estaciones de trabajo como en servidores, así como también las actualizaciones de los distintos sistemas operativos y de esta manera poder ajustar adecuadamente la seguridad.

4.3.1.3.3 Respuesta a Vulnerabilidades

Consiste en determinar una respuesta apropiada para mitigar o reparar una vulnerabilidad anteriormente detectada, esto implica que los miembros del equipo deben estar en constante investigación y desarrollo de correcciones y soluciones provisionales, como instalación de actualizaciones en sistemas operativos, bloqueo de puertos, prevención de intrusos, prevención ante fugas de información, entre otras opciones más que se podrían evaluar según los objetivos del negocio.

4.3.1.3.4 Coordinación a Respuesta a Vulnerabilidades

El CSIRT está en la obligación de notificar a la institución sobre las debilidades encontradas y compartir toda la información que sea posible sobre las acciones que se tomaron para mitigar o reparar la vulnerabilidad.

La respuesta que se pueda dar a las vulnerabilidades detectadas tendrá q ser en el menor tiempo posible, ya que de esta manera se podrá eliminar posibles ataques posteriores.

4.3.2 Servicios Proactivos

Este tipo de servicio tendrá como prioridad anticipar los posibles ataques, problemas o amenazas que puedan surgir dentro de la red de datos de la Corte Constitucional; de esta forma tener la capacidad de proteger y asegurar la información.

El servicio proactivo servirá para reducir la cantidad de posibles incidentes en el futuro, se dividen de la siguiente manera:

SERVICIOS PROACTIVOS	
Anuncios	Posibles problemas de la red
Observación	Observación de la tecnología
Auditorías	Evaluaciones de seguridad
Seguridad	Infraestructuras y servicios
	Desarrollo de herramientas
	Configuración de las herramientas
	Servicios de detección de intrusos
	Difusión de información de seguridad

Tabla 4.2: Servicios Proactivos de un CSIRT
Autor: Tesista
Fuente: www.enisa.europa.eu/act/cert/support/guide/csirt/fullReport

4.3.2.1 Anuncios

Este tipo de servicio permite informar a los usuarios sobre las nuevas vulnerabilidades, ataques y herramientas de intrusión que se han detectado últimamente, facilitando de esta forma que los funcionarios estén enterados sobre la forma de atacar de personas externas y poder tomar medidas para proteger sus sistemas sobre los problemas encontrados.

4.3.2.2 Observación

El observatorio de tecnología proporciona un servicio de investigación continua para el CSIRT, averiguando sobre los últimos avances en lo que se refiere a nuevas formas de ataque, pero sobre todo, el cómo prevenirlas y evitarlas en un futuro.

Para mejorar este servicio hay la posibilidad de ponerse en contacto con otros CSIRTs que ya hayan tenido experiencia en resolver incidentes, por lo general éstos utilizan listas de correo, sitios web de seguridad y artículos actuales sobre tecnología para distribuir información del tema y de esta manera la organización se mantiene informada y actualizada.

4.3.2.3 Auditorías

Esta tarea consiste en un conjunto de acciones que realiza el personal en áreas que corresponden a la auditoría, con la finalidad de asegurar que todos los recursos operen en un ambiente de seguridad y control eficiente, para evitar ataques y vulnerabilidades a los sistemas de seguridad de la entidad.

Todas las evaluaciones realizadas dentro de la auditoría son a nivel de seguridad lógica y física, en donde deben estar establecidas políticas de seguridad, estrategias de continuidad del negocio y realizar pruebas a los sistemas para determinar cuáles podrían ser los más vulnerables.

4.3.2.4 Seguridad

4.3.2.4.1 Infraestructuras y Servicios

Este servicio consiste en realizar una guía de cómo configurar y mantener de forma segura las herramientas y aplicaciones propias de la entidad que van a ser administradas por el CSIRT.

El CSIRT estará en la obligación de realizar las configuraciones y el mantenimiento preventivo como correctivo pertinente a todos los equipos y herramientas de seguridad, tanto de funcionarios como usuarios externos, tomando en cuenta todas las normas de seguridad.

4.3.2.4.2 Desarrollo de Herramientas

Esta actividad comprende el desarrollo de herramientas principalmente de software, para mejorar el ambiente de seguridad de los usuarios; como por ejemplo podría ser el desarrollo de aplicativos que distribuyan actualizaciones de parches de sistema operativo a las estaciones de trabajo de los usuarios de forma remota.

Estas herramientas generalmente son desarrolladas a medida que las investigaciones del CSIRT lo requieran.

4.3.2.4.3 Configuración de las Herramientas

La configuración de herramientas de seguridad instaladas para servicio tanto de funcionarios como de usuarios deberá contemplar la aceptación de tráfico necesario, es decir, se tendrá que asegurar la red de manera equitativa para no restringir todo el tráfico, pero tampoco dejar pasar todo tipo de información que dejaría vulnerable a toda la entidad.

La configuración será estabilizada durante un período de prueba prudencial hasta llegar a satisfacer las necesidades del negocio como la de los funcionarios y usuarios que utilizan diversos servicios.

4.3.2.4.4 Servicios de Detección de Intrusos

Este servicio consiste principalmente en tener la posibilidad de implementar un sistema de detección de intrusos, con el objetivo de tener la posibilidad de revisar los archivos de log, para detectar alarmas o intentos de ataques a la red, y proceder a aplicar estrategias para minimizarlos y mitigarlos completamente.

En algunos casos se requiere de herramientas o conocimientos especializados para analizar e interpretar la información y así identificar alarmas y posibles ataques a la red, luego del análisis se procede a aplicar las estrategias necesarias para solucionar los problemas detectados.

4.3.2.4.5 Difusión de Información de Seguridad

La difusión de información es uno de los puntos primordiales del CSIRT, ya que de esta manera se comunica a la entidad sobre las vulnerabilidades y amenazas que se han descubierto, pero sobre todo, a cómo evitarlas y mejorar constantemente la seguridad, estos informes pueden incluir:

- Estadísticas sobre incidentes detectados
- Comunicados de alertas y vulnerabilidades
- Desarrollo de actualizaciones correctivas en estaciones de trabajo
- Asesoramiento sobre seguridad informática.

4.3.3 Servicios de Gestión de Calidad de la Seguridad

Estos hacen referencia a los beneficios obtenidos de la puesta en marcha del diseño de los servicios reactivos y proactivos para mejorar la seguridad de la organización.

Los servicios de gestión de calidad de la seguridad contemplan los siguientes puntos a ser tomados en cuenta:

- **Análisis de riesgo.-** comprende la capacidad de la entidad de evaluar y analizar todas las amenazas y riesgos que se puedan presentar, realizando un análisis respectivo de toda la infraestructura tanto lógica como física, de esta manera se logrará como organización tener la habilidad de combatir amenazas reales.
- **Continuidad del negocio.-** sin importar el tipo de amenaza o de vulnerabilidad detectada se tiene que priorizar la continuidad de las funciones de la entidad, por esta razón es que se deben desarrollar planes de contingencia para determinar la mejor forma de responder a una emergencia, y así asegurar la continuidad de las operaciones.
- **Concientización del personal.-** consiste en hacer entender a los funcionarios de una entidad sobre las políticas que se deben seguir, esto es muy importante, ya que al lograr que el personal entienda la importancia del uso de políticas de seguridad se va a conseguir que todos los procedimientos que ellos realicen sean seguros, se minimicen pérdidas y puedan reportar sobre algún ataque.

4.4 TIPOS DE EQUIPOS DE RESPUESTA A INCIDENTES CSIRTs

Los CSIRTs tienen diferente estructura dependiendo del sector al que quieran atender, los aspectos en los que difieren según su sector son:

1. Misión y objetivos del equipo
2. Comunidad a la que brinda servicios
3. Los servicios que brindará a la organización.

Actualmente los CSIRTs están divididos en los siguientes sectores:

4.4.1 CSIRT del Sector Académico

Los equipos de respuesta del sector académico prestan servicios a centros de educación, como universidades, colegios o centros de investigación y a sus campus virtuales si es que los poseen.

El grupo de usuarios atendido por este sector está formado por el personal administrativo, docentes y estudiantes de cada uno de los establecimientos académicos.

4.4.2 CSIRT del Sector Comercial

Estos equipos de respuesta prestan servicios comerciales a sus clientes. Puede ser que en el caso de un proveedor de servicios de internet, el CSIRT presta principalmente servicios de respuesta de incidentes, como denegación de servicio, perjudicando a los usuarios finales al quedarse sin servicio de Internet por un tiempo prolongado.

El grupo de usuarios atendido por un CSIRT comercial, son aquellos clientes que pagan por ello.

4.4.3 CSIRT del Sector Público

Los equipos de respuesta implementados en el sector público prestan servicios a entidades del estado, y en algunos países también a los ciudadanos. En países de Sudamérica como Chile, Argentina y Brasil se ha implementado un CSIRT a nivel nacional para proveer consejos importantes sobre seguridad a cada una de las entidades gubernamentales, mejorando el sistema de detección proactiva de vulnerabilidades e incidentes.

El grupo de usuarios atendido en este sector contempla a las entidades públicas, sus administradores y funcionarios.

4.4.4 CSIRT Interno

Los equipos de respuesta implementados de forma interna prestan servicios a la organización a la que pertenecen, esto quiere decir que prioriza más el funcionamiento que dará internamente que su pertenencia a un sector. Varias organizaciones de telecomunicaciones y bancos cuentan con sus propios CSIRT internos para poder mitigar amenazas.

El grupo de usuarios que se beneficia con este tipo de CSIRT es el departamento y personal de tecnología de la organización.

4.4.5 CSIRT del Sector Militar

Los equipos de respuesta de este sector como su nombre lo indica prestan servicios a organizaciones militares con responsabilidades en infraestructuras de TI, necesarias con fines de defensa.

El grupo de usuarios atendido por este sector corresponde a instituciones militares y de entidades estrechamente relacionadas con éstas.

4.4.6 CSIRT Nacional

Este tipo de equipo de respuesta se considera un punto de contacto de seguridad a nivel de país. En algunos casos, el CSIRT del Sector Público también puede ser considerado como Nacional, ya que ambos equipos de respuesta se encuentran trabajando para mejorar la seguridad gubernamental, la diferencia estaría en que el CSIRT Nacional sirve como intermediario entre los CSIRT del Sector Público para desempeñar sus funciones.

Los usuarios atendidos por este grupo corresponden a un sector de clientes directo, elegido al momento de poner en marcha este tipo de equipo.

4.4.7 CSIRT de la Pequeña y Mediana Empresa PYME[97]

Se trata de un equipo de respuesta organizado por sí mismo que presta servicios a las empresas del mismo tipo o a un grupo de usuarios similar. Las pequeñas y medianas empresas son entidades independientes, con una alta predominancia en el mercado de comercio y que se encuentran excluidas del mercado industrial por el alto nivel de inversión que se necesita.

El grupo de clientes atendido por estos CSIRT pueden ser las pequeñas y medianas empresas y su personal, o grupos de interés especial dentro de un país, como podría ser un grupo de municipalidades o gobernaciones.

4.4.8 CSIRT de Soporte

Los equipos de respuesta de soporte se centran en productos específicos. Suelen tener por objetivo desarrollar y facilitar soluciones para eliminar vulnerabilidades y mitigar posibles efectos negativos a sus usuarios finales.

El grupo de clientes atendido por estos CSIRT corresponden a los propietarios de productos que necesitan soporte ante posibles amenazas.

4.5 DEFINIR LA ESTRUCTURA DE UN CSIRT

Dependiendo del tipo de CSIRT, su estructura organizacional, su misión, sus servicios y la comunidad que va a ser atendida, se debe buscar personal capacitado para generar un equipo de respuesta acorde con las necesidades de la entidad.

El equipo de respuesta tiene la responsabilidad del control, la respuesta de incidentes y vulnerabilidades encontradas, de manera que al momento de ocurrir alguna amenaza o incidente el equipo está preparado para controlarlos.

Por las razones antes descritas un CSIRT necesita de los siguientes integrantes:

---

[97] **PYME,** acrónimo lexicalizado de pequeña y mediana empresa, es una empresa con características distintivas, y tiene dimensiones con ciertos límites ocupacionales y financieros prefijados por el Estado. Obtenido en, http://es.wikipedia.org/wiki/Peque%C3%B1a_y_mediana_empresa.

- **Director general.-** Las características del director general tendrán que ser las de un líder para todo el grupo, ya que tiene que poder comunicar las distintas tareas de investigación pero sobre todo ser capaces de tomar decisiones rápidas ante ataques y situaciones de emergencia de manera que nada quede sin ser atendido. Algunas de las funciones y responsabilidades del Director General se detallan en la Tabla 4.3:

FUNCIONES	RESPONSABILIDADES
Coordinar actividades del equipo	Revisar los avances de investigación
Asignación de tareas para los miembros del grupo	Representar al equipo ante las autoridades
Dirigir las investigaciones sobre incidentes y vulnerabilidades	Toma de decisiones sobre incidentes detectados
Coordinar a los miembros del equipo para que puedan capacitar a los funcionarios	Comunicar a las autoridades sobre incidencias o vulnerabilidades detectadas
Entrevistar a los nuevos integrantes	Capacitación de los miembros del equipo.

Tabla 4.3: Funciones y Responsabilidades del Director General
Autor: Tesista
Fuente: Tesista

- **Jefe del equipo técnico.-** como jefe del equipo técnico se encuentra el Administrador de la Red que se encarga de todos los aspectos que se relacionan con el área de la red y datacenter de la organización, por esta razón son los encargados de mantener la infraestructura de red del CSIRT, a través de servidores seguros, correo electrónico seguro y cualquier otro requerimiento exigido por la organización. Algunas de las funciones y responsabilidades del Jefe del equipo técnico se detallan en la Tabla 4.4:

FUNCIONES	RESPONSABILIDADES
Coordinar actividades de los técnicos	Revisar los avances de investigación
Asignación de tareas para los técnicos e investigadores	Representar al equipo ante el Director General
Incentivar la búsqueda continua sobre nuevas incidencias.	Conocimiento sobre seguridad de la información
Capacitar a los técnicos e investigadores del equipo	Comunicar al Departamento de Tecnología sobre incidencias o vulnerabilidades detectadas

Tabla 4.4: Funciones y Responsabilidades del Jefe Técnico
Autor: Tesista
Fuente: Tesista

Sus características técnicas tienen que ver con el conocimiento sobre seguridad de la información, sistemas operativos, aplicaciones y protocolos usados en la entidad, que servirán para coordinar posibles auditorías de vulnerabilidades y riesgos con los técnicos de prestación de servicios.

- **Técnicos encargados de la prestación de servicios.-** personal que atenderá las llamadas telefónicas dirigidas al equipo de respuesta, en las que se reporten incidentes de seguridad, brindan asistencia inicial de acuerdo al tipo de incidente que se reporte. La clasificación de incidente debe ser realizada de acuerdo a las prioridades que se han establecido en el equipo.

FUNCIONES	RESPONSABILIDADES
Atender a los funcionarios	Solucionar problemas en estaciones de trabajo
Acudir a dar soporte en el lugar de incidencia	Llevar reporte sobre incidencias
Presentar informes al Jefe Técnico sobre incidentes y vulnerabilidades reportadas	Comunicar al Jefe Técnico sobre incidencias o vulnerabilidades detectadas
Atención de llamadas y clasificación de incidentes	Recomendaciones a los funcionarios sobre lo que no se tiene que hacer

Tabla 4.5: Funciones y Responsabilidades de los Técnicos
Autor: Tesista
Fuente: Tesista

Estos técnicos se ven en la obligación de trabajar junto con los desarrolladores web, para también poder brindar asistencia a los usuarios con las aplicaciones creadas internamente.

- **Investigador.-** por último el investigador que es parte del CSIRT debe mantenerse constantemente actualizado sobre los nuevos incidentes y vulnerabilidades detectados, ya sea por otros CSIRTs a nivel mundial o por boletines de prensa. El objetivo de los investigadores es mantener un paso adelante a todo el equipo de respuesta ante posibles incidencias de seguridad de TI.

4.5.1 Modelo de Estructura

Una vez que se ha definido el personal que va a formar parte del CSIRT, se debe definir la estructura organizativa del equipo. Los distintos modelos se muestran a continuación en la Tabla 4.3 y estos son:

#	Modelos
1	Modelo de Estructura Independiente
2	Modelo Incrustado
3	Modelo Universitario
4	Modelo Voluntario

Tabla 4.6: Modelos Estructurales de un CSIRT
Autor: Tesista
Fuente: www.enisa.europa.eu/act/cert/support/guide/csirt/fullReport

4.5.1.1 Modelo de Estructura Independiente

Es un modelo extendido que actúa como una organización independiente dentro de la entidad donde se va a desarrollar y se encuentra conformado generalmente por su propio personal. La distribución de este modelo se muestra en la siguiente Figura 4.1:

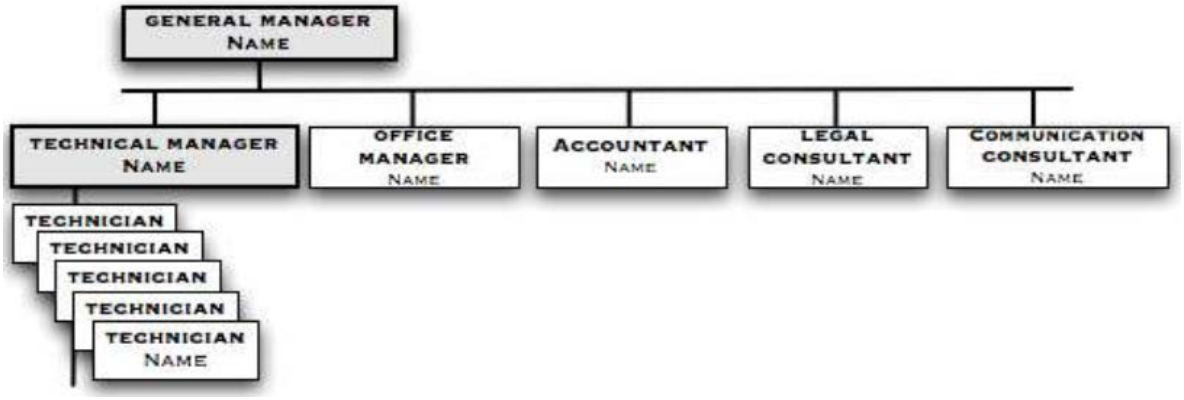


Figura 4.1: Modelos de Estructura Independiente
Autor: Tesista
Fuente: www.enisa.europa.eu/act/cert/support/guide/csirt/fullReport

De acuerdo a lo observado en la figura anterior, este equipo se encuentra organizado por los siguientes miembros:

- **General Manager:** Director General del Equipo
- **Technical Manager:** Jefe del equipo Técnico

- Técnicos del equipo
- Investigadores

- **Office Manager:** Director de la Oficina
- **Accountant:** Personal Contable
- **Legal Consultant:** Asesor Jurídico
- **Communication Consultant:** Consultores externos

4.5.1.2 Modelo Incrustado

Este modelo es apropiado cuando se ve la necesidad de crear un CSIRT dentro de una organización existente, usando un Departamento de Tecnología ya existente. En este caso el Director del Departamento de Tecnología es el responsable de todas las actividades del equipo de respuesta. En caso de que se presente algún incidente el jefe reunirá todos los técnicos necesarios para dar solución a los problemas, y de ser necesario podría solicitar asistencia externa. El modelo se muestra en la Figura 4.2 a continuación:

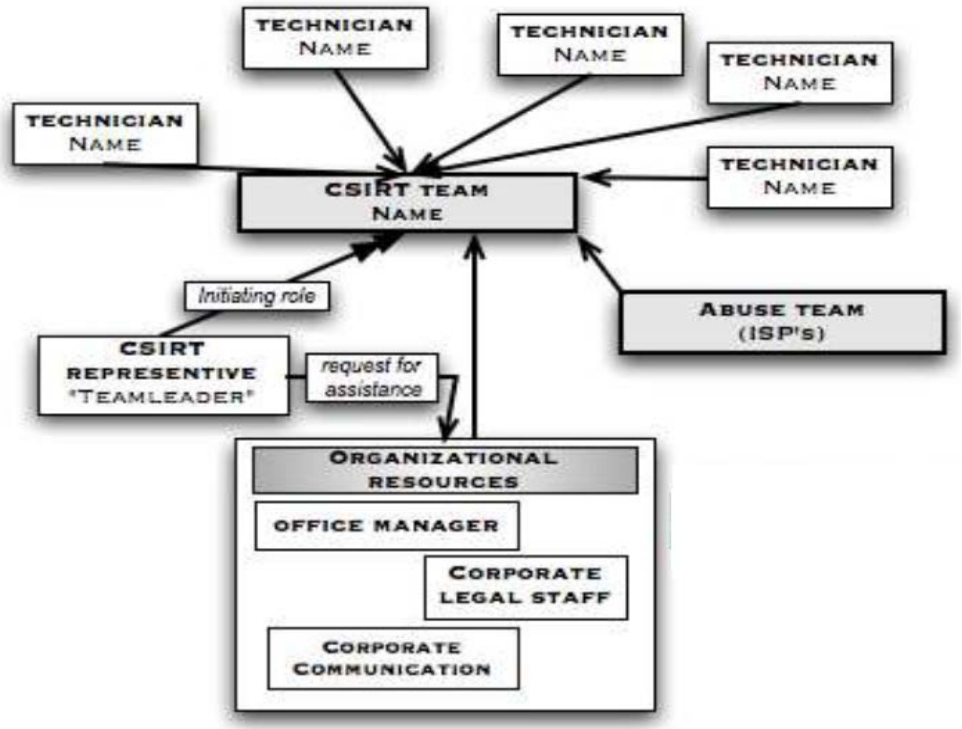


Figura 4.2: Modelos de Estructura Incrustado
Autor: Tesista
Fuente: www.enisa.europa.eu/act/cert/support/guide/csirt/fullReport

Con respecto a la figura anterior el personal que se necesita para este modelo es:

- **CSIRT Representive:** Líder o Representante del CSIRT, que es el que atenderá las necesidades del negocio y representará al equipo de respuesta ante los departamentos administrativos de la entidad.
- **Technician:** Técnicos responsables de la asistencia a incidentes de seguridad.
- **Technician Investigador:** Persona responsable de investigar sobre nuevos incidentes y vulnerabilidades.

4.5.1.3 Modelo Universitario

Como su nombre hace referencia este modelo generalmente se lo adopta en establecimientos académicos y de investigación. La mayor parte de estas instituciones están formadas por dos o más facultades distribuidas en diferentes ubicaciones, que pueden estar dentro de una misma región como diseminadas en todo el país.

Por lo general todos estas facultades o campus son independientes entre sí y pueden poseer su propio CSIRT, pero se encuentran organizados por un CSIRT central que los coordina y es el único punto de contacto para realizar toma de decisiones, también desde aquí se informará a los otros CSIRTs sobre los nuevos incidentes detectados. El modelo estructural se muestra en la Figura 4.3:

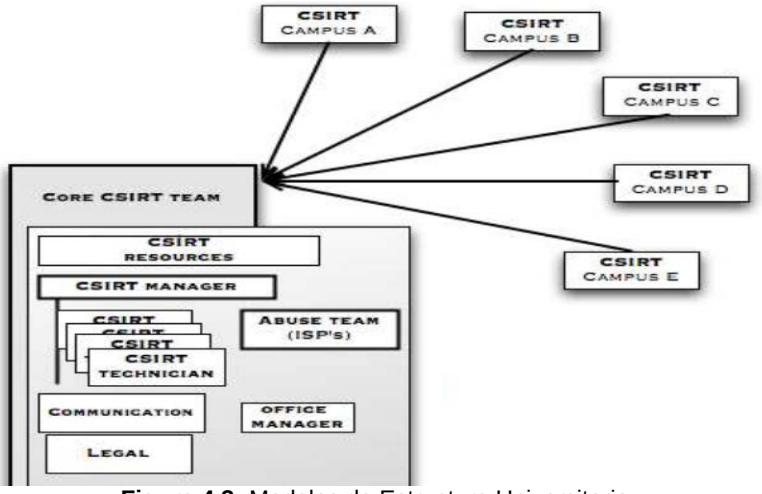


Figura 4.3: Modelos de Estructura Universitario
Autor: Tesista
Fuente: www.enisa.europa.eu/act/cert/support/guide/csirt/fullReport

Los elementos que intervienen en este modelo son:

- **CSIRT Central:** Que estará conformado por el Director del equipo de respuesta, los técnicos que brindarán asistencia, los investigadores de incidencias y un Departamento Legal como de Comunicación para completar las funciones de este punto central.
- **CSIRTs de Campus:** Que estarán creados en cada campus o facultad miembro de la institución académica o de investigación.

4.5.1.4 Modelo Voluntario

Este modelo corresponde a un grupo de personas que se reúnen para asesorarse y apoyarse entre sí de forma voluntaria. Actúan de forma espontánea y sus resultados dependerán de la motivación de los participantes que sean miembros de este modelo.

En el Capítulo a continuación se definirá el Diseño del CSIRT de la Corte Constitucional, definiendo todo lo explicado anteriormente, como los servicios que va a brindar, el tipo de equipo de respuesta que se establecerá dependiendo de la organización y el modelo de estructura para que preste sus servicios de seguridad internamente.

CAPITULO 5

DISEÑO DEL CSIRT CORTE CONSTITUCIONAL

5.1 COMPARACION ENTRE METODOLOGÍA ISACA Y CSIRT PARA EL DISEÑO DEL EQUIPO DE RESPUESTA DE LA CORTE CONSTITUCIONAL

Antes de comenzar con el diseño del CSIRT para la Corte Constitucional se analizará la metodología más adecuada para ser implementada dentro de la entidad, se resumirán las dos metodologías y se especificarán las razones pertinentes para escoger una de las dos propuestas.

5.1.1 Metodología CERT/CC

La metodología CERT/CC se basa en la siguiente distribución para el análisis y gestión de la seguridad para el diseño del CSIRT de la Corte Constitucional, como lo muestra la Figura 5.1 a continuación:

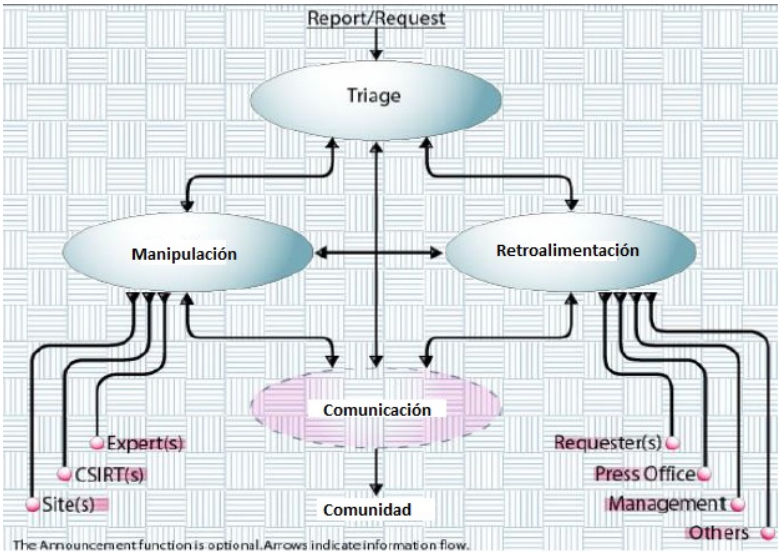


Tabla 5.1: Modelo de metodología CSIRT
Autor: Tesista
Fuente: http://www.csirt.org

Las funciones que propone este método dependiendo de sus categorías son:

Función Triage.- esta función se encarga de asegurar que toda la información destinada para el manejo de incidentes sea canalizada a través de un único centro de coordinación independientemente del medio, como por ejemplo: correo electrónico, fax o teléfono, estas herramientas se utilizarán para enviar la información y en base a esto poder responder con el apropiado manejo y distribución de responsabilidades.

Este proceso consiste en recibir la información, clasificarla y ordenarla con la finalidad de determinar si el reporte que se recibe está relacionado con eventos pasados o son nuevos eventos, luego se asignará una prioridad inicial que esté de acuerdo al esquema de prioridades que se esté manejando dentro del equipo.

Función Manipulación.- esta función se encarga de proporcionar respuesta y soporte a los informes recibidos de los usuarios a los que se brinda el servicio, entre estos se podría definir el lugar para la presentación de informes, donde se pueda receptar todas las solicitudes generadas por las personas afectadas, así como también, realizar los análisis de los sitios afectados, revisar los documentos y generar los avisos técnicos para proveer soporte técnico y asistencia en el lugar del incidente, generando con esto un proceso de notificación que brinde una adecuada respuesta y recuperación de la información, manteniendo una constante comunicación con las personas afectadas por el incidente.

Función Comunicación.- el propósito de esta función es generar información para la comunidad atendida por el equipo de respuesta CSIRT, el objetivo específico de la comunicación es la de revelar y compartir con los usuarios afectados los detalles de las amenazas actuales, y de las medidas que pueden ser tomadas para que los incidentes sean mitigados.

Parte de este proceso tiene que ver con la capacitación de los usuarios, para que no vuelvan a generar un incidente dos veces, así como también, se pueden crear avisos, guías o procedimientos técnicos que tendrán que seguir en caso de que se presente algún evento en contra de la seguridad de la información.

Función Retroalimentación.- el manejo de incidentes es el objetivo de todo CSIRT pero también es necesario atender otro tipo de requerimientos que son parte da la retroalimentación de funciones, como por ejemplo: la seguridad general de los computadores, actualización continua de licencias y recuperación eficaz de información, todo esto es importante porque así no se afectará la imagen del equipo en el sentido de que no brinda respuesta a otro tipo de solicitudes o requerimientos que son distintos del manejo de incidentes.

5.1.2 Metodología ISACA

ISACA es una organización mundialmente reconocida como líder por proveer conocimiento, certificaciones, apoyo y educación en seguridad, además de, aseguramiento de sistemas de información, administración de TI y de riesgos relacionados con TI. Debido a todo este proceso de estudios ha generado el "Modelo de Negocio para la Seguridad de la Información[98]" para mejorar la gestión de seguridad en las organizaciones y se muestra en la Figura 5.2 a continuación:

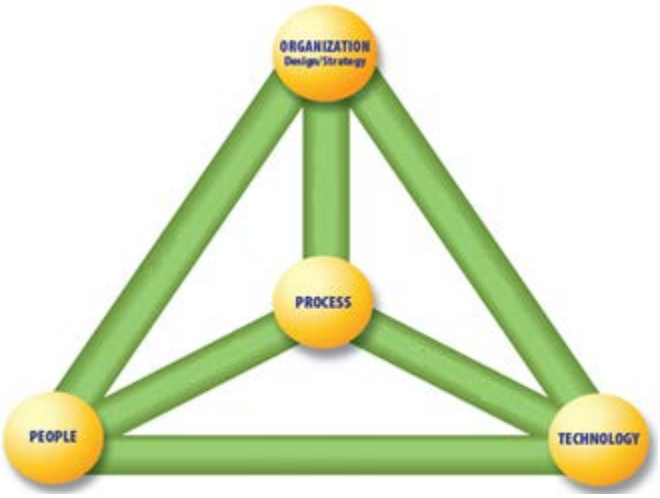


Tabla 5.2: Modelo de Negocio para la seguridad de la Información
Autor: Tesista
Fuente: http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx

Este modelo se basa en un diseño piramidal que consta de los siguientes niveles para la gestión de procesos de seguridad y que ayudará a la creación del CSIRT de la Corte Constitucional:

Organización.- según este modelo una organización es una red de personas, bienes y procesos que interactuarán entre sí en roles definidos, para trabajar hacia una meta en común que es la seguridad de su información, definiendo los siguientes parámetros para su creación:

[98] **Business Model Information Security (BMIS),** el Modelo de negocio para Seguridad de la Información. Obtenido en, www.isaca.org/Knowledge-Center/BMIS/Pages /Business-Model-for-Information-Security.aspx

- Dependiendo del tipo de organización y de la información que se desee precautelar, se deberá generar los procesos más adecuados para proteger la información
- Generar un modelo de estructura y caacitación para las personas que estarán a cargo de atender las fallas de seguridad.
- Definir los servicios que brindará la gestión de seguridad dentro de la organización, y su debida comunicación a las personas beneficiadas por el proceso.

Por esta razón es que la estrategia de una empresa es especificar sus objetivos de negocio y los objetivos a alcanzar así como los valores y misiones que se persiguen. La fórmula del éxito será definir su orientación básica, y la estrategia deberá adaptarse a los factores internos y externos. Las necesidades sobre seguridad serán la materia prima para diseñar la estrategia apropiada.

Procesos.- incluye mecanismos formales como utilización de normas técnicas e informales como creación de grupos de seguridad para realizar las distintas actividades, esto favorecerá a los procesos de identificación, gestión, control de riesgo y comunicación, así como también, a la disponibilidad, integridad y confidencialidad de la información. La creación de estos procesos puede incluir:

- La forma de reportar los eventos de seguridad.
- La creación de formularios para documentar las incidencias detectadas.
- Normas para responder a vulnerabilidades detectadas
- Asignación de responsabilidades y procedimientos a las personas involucradas en atender las falencias de seguridad.

Los procesos deben cumplir con los requerimientos del negocio y estar alineados a la política de la entidad, además de ser revisados periódicamente, una vez que estén en su lugar, asegurando de esta forma la eficiencia y la eficacia del modelo.

Personas.- este elemento representará a los recursos humanos, los problemas de seguridad que los rodean y la capacitación que se les puede brindar. Internamente, es muy importante para el gerente de seguridad de la información

trabajar con los recursos humanos y servicios jurídicos para hacer frente a cuestiones tales como: las estrategias de contratación de nuevo personal, la asignación de responsabilidades dentro de la entidad y si fuera el caso la terminación de sus labores. Todo esto para mantener un buen esquema de seguridad sobre las personas que laboran dentro de la organización.

Tecnología.- el elemento de la tecnología se compone de todas las herramientas, las aplicaciones y la infraestructura que pueden hacer más eficientes los procesos. Este proceso contempla la dependencia de la empresa en la tecnología, ya que ésta constituye una parte fundamental de la infraestructura y un componente esencial para prevenir ataques contra la seguridad de la información.

Normalmente a este proceso no se lo toma en cuenta en varios modelos ya que las personas todavía desconfían de la tecnología y de sus beneficios. Independientemente de la razón para no usar esta herramienta, los administradores de seguridad de la información deben ser conscientes de que mucha gente va a tratar de eludir los controles técnicos generados y para cubrir esa área esta la tecnología.

5.1.3 Justificación sobre metodología escogida para el diseño del CSIRT

Después de haber analizado los dos tipos de metodologías, en este caso se utilizará el “Modelo de Negocio para la Seguridad de la Información” de ISACA para poner en marcha el diseño del CSIRT de la Corte Constitucional, por las siguientes razones:

- La principal razón para utilizar este modelo es que contiene toda la metodología de CSIRT, pero, además añade la parte de administración de tecnología, que es primordial en las empresas y organizaciones para respaldar los procesos de aseguramiento de la información, sin contar con las técnicas de prevención que se puedan implementar.
- Este modelo fue creado específicamente para manejar la gestión de seguridad en las organizaciones, ya que consta de un módulo de procesos que se basa en técnicas formales para administrar a los módulos de

personas y tecnología, brindando gran beneficio a la organización que lo implemente.

- Proporciona una herramienta para administrar la seguridad de la información, además de poder generar todo el proceso del equipo CSIRT dentro de esta metodología.
- Por último los procesos son expandibles según los requerimientos de la organización y sobre todo se podrán adaptar al equipo de seguridad CSIRT de la Corte Constitucional para brindar un mejor servicio proactivo a todos los funcionarios.

5.2 METODOLOGÍA ISACA PARA LA DEFINICIÓN DEL CSIRT CORTE CONSTITUCIONAL

El “Modelo de Negocio para la Seguridad de la Información” de ISACA, ayudará a dar un enfoque integral y orientado sobre la gestión de seguridad de la información que manejará el CSIRT.

Este modelo de negocios para la seguridad de la información permitirá al equipo CSIRT examinar la seguridad desde la perspectiva de los sistemas, creando un ambiente donde la seguridad se puede gestionar de manera integral, permitiendo que los riesgos reales sean abordados por procesos proactivos. Este modelo es mejor visto como una solución flexible, con una estructura piramidal que se compone de cuatro elementos como se puede apreciar en la Figura 5.3:

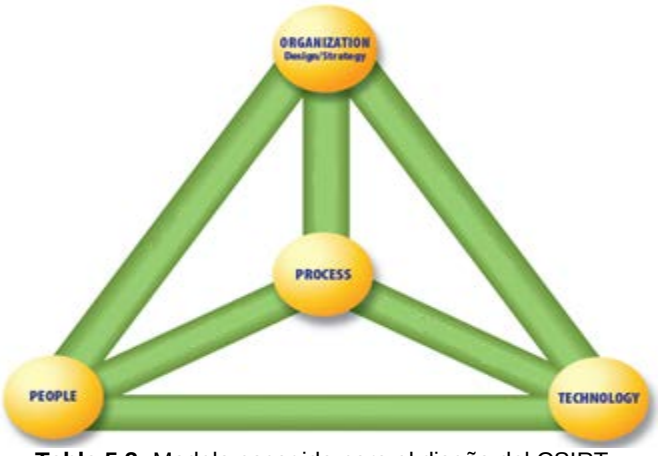


Tabla 5.3: Modelo escogido para el diseño del CSIRT
Autor: Tesista
Fuente: http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx

Las cuatro partes que se observaron en la pirámide como son: Organización, Proceso, Tecnología y Personal, se utilizarán para definir el diseño y procedimientos del CSIRT de la Corte Constitucional y serán detallados individualmente a continuación.

5.2.1 Organización

Para crear el diseño del CSIRT de la Corte Constitucional primero habrá que definir detalles como el “Tipo de equipo de respuesta que se va a implementar en la entidad”, así como también su “modelo estructural” y los “servicios que podría brindar a los funcionarios”, de acuerdo a lo que se detalló como parte introductoria en el capítulo anterior.

Un CSIRT no posee una manera definida para su creación, al contrario, este tipo de equipo de respuesta puede ser creado según las necesidades actuales de la organización en la que se desee implementar, por esta razón es que todas las políticas y procedimientos que se detallarán a continuación representan una necesidad actual de la Corte Constitucional.

Cabe mencionar que el presente análisis quedará tan solo como un diseño propuesto para mejorar la gestión de incidentes en la Corte Constitucional, entidad que de ser necesario y de requerirlo lo implementará posteriormente.

5.2.1.1 Tipo de CSIRT

A pesar de que la Corte Constitucional es una entidad que pertenece al sector gubernamental no se escogerá el CSIRT del Sector Público, puesto que este tipo de equipo de respuesta normalmente es creado para dar servicio a todas las instituciones públicas que son parte de un país, y en este caso solo se lo necesita diseñar de manera interna para cubrir con las necesidades del negocio de la Corte Constitucional. Por esta razón es que de entre todos los tipos de equipos de respuesta el más conveniente para las necesidades de la Corte es el “CSIRT Interno”, ya que este se dedicará a dar soporte solo a la organización a la que pertenece.

Este equipo de respuesta CSIRT se encargará tanto de la seguridad interna como externa de la organización, se manejará también problemas de seguridad y tecnologías como firewalls, antivirus, detección y prevención de intrusiones, fuga de información, entre otras, dependiendo de las necesidades inmediatas de la entidad, de los funcionarios o de los usuarios externos.

El objetivo principal de este CSIRT Interno será configurar, detectar anomalías de seguridad, proteger la infraestructura y las aplicaciones, logrando un desempeño óptimo para el cuidado de los bienes y servicios ofrecidos por la Corte Constitucional, estará encargado de realizar actividades tanto reactivas como proactivas.

A su vez, el equipo de respuesta deberá contar con personal preparado para responder a las anomalías detectadas de forma reactiva, como también de forma proactiva con personal que a menudo se encuentre en búsqueda de posibles brechas de seguridad en la red o en las aplicaciones que estén funcionando.

5.2.1.2 Modelo de Estructura del CSIRT

El modelo que se utilizará para el diseño del CSIRT de la Corte Constitucional es el “Modelo de Estructura independiente”, ya que este modelo se desarrolla dentro de la entidad y además utiliza su propio personal para desempeñar sus funciones.

De acuerdo al personal que posee actualmente el Departamento de Tecnología la distribución del modelo estructural sería la siguiente como muestra la Figura 5.4:

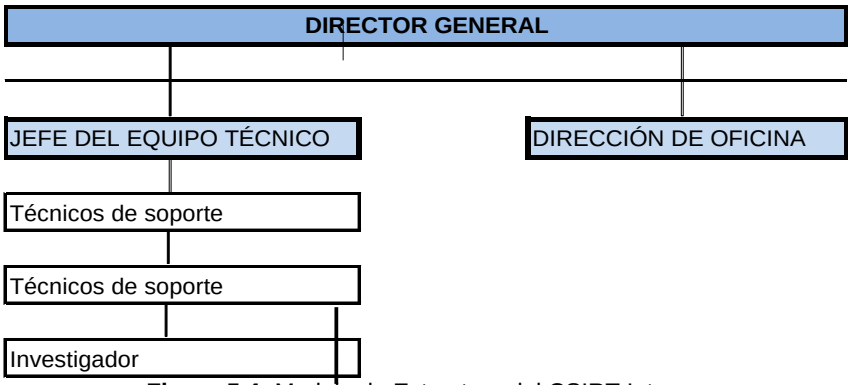


Figura 5.4: Modelo de Estructura del CSIRT Interno
Autor: Tesista
Fuente: Tesista

- **Director General del CSIRT:** Director del Departamento de Tecnología
- **Jefe del Equipo Técnico:** Administrador de la Red
    - Técnicos de Soporte
    - Investigador
- **Dirección de Oficina:** Coordinadora de Sistemas

El éxito con la implementación de este modelo se logrará con la cooperación entre todos los miembros que son parte del CSIRT, de esta manera la coordinación y conocimiento de todas las actividades que realizará el equipo de respuesta estarán a cargo del Director General, además de esto se deberán generar políticas y procedimientos claros sobre el manejo de vulnerabilidades e incidentes, pero sobre todo de cómo respondes a éstos en un momento determinado.

5.2.1.3 Servicios del CSIRT

Algunos de los servicios proactivos y reactivos que se podrían obtener con este diseño se los detallará en la Tabla 5.1 a continuación:

#	Actividades Proactivas	Actividades Reactivas
1	Analizar el soporte de concurrencia de los servidores para evitar ataques de DoS[99].	Atención a infección de virus en estaciones de trabajo
2	Realizar análisis periódicos de vulnerabilidades, generando alertas sobre los peligros detectados.	Instalación de infraestructura tecnológica para cubrir falencias de seguridad encontrada, como UTMs, Firewalls, etc.
3	Coordinar respuestas y recuperación después de que se presente un posible incidente.	Instalación de equipos de prevención y detección de intrusos a la red.
4	Investigación sobre ataques a otras entidades públicas para prevenir el mismo patrón de amenaza.	Poseer personal para poder reaccionar contra ataques que se presenten en tiempo real
5	Comunicar a los funcionarios sobre los peligros de infección con virus que existen en internet, como publicidad engañosa, correos de destinatarios desconocidos, etc.	Soporte técnico presencial en el momento en que se reporte algún incidente ya sea de un funcionario como de un usuario.

Tabla 5.1: Actividades Proactivas y Reactivas del CSIRT Interno
Autor: Tesista
Fuente: Departamento de Tecnología

[99] **DoS (Denial of Service),** un ataque de denegación de servicio es una violación a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Obtenido en, http://es.wikipedia.org/wiki/Ataque_de_denegación_de_servicio

Cabe mencionar que los servicios del equipo de respuesta van de acuerdo a cómo se va a responder a los diferentes incidentes y las actividades proactivas que se van a implementar.

Los servicios proactivos generados a partir de su implementación podrían incluir herramientas de seguridad, capacitación de funcionarios o investigación continua para generar nuevos tipos de alerta y prevención a toda la institución, mientras que los servicios reactivos atenderán de manera inmediata falencias encontradas en la red o en aplicaciones.

Por otra parte para la generación de respuesta a incidentes se podría evaluar informes de incidentes y realizar su respectivo seguimiento, o a su vez, realizar la coordinación y notificación de incidentes; con la explotación de estas vulnerabilidades y el estudio de lo que estas puedan causar se podrá brindar ayuda en la recuperación de los sistemas afectados.

5.2.2 Proceso

Dentro de cualquier organización ya sea esta pública o privada la prioridad será la de proteger la información, utilizando para este caso un proceso de creación de políticas y procedimientos, la gestión de seguridad de datos en la Corte Constitucional y este diseño propuesto esta guiado para prevenir la perdida de información importante con la generación de de estas reglas de seguridad, que no son más que un conjunto detallado de pasos a seguir para proteger los recursos importantes de la organización.

Las políticas que se propondrán para este diseño están creadas para garantizar los tres puntos principales de la seguridad de las tecnologías de la información, como son:

- Integridad
- Confidencialidad
- Disponibilidad

Como se puede apreciar en la Figura 5.5 a continuación:

Figura 5.5: Seguridad de la Información
Autor: Tesista
Fuente: Tesista

Las políticas por lo general se desarrollan dependiendo del tipo de organización, además de utilizar normas y procedimientos para lograr su ejecución de forma óptima en la Corte. De forma resumida se explicará cada uno de los puntos para la seguridad de la información:

Confidencialidad.- dentro de una organización la confidencialidad se resume como el acceso a información específica que se le da a un funcionario o grupo de funcionarios. El precautelar la confidencialidad de la información que pasa a través de la red o que se almacena en los distintos servidores de la Corte Constitucional es responsabilidad del Departamento de Tecnología, evitando que la información sea divulgada entre personas o sistemas no autorizados.

Integridad.- es el acto de procesar y mostrar la información libre de modificaciones por personal no autorizado. Tomando en cuenta que la Corte Constitucional es la entidad obligada a impartir justicia a nivel nacional su prioridad es mantener integra la información que se genera a diario, por este motivo habrá que generar un diseño que garantice que la información no ha sido manipulada y que se la presentará tal cual fue generada.

Disponibilidad.- es la cualidad de disponer de la información o de los aplicativos por funcionarios autorizados en el momento en el que lo requieran. El acceso a la información está ligado a la alta disponibilidad, ya que se deben brindar los recursos tecnológicos necesarios para que siempre se encuentre disponible la información, como por ejemplo, creando enlaces redundantes para no quedarse sin servicio de internet.

5.2.2.1 Norma ISO 27002

En un principio esta norma fue creada como un conjunto de pasos y buenas prácticas para obtener una adecuada seguridad de la información, este estándar fue publicado por primera vez en el año 2000 por la ISO/IEC[100] como: 17799, con el título de, “Código de prácticas para la administración de seguridad de la información”; sin embargo, después de un período de actualizaciones y revisiones que duró 5 años, se publica en el año 2005 la versión final de esta norma que cambia su denominación de ISO/IEC 17799 por ISO/IEC 27002, la seguridad de la información dentro del estándar se define como:

> *"La preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información)"*[101]

Actualmente la norma 27002:2005 está compuesta por 11 dominios, 39 objetivos de control y 133 controles que ayudarán a las distintas organizaciones a generar políticas y procedimientos de gestión de seguridad de la información, los dominios por los que está compuesta esta norma se detallan en la siguiente Tabla 5.2 en la página a continuación:

---

[100] **ISO/IEC Organización Internacional para la Estandarización/Comisión Electrotécnica Internacional,** el objetivo de estas dos organizaciones es proporcionar a los usuarios información acerca de la normalización, las normas y cuestiones conexas. Obtenido en, http://www.standardsinfo.net/info/index.html.

[101] Definición de Seguridad de la Información según la norma ISO/IEC 27002:2005.

#	DOMINIO	CONTROLES	OBJETIVO
1	Política de seguridad	1	Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.
2	Organización de seguridad de la información	2	Manejar la seguridad de la información dentro de la organización estableciendo un marco referencial de gerencia para iniciar y controlar la implementación de la seguridad de la información.
3	Gestión de activos	2	Lograr y mantener una apropiada protección de los activos organizacionales; debiendo ser inventariados y contar con un propietario nombrado.
4	Seguridad de recursos humanos	3	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.
5	Seguridad física y ambiental	2	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.
6	Gestión de la comunicaciones y operaciones	10	Asegurar la operación correcta y segura de los medios de procesamiento de la información.
7	Control de acceso	7	Controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	6	Garantizar que la seguridad sea una parte integral de los sistemas de información.
9	Gestión de un incidente en la seguridad de la información	2	Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.
10	Gestión de la continuidad del negocio	1	Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información.
11	Cumplimiento	3	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

Tabla 5.2: Dominios de la norma ISO/IEC 27002:2005
Autor: Tesista
Fuente: http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

En la tabla anterior se detallaron los dominios de la norma 27002, los cuales tienen que ser aplicados de acuerdo a la situación actual de la organización, por esta razón es que se utilizará este estándar para generar las políticas y procedimientos que se van a utilizar en el diseño del CSIRT de la Corte Constitucional, sin embargo, no se utilizarán todos los dominios, solo se tomará base del dominio 9 que hace referencia a: Gestión de incidentes de seguridad de la información.

5.2.2.1.1 Gestión de incidentes de seguridad de la información

Para el estudio de incidencias que se puedan generar dentro de una organización este dominio se divide a su vez en dos partes que son:

Reporte de los eventos y debilidades de la seguridad de la información

El objetivo de este paso es establecer procedimientos formales de reporte de incidentes y de la solución que se le va a dar a cierto evento. Todos los funcionarios y usuarios que son parte activa de una organización deben estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos de la organización.

- **Reporte de eventos en la seguridad de la información**

Para cumplir con el reporte de eventos sobre los incidentes de seguridad se recomienda seguir con los siguientes procesos:

- Control.
- Lineamiento de implementación.
- Información adicional para el reporte de incidencias.

Los procesos mencionados anteriormente serán explicados en la Tabla 5.3 a continuación:

Procesos	Objetivo	Pasos
Control	Informar cualquier evento que pueda atentar contra la seguridad debe ser reportado de forma rápida al Director de Tecnología	1. Revisar posible brecha de seguridad 2. Informar al Director
Lineamiento de implementación	Establecer un procedimiento de reporte, respuesta y seguimiento sobre los eventos que puedan atentar contra la seguridad de la información.	1. Notificar sobre los resultados obtenidos al atender un incidente 2. Generar formatos de reporte para almacenar la información sobre los eventos de seguridad presentados 3. Capacitación de los funcionarios que han sido responsables de violaciones de seguridad
Otra información	Informar sobre diferentes tipos de incidentes a la seguridad.	Llevar registro de: 1. Pérdida de equipos o servicios de red 2. Violaciones de acceso 3. Mal funcionamiento del sistema 4. Incumplimiento de políticas 5. Violaciones de seguridad física

Tabla 5.3: Procesos para el reporte de eventos
Autor: Tesista
Fuente: http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Para realizar este proceso hay que tener un cuidado especial con la confidencialidad de la información, sin olvidar que los eventos que se presentaron servirán para la capacitación de los funcionarios y que no vuelva a ocurrir.

El mal funcionamiento o cualquier otra conducta anómala del sistema pueden ser un indicador de un ataque a la seguridad o una verdadera violación de la seguridad y, por lo tanto, siempre debiera reportarse como un evento en la gestión de seguridad.

- **Reporte de las debilidades en la seguridad de la información**

Al igual que con el reporte de eventos hay que seguir algunos procesos dentro del reporte de debilidades como pueden ser: control, lineamiento de implementación e información complementaria, esto ayudará a la recopilación de información y a la elaboración de las políticas y procedimientos. Los procesos del reporte de debilidades se muestran a continuación en la Tabla 5.4:

Procesos	Objetivo	Pasos
Control	Controlar que todos los usuarios o funcionarios informen sobre cualquier debilidad observada en los sistemas o servicios.	1. Observar debilidades en sistemas 2. Informar al Departamento de Tecnología
Lineamiento de implementación	Reportar al Director de Tecnología o al proveedor del servicio la debilidad detectada para solucionarlo lo más pronto posible.	1. Reporte de debilidades 2. Investigación de debilidades 3. Informar al Director de Tecnología
Otra información	Advertir tanto a usuarios como a funcionarios de no tratar de probar las debilidades de seguridad detectadas.	1. Crear advertencias de seguridad 2. Informar sobre las debilidades detectadas

Tabla 5.4: Procesos para el reporte de debilidades
Autor: Tesista
Fuente: http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Una debilidad o vulnerabilidad significa que un atacante interno o externo puede utilizar cualquier brecha de seguridad detectada para acceder a servicios o equipos no autorizados, por esta razón es que se pretende generar reportes de debilidades detectadas y poder corregirlas a tiempo antes de que puedan ser explotadas.

La prueba de debilidades ya sea por un funcionario o usuario podría ser interpretada como un mal uso potencial del sistema, por los daños que pueda causar la red o a las aplicaciones y resultar en responsabilidad legal para la persona que haya realizado la prueba.

Gestión de los incidentes y mejoras en la seguridad de la información

Para poder realizar una correcta gestión incidentes según esta norma hay que las debidas responsabilidades y procedimientos para manejar y atender de manera efectiva las debilidades detectadas en la gestión de seguridad de la información.

Para realizar este proceso se debe aplicar un mejoramiento continuo de todo el equipo de tecnología para poder responder, monitorear y evaluar de la mejor manera los incidentes que se presenten, además, poder recolectar y almacenar evidencia que se podrá presentar ante el requerimiento de cualquier funcionario o entidad.

La gestión de los incidentes y mejoras en la seguridad de la información se debe a tres procesos claves que son:

- Responsabilidades y procedimientos
- Aprender de los incidentes en la seguridad de la información
- Recolección de evidencia

A continuación se ampliará la información de cada uno de estos procesos.

- **Responsabilidades y procedimientos**

En este proceso se deben establecer las responsabilidades y procedimientos del Director de Tecnología para asegurar una respuesta rápida, efectiva y metódica ante los posibles incidentes que se podrían presentar.

Los lineamientos de implementación de este proceso además de reportar los eventos en la seguridad, deben también utilizar monitoreos del sistema, generación de alertas y análisis de vulnerabilidades para detectar los incidentes en la seguridad de la información.

Algunos de los lineamientos que se pueden considerar son:

a) Establecer políticas y procedimientos para manejar los diferentes tipos de incidentes detectados.
b) Generar planes de contingencia para responder a los incidentes.
c) Recolectar y asegurar rastros de auditorías generadas y evidencia similar sobre incidentes para poder sacar conclusiones en base a correlación de eventos.
d) Controlar cuidadosamente las acciones para la recuperación de las violaciones de seguridad y para corregir las fallas en el sistema.

Para culminar con el desarrollo de este proceso se debe acordar con el Director de Tecnología[102] las políticas y procedimientos para la gestión de incidentes en la seguridad de la información, además de asegurar que aquellos responsables de la

[102] **Director de Tecnología,** persona responsable de la toma de decisiones y del Departamento de Tecnología de una entidad u organización.

gestión de incidentes en la seguridad de la información entiendan las prioridades de la organización para el manejo de los incidentes.

Para poder responder a los incidentes detectados actualmente se necesita cada vez más coordinar las respuestas y compartir esta información sobre los eventos sucedidos con organizaciones externas que ya las hayan enfrentado.

- **Aprender de los incidentes en la seguridad de la información**

Para realizar este proceso se debe cuantificar y monitorear los tipos de eventos contra la seguridad, su volumen de impacto y el costo que representó a la organización.

Los lineamientos según la norma para poder aprender de los incidentes ocurridos recomiendan que se debe utilizar la información obtenida de la evaluación de los incidentes, para poder identificar cuál de ellos se ha presentado de forma recurrente o que hayan generado un alto impacto para los activos de la organización.

Este tipo de evaluación ayudará al equipo técnico a incrementar o establecer controles adicionales para limitar la frecuencia de eventos, así como también, el daño y costo que puedan representar este tipo de incidencias para la organización en el futuro.

- **Recolección de evidencia**

Para continuar con el último de los procesos se debe generar un control especial sobre la recolección, almacenamiento y presentación de pruebas en caso de ser necesario, sobre todo, si esta evidencia encontrada hace responsable a una organización o persona después de ser detectado un incidente contra la seguridad de la información, ya que esta involucra una acción legal.

Generalmente para poder recurrir a la implementación de este proceso se debe seguir los procedimientos internos que maneja la organización cuando se

recolecta y se presenta evidencia con propósitos de una acción disciplinaria contra un funcionario.

En general, las reglas de evidencia que recomienda la norma debieran abarcar:

a) **Admisibilidad de evidencia,** esto quiere decir que la organización debe asegurar que sus activos tecnológicos cumplan con los estándares publicados para la recolección de evidencia admisible, esto podría darse ya sea por la instalación de hardware o software especializado para desarrollar esta función.

b) **Peso de la evidencia,** con esto se debe demostrar mediante una auditoría la calidad e integridad de los controles utilizados para proteger correctamente la evidencia encontrada, esto habrá que realizar durante todo el período en que la información fue recuperada, almacenada y procesada.

También se recomienda realizar copias del material de evidencia, para proteger la integridad del material; el copiado del material debe ser supervisado por personal confiable y se debe registrar la información sobre cuándo y dónde se realizó el proceso de copiado, además de, obtener información de la persona que realizó el copiado y cuáles fueron los programas o herramientas que se utilizaron.

Por último habrá que tomar en cuenta que cuando se detecta un evento en la seguridad de la información, puede no ser obvio si el evento resultará, o no, en una acción legal dentro de la organización, por esta razón, existe el peligro de destruir la evidencia de forma involuntaria o accidentalmente antes de percatarse de la seriedad del incidente. Para poder solucionar esta eventualidad es aconsejable asesorarse de forma legal con un abogado desde que se presente la sospecha de un incidente de seguridad.

5.2.3 Definición de Políticas y Procedimientos

Las políticas y procedimientos para el diseño del CSIRT de la Corte Constitucional estarán acorde a la norma ISO/IEC 27002 dominio 9 sobre la gestión de incidentes para la seguridad de la información y serán detalladas a continuación.

5.2.3.1 Reporte de eventos en la seguridad de la información

Política: Todo incidente o vulnerabilidad detectada deberá ser reportada al equipo de respuesta CSIRT, para que éste a su vez pueda responder y realizar un seguimiento del evento, proporcionando una acción ágil y oportuna para todos los funcionarios de la Corte Constitucional.

Procedimientos: Notificar a los funcionarios de la Corte sobre lo eventos atendidos y solucionados para asegurar que las personas que reportan un evento se encuentren informados de que el equipo se encuentra trabajando constantemente.

Realizar un formulario de reporte de incidentes para poder respaldar la acción de reporte notificada, y ayudar a la persona que realiza el reporte a recordar toda la información que proporcionó en el momento exacto. Para generar un formulario de reporte de incidentes existen algunos puntos a tomar en cuenta que son:

- **Anotar detalles relevantes,** se debe tener espacio para tomar nota de información como: tipo de violación generada, mal funcionamiento de las aplicaciones, mensajes en pantalla o conducta extraña.
- **El tipo de actividad a reportar,** en el informe se debe incluir los tipos de incidentes que los usuarios pueden reportar, como: Acceso no autorizado a los sistemas, el uso no autorizado de las aplicaciones, cambios en el hardware o software, entre otros.
- **La prioridad que se da a los incidentes,** cuando se incrementa el número de reportes de incidentes, en este caso se requiere dar prioridad a los más urgentes, los reportes que pueden ser considerados como emergencias

pueden ser: ataques a la red, a los servidores, puntos de acceso de red, ataques al sitio web de la Corte.

Es importante realizar un informe sobre los reportes de incidentes y vulnerabilidades generados, porque de esa manera se podría recibir ayuda técnicas por parte de otros CSIRTs, además, es importante tomar en cuenta que la relación con otros CSIRTs puede ser de dos formas, ya sea trabajando de manera conjunta así como también compartiendo información, o simplemente manteniendo un contacto continuo que brinde asesoría o información.

5.2.3.2 Reporte de debilidades en la seguridad

Política: Toda debilidad detectada en la instalación, configuración o en el momento de ejecución de cualquier componente de tecnología o aplicativo deberá ser reportada al equipo de respuesta CSIRT, para que éste a su vez pueda encontrar una solución rápida o en caso de requerirlo, tratarlo directamente con el proveedor de la solución.

Procedimientos: Los funcionarios o los miembros del Departamento de Tecnología de la Corte deberán comunicar al equipo de respuesta CSIRT sobre cualquier debilidad observada o sospechada tanto en los activos de tecnología como en los aplicativos instalados.

Utilizar el formulario de reporte de incidentes para poder respaldar la acción de debilidad notificada.

Capacitar a los funcionarios sobre los riesgos que pueden encontrar en internet, como por ejemplo: abrir correo electrónico de remitentes desconocidos, links[103] dentro de correo electrónico que podría ser para descarga de virus, abrir correo basura, ingresar a páginas restringidas, entre otras; una o varias de estas acciones de los usuarios podrían debilitar la seguridad de los activos de la Corte Constitucional.

[103] **Link o hiperenlace,** es la palabra que hace referencia a un documento de hipertexto o recurso que por lo general necesitará conectarse a internet para poder ser visto. Obtenido en, http://es.wikipedia.org/wiki/Link.

Advertir a los funcionarios de no tratar de explotar ninguna debilidad detectada por el equipo de respuesta CSIRT, ya que una acción de estas podría incurrir en acciones legales contra la persona responsable.

5.2.3.3 Responsables y procedimientos para la gestión de incidentes

Política: El Director del Equipo de Respuesta CSIRT deberá generar las responsabilidades tanto para el Jefe del Equipo como para los técnicos e investigadores, que serán los responsables de tomar acciones si se presenta un atentado contra la seguridad de la información.

Procedimientos: Todos los miembros del equipo de respuesta CSIRT deberán coordinar sus acciones para poder atender los diferentes tipos de incidentes que se puedan presentar, como por ejemplo:

- Detección de código malicioso
- Denegación de servicio
- Violaciones de confidencialidad e integridad de información
- Mal uso de las aplicaciones instaladas para los usuarios
- Fallas de la red o de las aplicaciones

Se deberán generar planes de contingencia que garanticen la continuidad del negocio en caso de desastres, así como también procurar una alta disponibilidad de servicios para los funcionarios; este tipo de análisis también podría incluir:

- Análisis e identificación sobre la causa de un incidente
- Planeación sobre las acciones correctivas a tomar para evitar que vuelva a ocurrir
- Comunicar sobre la recuperación de un incidente a los funcionarios afectados
- Reportar las acciones tomadas al Director del CSIRT

El equipo deberá almacenar toda la evidencia necesaria sobre los incidentes de seguridad detectados, ya que podrían ser requeridos en cualquier momento por alguna autoridad o auditoría al Departamento de Tecnología.

El proceso de recuperación ante un incidente deberá asegurar que solo el personal involucrado tenga acceso a la información y la documentación sobre las acciones realizadas para solucionar la emergencia.

5.2.3.4 Aprendizaje y recolección de evidencia sobre incidentes

Política: Toda la información obtenida sobre los incidentes detectados servirá al equipo de respuesta CSIRT para prevenir que esto vuelva a ocurrir en estaciones de trabajo, red, servidores o aplicativos, disminuyendo de esta forma el costo en infraestructura tecnológica, a su vez, se deberá recolectar toda la evidencia que sea posible cuando se presente un incidente para poder tomar las acciones legales pertinentes si así fuera el caso.

Procedimientos: El CSIRT utilizará la información obtenida de las evaluaciones sobre incidentes para poder generar una correlación de eventos adecuada e identificar posibles ataques futuros, este procedimiento se podría realizar con hardware o software específico para esta labor.

Se deberá mantener un proceso de clasificación de la información así como también de los eventos, tomando en cuenta el tipo de información que maneja la Corte Constitucional esta se podría dividir en:

- Información Privada, hace referencia a la documentación que deberá ser tratada de forma sensible por los miembros del CSIRT y mostrar los informes al Director del Equipo de forma privada y con el debido cuidado.
- Información Pública, este tipo de documentación se podrá mostrar a los usuarios y funcionarios sin restricción alguna, como evidencia del trabajo, atención y solución de eventos que atiende el CSIRT de la Corte Constitucional.

5.2.4 Personas

Este elemento representa los recursos humanos y los problemas de seguridad que los rodean, para poder definir este proceso se deberá establecer y comunicar la

misión y Visión del CSIRT a todas las personas que van a ser beneficiadas por el equipo.

Misión

Brindar seguridad proactiva a los equipos y aplicaciones en base a investigación continua, con el fin de precautelar los servicios de los usuarios y funcionarios de la Corte Constitucional.

Visión

Ser el punto de partida para que en un futuro se puedan implementar más equipos CSIRTs en las entidades públicas, logrando de esta forma, aumentar la difusión de información entre equipos y disminuir los riesgos de los posibles ataques.

Comunicar a todos los usuarios y funcionarios de la Corte Constitucional sobre los objetivos, misión y visión del equipo CSIRT ayudará para que se sientan respaldados en todo momento y sobre todo para que estén al tanto de las funciones y beneficios que dará a la institución.

Comunidad

La comunidad hace referencia al grupo de personas que va a brindar los servicios el equipo CSIRT dentro de la Corte, que para este caso, será de forma principal a los funcionarios de la entidad con las respectivas capacitaciones de seguridad, la recepción de reportes y las respuestas inmediatas que se puedan dar a los incidentes comunicados; y de forma secundaria pero no menos importante a los usuarios, que se verán beneficiados de este proceso al estar conscientes de la seguridad con la que se manipula la información internamente.

5.2.5 Tecnología

La tecnología se compone de todas las herramientas, las aplicaciones y la infraestructura que pueden hacer más eficientes a los procesos. Debido a que actualmente las empresas dependen de la tecnología, ésta constituye una parte

fundamental de su infraestructura y un componente crítico en el cumplimiento de su misión.

Generalmente la tecnología se ve a menudo como una manera de resolver las amenazas de seguridad y los riesgos, sin embargo, la tecnología tiene que ir de la mano con los controles técnicos, que serán útiles para mitigar algunos tipos de riesgos, la tecnología no debe ser vista como un sistema de información de soluciones de seguridad, sino como una herramienta para solucionar problemas de seguridad.

Por estas razones es que el equipo de seguridad CSIRT se encargará de los controles técnicos, y la tecnología se encargará de ayudar a disminuir los riesgos de seguridad. Debido a que siempre se necesitará de tecnología para complementar los procesos de cuidado de la información y con respecto al análisis de vulnerabilidades del Capítulo 3, la Corte Constitucional ha visto la necesidad de implementar un equipo UTM[104] a su infraestructura actual para mejorar los niveles de servicio.

De acuerdo con su “Proyecto de fortalecimiento de infraestructura Corte Constitucional 2012” y de su “POA”, el Departamento de Tecnología posee un presupuesto para mejorar la tecnología de seguridad de la información, que ha sido destinado para la compra de este equipo de Gestión Unificada de Amenazas.

UTM

Este gestor unificado de amenazas es un equipo de propósito dedicado que funciona como un firewall de red con múltiples funciones añadidas, trabajando a nivel de la capa aplicación. Este equipo tiene la capacidad de realizar el estudio del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo.

[104] **UTM (Unified Threat Management) o Gestión Unificada de Amenazas,** se utiliza para describir los cortafuegos de red que engloban múltiples funcionalidades en un mismo equipo. Obtenido en, http://es.wikipedia.org/wiki/Unified_Threat_Management.

Existen dos modos de configuración del equipo dentro de la red, eso sí, dependiendo de su capacidad operativa y de la marca, la configuración puede ser:

- **Modo proxy:** quiere decir que hace uso de proxies para poder procesar y redirigir todo el tráfico interno.
- **Modo Transparente:** que no redirigen ningún paquete que pase por el dispositivo, simplemente lo procesan y son capaces de analizar en tiempo real todos los paquetes. La desventaja de esta configuración es que requiere de unas altas prestaciones hardware.

Algunas de las funcionalidades que puede incluir este equipo dependiendo del modelo y del fabricante son las siguientes:

- **Antivirus.-** con base de datos de virus propia del fabricante.
- **Creación de VPN[105].-** para conexiones remotas.
- **Antispam.-** para evitar el correo basura.
- **Antiphishing[106].-** pera evitar la duplicación de páginas web.
- **Antispyware.-** detectar software malicioso.
- **Filtro de contenidos.-** restringir la visita de páginas web.
- **Control de aplicaciones.-** restringir el uso de programas en horas laborales.
- **Detección/Prevención de Intrusos (IDS/IPS).-** para detectar métodos de intrusión a la red.
- **Control de ancho de banda.-** para poder dar prioridad a ciertas aplicaciones.

De acuerdo a las características del dispositivo UTM, se generó un documento para comunicar los servicios que brindará el equipo de seguridad tanto a los funcionarios de la Corte Constitucional como al Departamento de Tecnología, Anexo F.

---

[105] **VPN (Virtual Private Network) o red privada virtual,** es una tecnología de red que permite una extensión de la red local sobre una red pública. Obtenido en, http://es.wikipedia.org/wiki/Red_privada_virtual.

[106] **Phishing,** es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas. Obtenido en, http://es.wikipedia.org/wiki/Phishing.

Para realizar el proceso de escoger el proveedor adecuado para la adquisición de esta solución se analizó el cuadro mágico de Gartner[107], y así, tener una perspectiva sobre cuál es la empresa mejor posicionada en la fabricación de este tipo de soluciones, como muestra la Figura 5.4 a continuación:

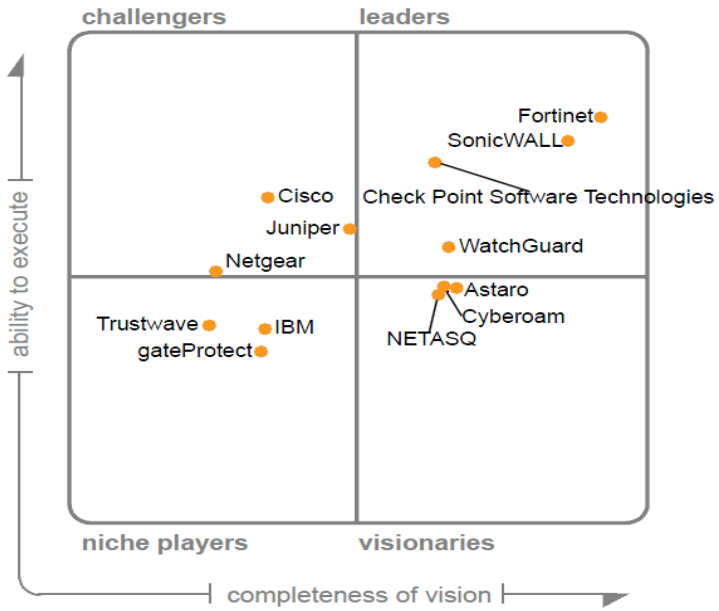


Figura 5.6: Posicionamiento de proveedores UTM según Gartner
Autor: Tesista
Fuente: UTM-Report_Gartner_2010.pdf

De todas las empresas que constan en el cuadro de Gartner, se escogió a cuatro que tienen representación en Ecuador y que el Departamento de Tecnología ya ha trabajado con ellas, y son:

- Astaro, como visionario de la solución
- Cisco, como actual competidor y por la compatibilidad de infraestructura.
- Check Point Software Tecnologies, como uno de los fabricantes líderes.
- Fortinet, al igual que la empresa anterior como parte de los líderes.

A continuación se detallará en rasgos generales las características de los equipos de cada uno de los fabricantes.

[107] **Gartner,** es una empresa muy prestigiosa consultora y de investigación de las tecnologías de la información. Obtenido en, www.gartner.com.

- **Astaro**

De este fabricante se escogió el modelo Astaro Security Gateway 425 que consta de los siguientes servicios dentro de la aplicación:

Astaro Network Security: firewall, prevención de intrusos, protección DoS, control de ancho de banda, VPN para Sucursales, acceso remoto SSL, acceso remoto IPSec, acceso remoto para Windows nativo, autenticación de directorio, seguridad de red, acceso remoto, registro / reporte, administración.

Astaro Web Security: filtrado URL, escaneo antivirus, reportes de usuario, anti spam, anti phishing.

Web Application Security: protege servidores de aplicaciones publicados en la web contra ataques avanzados como inyecciones SQL y Cross Site Scripting (XSS).

Y las características técnicas de dispositivos se muestran en la Tabla 5.5:

Descripción	Capacidad
Número máximo de licencias	Ilimitado
Número máximo de usuarios recomendado	600
Rendimiento del firewall	6 Gbps
Rendimiento IPS	2000 Mbps
Rendimiento de la VPN	780 Mbps
Rendimiento de UTM	300 Mbps
Rendimiento de red	160 Mbps
Rendimiento correo electrónico	1.200.000 correos/hora
Conexiones simultáneas	1.000.000
Unidad de almacenamiento	160 Gb

Tabla 5.5: Características técnicas UTM Astaro 425
Autor: Tesista
Fuente: https://www.astaro.com/node/18319

- **Cisco**

La serie Cisco ASA 5550 Adaptive Security Appliance ofrece servicios de seguridad de alta disponibilidad de tipo “activo / activo” o “activo / pasivo”, fibra y conectividad Gigabit Ethernet.

Este dispositivo también ofrece una muy alta disponibilidad y compatibilidad con toda la infraestructura existente en la Corte Constitucional y sus características técnicas se muestran a continuación en la siguiente Tabla 5.6:

Descripción	Capacidad
Número máximo de licencias	Ilimitado
Número máximo de usuarios recomendado	500
Rendimiento del firewall	1,2 Gbps
Rendimiento IPS	1000 Mbps
Rendimiento de la VPN	425 Mbps
Rendimiento de UTM	800 Mbps
Conexiones simultáneas	650.000
Unidad de almacenamiento	4 Gb

Tabla 5.6: Características técnicas Cisco ASA 5550
Autor: Tesista
Fuente: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet.html

- **Check Point**

El dispositivo Check Point ofrece una seguridad de tipo, todo en uno, con su modelo UTM-1 Series 3078, es una solución de gestión unificada de amenazas que incluyen todo lo necesario para asegurar la red. Este dispositivo incluye una gestión centralizada integrada, junto con las actualizaciones de seguridad completas, hardware y soporte al cliente.

Sus características técnicas a continuación en la Tabla 5.7:

Descripción	Capacidad
Número máximo de licencias	Ilimitado
Número máximo de usuarios recomendado	650
Rendimiento del firewall	4,5 Gbps
Rendimiento IPS	4 Gbps
Rendimiento de la VPN	1100 Mbps
Rendimiento de UTM	800 Mbps
Conexiones simultáneas	1.100.000
Unidad de almacenamiento	160 Gb

Tabla 5.7: Características técnicas UTM-1 Series 3078
Autor: Tesista
Fuente: http://www.checkpoint.com/products/utm-1-appliances/index.html

- **Fortinet**

El FortiGate-311B se encuentra dentro de la serie de dispositivos de seguridad consolidados para ofrecer seguridad integrada a una alta velocidad de procesamiento de información. Este equipo cuenta con ranuras de expansión modular que proporcionan un rendimiento adicional o aumento de almacenamiento en disco. Sus características técnicas son las siguientes según la Tabla 5.8:

Descripción	Capacidad
Número máximo de licencias	Ilimitado
Número máximo de usuarios recomendado	600
Rendimiento del firewall	8 Gbps
Rendimiento IPS	800 Mbps
Rendimiento de la VPN	6 Gbps
Rendimiento de UTM	400 Mbps
Conexiones simultáneas	600.000
Unidad de almacenamiento	64 Gb

Tabla 5.8: Características técnicas Fortigate-311B
Autor: Tesista
Fuente: http://www.fortinet.com/products/fortigate/310B.html

Luego de haber analizado cada uno de los modelos de equipo UTM con sus respectivas características, cabe mencionar que, sin importar cual sea el fabricante de la solución requerida las ventajas y desventajas que se puede encontrar al adquirir este tipo de equipos son:

Ventajas:

- Se pueden sustituir varios sistemas independientes por uno solo facilitando su administración.
- Es posible añadir módulos de análisis dependiendo del modelo para extender sus servicios.
- Poseer un mejor control sobre la utilización de aplicaciones y servicios sobre la red.
- Distribución de ancho de banda.
- Se puede generar reportes ejecutivos para análisis de incidencias.

Desventajas:

- Se crea un punto único de fallo y un cuello de botella, es decir si falla este sistema la organización queda desprotegida totalmente.
- Tiene un coste fijo periódico debido a la actualización de licencias.

Para cubrir con las desventajas antes mencionadas, el Departamento de tecnología ha visto necesario el adquirir dos equipos UTM de las mismas características, generando así, una redundancia entre equipos, de esta forma si llegara a quedar sin servicio uno de ellos, el otro se activaría para no dejar sin protección a la red de la Corte Constitucional; y con respecto al valor de actualización de licencias, según los requerimientos de adquisición, la oferta del equipo por parte de la empresa fabricante debe contemplar el costo de renovación de licencias por un mínimo de 3 años.

Para poder crear un margen de calificación de los proveedores, se generó un formato sobre las “Bases Técnicas” requeridas como mínimas para la adquisición del equipo, Anexo G, y estas se las publica en el Sistema Nacional de Compras Públicas para que las empresas ofertantes puedan comparar sus equipos con los requerimientos de la Corte Constitucional y las que no pudieran cumplir con estas características mínimas serían descalificadas del proceso por parte de la entidad o no ingresarían al mismo de forma voluntaria.

Luego de haber presentado estos requerimientos por medio de las Bases Técnicas habrá que tomar en cuenta que el Departamento de Tecnología posee un presupuesto máximo de $70.000 dólares para la compra de este dispositivo, por estas razones, marcas fabricantes como Cisco y Check Point no pudieron entrar al proceso de presentación de su oferta formal, ya que sus equipos sobrepasaban el presupuesto fijado, y la marca Astaro no presentó su propuesta por no cumplir con los requerimientos mínimos de las Bases Técnicas generadas.

Debido a esto, el único fabricante que restaba era Fortinet con su equipo Fortigate-311B, marca representada oficialmente en el Ecuador por dos empresas que son: Work Computer y Evolutionet, las cuales sí presentaron su propuesta

para la venta del equipo UTM a la Corte Constitucional. Luego de ser analizadas las dos propuestas por el Departamento Jurídico y Financiero de la institución, se detectó que la empresa Evolutionet tenía su RUC[108] deshabilitado, razón por la cual esta empresa fue descalificada del proceso, resultando como ganadora la empresa Work Computer.

Con la adquisición de este equipo se ha concluido con el presente trabajo e investigación de tesis, siendo esta compra, el primer paso para combatir con las vulnerabilidades e incidencias detectadas en el Capítulo 3, ya que este UTM se considerada como la principal herramienta para mejorar la seguridad de la información que pasa a través de la red de la Corte Constitucional actualmente, luego y como segundo paso se ha dejado diseñado un modelo de gestión de seguridad en base a la creación de un equipo CSIRT, que podría ayudar a generar y controlar procesos contra posibles ataques a la red. Anexo H resumen ejecutivo del diseño.

[108] **RUC o Registro Único de Contribuyente,** es un registro que identifica a las empresas dentro del país en cuestión y que se necesita de forma obligatoria para comenzar con sus operaciones financieras. Obtenido en, http://es.wikipedia.org/wiki/RUC.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

En referencia al estudio de riesgos sobre los bienes tecnológicos de la Corte se logró definir qué: una vulnerabilidad es una incidencia que se puede encontrar en los activos o servicios de una entidad, y que puede ser explotada tanto por un funcionario de la misma como por un agente externo, por esta razón es que, la labor del Departamento de Tecnología es cuidar de que la seguridad de la información sea lo más efectiva posible, creando métodos, políticas o grupos de personas que ayuden a cumplir con este objetivo.

De los intentos de ataque realizados a las direcciones IP seleccionadas de los servicios institucionales se pudo concluir que de acuerdo al Libro Naranja los sistemas actualmente cuentan con una seguridad de tipo “C-Protección discrecional” que deberá ser incrementada, ya que dependiendo desde donde se genere el ataque, es decir, si éste se procesa con la ayuda de sistemas operativos convencionales, la probabilidad de éxito es casi nula, pero, si se utilizan herramientas especializadas como las que contiene BackTrack se pueden obtener resultados favorables debido a sus aplicaciones de propósito específico.

El propósito del análisis de la red de datos fue dejar al descubierto todas las brechas de seguridad posibles que se puedan encontrar en los servidores de la entidad como: puertos abiertos, claves débiles, conexiones remotas no autorizadas o falta de actualización en los sistemas operativos, que son las formas que utilizaría cualquier intruso para explotar una debilidad, y además, dejar en claro que así como se encontró y se manipuló vulnerabilidades, los demás equipos que no fueron parte de este estudio también podrían tener alguna debilidad de configuración o actualización que pueda ser explotada.

Un riesgo en las TI es el resultado de, detectar una vulnerabilidad, más explotar una amenaza, eso quiere decir que si un servidor se encuentra desactualizado, existirá una herramienta que pueda sacar provecho de esto y proporcionar acceso a la configuración del mismo, en conclusión una correcta manipulación de la

gestión de riesgos ayudará a anticipar la vulnerabilidad y mitigar la amenaza, mas no a solucionarla, ya que se debe tener presente que los riesgos evolucionan con la tecnología.

Este tipo de estudio sobre las vulnerabilidades e incidencias que se pueden presentar dentro de la infraestructura de la Corte Constitucional es sumamente importante debido al tipo de información que se maneja diariamente, por esta razón, es que se debería contar con un departamento o un equipo de personas que se dediquen de tiempo completo de verificar la seguridad de toda la red de datos de la entidad, y se alineen con el objetivo del negocio que es precautelar la información judicial.

El CSIRT es un grupo de personas que se dedicarán a atender y llevar una estadística sobre los incidentes de seguridad que se puedan presentar, generando de esta manera políticas y procedimientos para poder reaccionar en caso de que se reporte un ataque, sin dejar de lado la capacitación tanto de los miembros del equipo como la de los funcionarios que van a ser beneficiados por los servicios del equipo, y la constante investigación harán de este nuevo modelo de seguridad un método para reducir la posibilidad de ser víctima de una violación a la seguridad de la información.

El diseño del CSIRT de la Corte Constitucional deja como resultado una propuesta sobre la organización, distribución, procesos y procedimientos que se podrían seguir para gestionar los incidentes de seguridad dentro de la entidad, que fueron creados con la ayuda de la norma ISO 27002, con la intención no solo de atender a los posibles ataques, sino más bien dedicado a crear una cultura de seguridad en los funcionarios, ya que para una protección externa existen muchas herramientas, pero para proteger internamente una organización el punto principal es precautelar la conciencia sobre los actos de las personas, que podrían poner en peligro los procesos, bienes y servicios de la institución.

RECOMENDACIONES

Contratar un enlace de datos para la Corel Constitucional, adicional al que se tiene actualmente con la empresa CNT, para que sirva como respaldo y que pueda generar redundancia en caso de presentarse un fallo del proveedor actual, pero principalmente, para incrementar el nivel de disponibilidad operativa asegurando su conectividad.

Realizar un análisis de vulnerabilidades a todos los servidores que sean parte de la entidad, así como también, el escaneo de sus puertos, con el fin de detectar y anticipar cualquier tipo de inconveniente futuro o incidencia que pudiera ser explotada por terceros, generando desde ya una protección proactiva de los bienes de la institución.

Con respecto a las intrusiones ejecutadas, se recomienda configurar las páginas de administración de aplicaciones sensibles con un método que pueda restringir el ingreso de claves, de acuerdo a un número máximo de intentos de validación, es decir, que un usuario pueda errar el ingreso de la contraseña tres veces como máximo, además de implementar políticas de contraseñas basadas en el Libro Naranja de Seguridad o en cualquier otra metodología con el fin de mantener claves seguras que garanticen la confidencialidad, disponibilidad e integridad de la información.

A su vez, también se debe implementar claves de seguridad a todas las impresoras de la entidad de acuerdo a una metodología específica o los parámetros que especifica el libro Naranja de Seguridad, ya que si se llega a cambiar alguna de las claves, la única solución sería cambiar el dispositivo de red de la impresora representando un costo relativamente bajo si es que se afecta un solo dispositivo, pero si un intruso llega a cambiar la configuración de más de una impresora el costo podría ascender considerablemente.

Motivar la implementación de un equipo de respuesta ante incidentes de seguridad CSIRT dentro de la Corte Constitucional, con el objetivo de independizar la seguridad tanto de los bienes como de los servicios que ofrece la institución al

público en general, esto se logra debido a que el CSIRT se encargará de promover la investigación continua de posibles vulnerabilidades en la infraestructura tecnológica y de tomar las acciones proactivas pertinentes para dar solución a las debilidades detectadas.

Contactar con equipos CSIRT que ya hayan sido implementados, ya sea a nivel nacional como internacional, para conocer de forma directa sobre los beneficios recibidos con la puesta en marcha de este tipo de proyectos, de cierta forma sería de mayor utilidad que el equipo contactado represente a una entidad pública o a su vez un CSIRT implementado a nivel nacional, tomando en cuenta el objetivo de negocio de la Corte Constitucional.

En caso de no implementar el CSIRT, se recomienda una capacitación continua a los usuarios, ya que son los que están expuestos día a día con las diferentes amenazas que se encuentran al exterior como al interior de la red, mencionar cosas como: revisión de virus antes de acceder a la información de un dispositivo usb, no abrir correos de remitentes desconocidos, publicidad engañosa en internet, descarga de programas sospechosos o ingreso a páginas que pondrían en peligro el desempeño del computador.

Por último y debido a todo el proceso de investigación realizado en este trabajo de tesis, se recomienda al Departamento de Tecnología adquirir un dispositivo UTM con el objetivo de disminuir los posibles problemas de seguridad que puedan presentarse y ayudar con la seguridad de la información de la intitución, este es un equipo dedicado a la gestión de amenazas sobre la red, que debe ser muy bien analizado, ya que podría convertirse en un cuello de botella para toda la información que pasará a través de este debido a sus múltiples opciones de configuración y de los servicios que presta, como por ejemplo: firewall, antivirus, antispam, filtro de contenido, detección y prevención de intrusos, entre otras características.

GLOSARIO

ADSL: Línea de Subscripción Asimétrica Digital. Tecnología que mejora el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16 Mbps gracias a una serie de métodos de compresión.

Ancho de Banda: Bandwidth en inglés. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información.

Backbone: La parte de la red que transporta el tráfico más denso: conecta LANs, ya sea dentro de un edificio o a través de una ciudad o región.

Base de datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente.

Bps: Bits por Segundo. Velocidad a la que se transmiten los bits en un medio de comunicación.

Browser: Aplicación para visualizar todo tipo de información y navegar por el internet con funcionalidades plenamente multimedia.

Cableado: Columna vertebral de una red la cual utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), de forma que la información se transmite de un nodo a otro.

Código fuente: Conjunto de instrucciones que componen un programa, escrito en cualquier lenguaje.

Conexión Remota: Operación realizada en una computadora remota a través de una red de computadoras, como si se tratase de una conexión local.

CSIRT: Computer Security Incident Response Team, es un equipo de respuesta ante incidentes de seguridad computacional, que provee servicios de investigación y mitigación de vulnerabilidades.

Data center: Lugar para colocar grandes cantidades de servidores y equipos de comunicación; tiene todas las facilidades de ancho de banda, seguridad física, aire acondicionado 24 horas.

Debian: Es una distribución de Linux que está totalmente compuesta de software gratuito y open source.

DHCP: Siglas del inglés "Dynamic Host Configuration Protocol." Protocolo Dinámico de Configuración del Host. Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP.

DNS: Servidor de Nombres de Dominio. Servidor automatizado utilizado en el internet cuya tares es convertir nombres fáciles de entender a direcciones numéricas de IP.

Dominio: Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario.

DoS: Denial Of Service (DoS), denegación de servicio, incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar.

Encriptación: Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos.

Ethernet: Tipo de red de área local y tiene un ancho de banda de 10 Mbps, por lo tanto tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

Firewall: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad.

Firma digital: Información cifrada que identifica al autor de un documento electrónico y autentica su identidad.

Gigabit: No debe ser confundido con Gigabyte. Un gigabit es igual a 10^9 (1,000,000,000) bits, que equivalen a 125 megabytes decimales.

Hacking ético: Hacking ético es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas.

HTTP: En inglés Hypertext Transfer Protocol. Protocolo de Transferencia de Hipertexto. HTTP es un protocolo con la ligereza y velocidad necesaria para distribuir y manejar sistemas de información hipermedia.

ISO: International Standards Organization es una red de institutos nacionales de estándares constituido por 157 países. Es el desarrollador y publicador de Estándares Internacionales más grande del mundo.

IT: Del inglés Information Technology (Tecnología de Información). Término muy general que se refiere al campo entero de la tecnología informática, que incluye hardware de computadoras y programación hasta administración de redes.

Kbps: Kilobits por segundo. Unidad de medida que comúnmente se usa para medir la velocidad de transmisión por una línea de telecomunicación.

LAN: Local Area Network. Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, y un enlace encargado de distribuir las comunicaciones.

Linux: Es una versión de libre distribución del sistema operativo basada en UNIX.

MD5: En criptografía, MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

Mitigación: Moderación o disminución de una cosa que es rigurosa o grave y se hace más suave o más soportable

MySQL: My SQL es uno de los Sistemas Gestores de Bases de Datos. Su ingeniosa arquitectura lo hace extremadamente rápido y fácil de personalizar.

Open source: Código fuente abierto o software libre, se refiere a un programa cuyo código fuente está disponible al público general, gratis, para usar y modificar.

POA: Un plan operativo anual es un documento en el cual los responsables de una organización establecen los objetivos que desean cumplir y estipulan los pasos a seguir.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes.

Proxy: Servidor encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red.

Puerto: Número que aparece tras un nombre de dominio en una URL. Canal de entrada/salida de una computadora.

QoS: Quality of Service - (Calidad de Servicio) Nivel de prestaciones de una red, basado en parámetros tales como velocidad de transmisión, nivel de retardo, rendimiento, horario, ratio de pérdida de paquetes.

Rack: Es un armario que ayuda a tener organizado todo el sistema informático de una empresa. Posee unos soportes para conectar los equipos con una separación estándar de 19".

RAID: Array Independent Disk. RAID es un método de combinación de varios discos duros para formar una única unidad lógica en la que se almacenan los datos de forma redundante.

SAN: Del inglés Storage area network, Red de área de almacenamiento. Es una red dedicada que proporciona acceso consolidado al almacenamiento de data en bloques.

Seguridad de la información: Son todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma.

Sendmail: Programa servidor de emails utilizado comúnmente en UNIX, FreeBSD y Linux, entre otros.

Servidor: Es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

Squid: Servidor caché / proxy de alta capacidad y rendimiento de código fuente abierto, muy usado en servidores Linux.

SSH: Secure Shell (SSH) es un protocolo de red seguro para la comunicación de data, que permite la conexión de dos computadoras, usualmente una de ellas es un servidor Unix o Linux.

TCP/IP: El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). En español es Protocolo de Control de Transmisión y Protocolo de Internet.

Telnet: Servicio de internet con el cual un usuario se puede conectar de forma remota a otra computadora, como si se hiciera desde un terminal local, usualmente por el puerto 23.

Virtualización: Es la creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

Vulnerabilidad: Hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

WLAN: Acrónimo en inglés para Wireless Local Area Network. Red inalámbrica de área local permite que un usuario móvil pueda conectarse a una red de área local (LAN) por medio de una conexión inalámbrica de radio.

REFERENCIAS BIBLIOGRÁFICAS

[1] Página web oficial Corte Constitucional
http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=1&Itemid=22

[2] Competencias de la Corte Constitucional
http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=352%3Aicuales-son-las-competencias-de-la-corte-constitucional&catid=31&Itemid=22

[3] Centro de estudios y difusión del derecho Constitucional
http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=67&Itemid=18

[4] Estructura Orgánica y Por Procesos de la Corte Constitucional
De:http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=54&Itemid=27

[5] Proceso de Tecnología e Informática
Libro de Estructura por Procesos de la Corte Constitucional, Propio del Departamento de Tecnología. Página: 357

[6] Problemática de la Corte Constitucional
Proyecto de “Fortalecimiento de Infraestructura y Equipamiento de la Corte Constitucional”
Departamento de Tecnología. Año 2012. Página: 5

[7] Constitución de la República del Ecuador
Suplemento Registro Oficial N° 87
Del lunes 14 de Diciembre del 2009
Tecnología de la Información, Pág. 48

[7] Subsecretaría de Informática
Estrategia para la Administración Pública
Disponible en: http://www.informatica.gob.ec/index.php/inicio/subsecretaria/base-legal

[8] Recomendaciones para Seguridad de Información Digital Gubernamental
Subsecretaría de Informática
Disponible en, http://www.informatica.gob.ec/files/SIRecSegInfGub.pdf

[9] Políticas de establecimiento de contraseñas de seguridad
Libro Naranja
Disponible en, http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[10] Cómo Crear un CSRIT paso a paso
Libro de Enisa
Disponible en, http://enisa.europa.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA-ES.pdf /

[11] A Process for Getting Started
Creating a Computer Security Incident Response Team
Disponible en, http://www.cert.org/csirts/Creating-A-CSIRT.html

[12] Gestión de Incidentes
ArCERT
Disponible en, http://www.arcert.gov.ar/ncursos/material/Gestion_de_incidentes _parte1_ vf.pdf

[13] Dominio 9 sobre la Gestión de Incidentes de seguridad
Norma ISO/IEC 27002:2005
Disponible en, http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

[14] Establecimiento de un Equipo de Respuesta a Emergencias Informáticas
CERT, “Darpa Establishes Computer Emergency Response”
Disponible en, http://www.cert.org/about/1988press-rel.html

[15] Un modelo de seguridad para redes empresariales
CISCO SAFE
Disponible en, www.etmk.cl/in72j/papers/safe_wp_es.pdf

[16] Control de la Seguridad de los Sistemas de la información
ISACA, Information Systems Audit and Control Association
Disponible en, www.isaca.org

[17] Modelo de negocio para Seguridad de la Información
Business Model Information Security (BMIS)
Disponible en, www.isaca.org/Knowledge-Center/BMIS/Pages/Business-model-for-Information-Security.aspx

[18] Cuadro mágico sobre las tecnologías y seguridades de la información
Gartner
Disponible en, www.gartner.com/gartner_report_2010.pdf

[19] Búsqueda información relevante
Wikipedia - Repositorio
Disponible en, http://es.wikipedia.org/wiki/Repositorio

ANEXOS

ANEXO A

ARQUITECTURA SAFE DE CISCO

La arquitectura SAFE de Cisco, es una arquitectura modular, que divide a la red corporativa en bloques, cada uno de los cuales representan un área funcional dentro de la red institucional. Esta división permite realizar un estudio de cada área funcional de una manera más detallada, dando la posibilidad de abarcar cada uno de los aspectos concernientes a una red corporativa.

Esta arquitectura se divide básicamente en dos niveles, el primer nivel corresponde a una vista general de la red corporativa y está representada por los siguientes módulos generales: Campus Empresarial, Borde Empresarial y Borde de los Proveedores de Servicio de Internet.

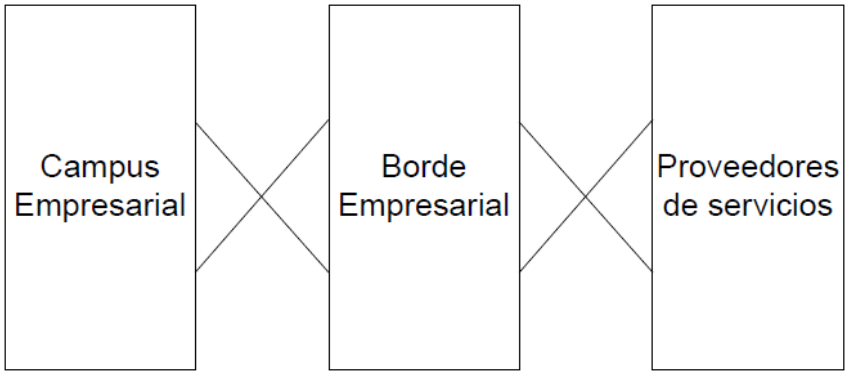


Figura A.1: Arquitectura SAFE de Cisco
Autor: yo
Fuente: www.etmk.cl/in72j/papers/safe_wp_es.pdf

El segundo nivel de esta arquitectura, representa una vista de los módulos con cada área funcional, estos módulos realizan roles específicos dentro de la red y tienen requerimientos específicos de seguridad.

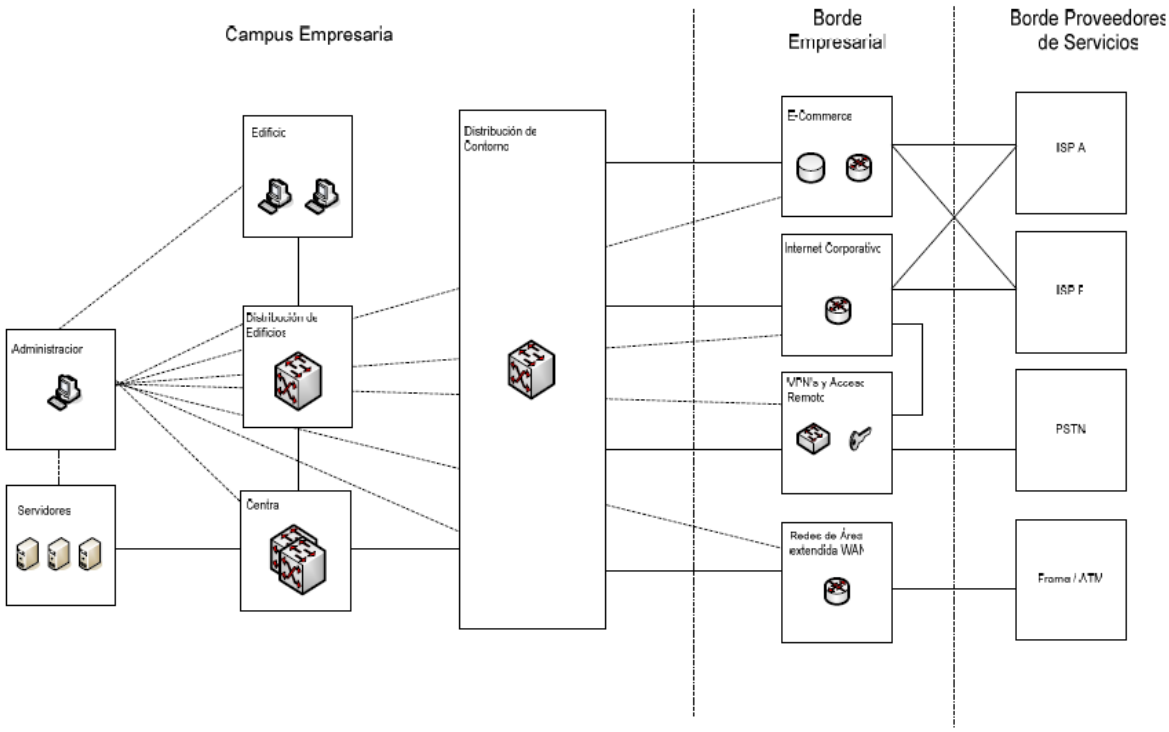


Figura A.1: Arquitectura SAFE de Cisco
Autor: yo
Fuente: www.etmk.cl/in72j/papers/safe_wp_es.pdf

A continuación se describirán las áreas funcionales que componen cada uno de los módulos de la arquitectura SAFE.

CAMPUS EMPRESARIAL

Cada uno de estos módulos están encargados de realizar roles específico dentro de la red. De igual manera tienen requisitos específicos de seguridad. A continuación se describen los módulos de Campus Empresarial.

Módulo Central

Este módulo se encarga de administrar las rutas y encaminar el tráfico tan rápido como le sea posible desde una red a otra. Los dispositivos dominantes son routers y switchs de capa 3 que encaminan los datos de la red de producción a otros módulos.

Módulo de Servidores

La meta fundamental de este módulo es de proporcionar servicios de aplicación como impresión, servicio de archivos, servicio de nombres de dominio, correo electrónico interno, antivirus, entre otros. Los servicios de aplicación definidos en este módulo son utilizados por los usuarios finales pertenecientes al módulo de edificio. Además este módulo se encarga de proveer servicios de capa 3 a los servidores, mediante dispositivos de comunicación como conmutadores de capa 3. Todo el tráfico que circula en el módulo servidor puede ser inspeccionado por los conmutadores de capa 3, mediante un sistema de detección de intrusos de red denominado NIDS.

Módulo de Distribución de Edificios

Este módulo está conformado por dispositivos como switchs de capa 2 y capa 3, y es el que proporcionará la primera línea de defensa y prevención contra ataques internamente originados.

Módulo de Edificio

Este módulo generalmente es la parte más extensa de la red. Ya que es el que contiene a las estaciones de trabajo que utilizan los usuarios finales, además de teléfonos y puntos de acceso asociados con la capa 2. Su meta fundamental es proporcionar servicios a los usuarios finales.

Módulo de Administración

La meta de este módulo es la de facilitar la supervisión segura de todos los dispositivos y estaciones de trabajo dentro de la red empresarial, para ello se debe proporcionar un segmento de red dedicado exclusivamente a la administración, en donde se puede contar con dispositivos especiales como servidores OPT, servidores de control de acceso, servidores de SNMP, servidores active directory, entre otros.

Módulo de Distribución de Contorno

La meta de este módulo es agregar conectividad a los elementos que se encuentran en el borde de la red en estudio, su tráfico es encaminado desde los módulos de borde y encaminado hacia el módulo central.

Este módulo es similar en algunos aspectos a módulo de Distribución de Edificio, en términos de la funcionalidad total. Ambos módulos emplean control de acceso para filtrar el tráfico, aunque el módulo de Distribución de Edificio puede confiar en el área funcional del borde para realizar funciones adicionales de seguridad. Ambos módulos utilizan la capa 3 para alcanzar alto rendimiento, pero el módulo distribución de contorno puede agregar funciones adicionales de seguridad porque los requerimientos de rendimiento no son grandes. El módulo Distribución de Contorno proporciona la última línea de defensa para todo el tráfico destinado al módulo general Campus Empresarial desde el módulo general Contorno Empresaria.

BORDE EMPRESARIAL

Como su nombre lo indica, los módulos del Contorno Empresarial son aquellos módulos que se encuentren contenidos dentro del borde de la infraestructura informática de la red empresarial. Estos módulos son los siguientes:

Módulo de Internet Corporativo

Este módulo provee a los usuarios internos, conectividad a los servicios de internet y a los usuarios de internet, acceso a la información que se encuentra en los servicios públicos. El tráfico fluye desde este módulo de Redes Privadas (VPN), y al módulo de Acceso Remoto.

Módulo de Redes Privadas Virtuales y Acceso Remoto

El objetivo de este módulo consta de tres partes fundamentales:

1. Establecer un encargado para finalizar el tráfico VPN de usuarios remotos,
2. Proporcionar un concentrador para finalizar el tráfico VPN de sitios remotos,

3. Por último finalizar el tráfico de los tradicionales usuarios dial-in.

Todo el tráfico enviado hacia el módulo general de Distribución de contorno por un usuario corporativo remoto, se debe autenticar de alguna manera a través del firewall existente.

Para el acceso remoto a VPNs se puede utilizar varios protocolos para hacer un túnel de seguridad. La arquitectura SAFE a elegido IPSec porque los clientes requieren una configuración mínima y al mismo tiempo que se les proporcione una buena seguridad.

Módulo de Comercio Electrónico

El objetivo de este módulo son las aplicaciones e-commerce, por lo que el equilibrio entre el acceso y la seguridad debe ser atendido cuidadosamente; para lograr esto se ha de dividir una transacción de tipo e-commerce en tres componentes como son: web, aplicación y base de datos, permitiendo que la configuración proporcione varios niveles de seguridad sin impedir el acceso a este servicio.

Módulo de Redes de Área Restringida (WAN)

La elasticidad está dada por una conexión dual proporcionada por el proveedor de servicio, a través de encaminadores, y para el módulo de Distribución del Contorno. La seguridad es proporcionada usando características de seguridad del IOS. Las listas de acceso de entrada se usan para bloquear todo el tráfico no deseado que proviene desde el extremo remoto.

ANEXO B

CARACTERÍSTICAS DE BLADE c3000

El HP BladeSystem c3000 Enclosure es una evolución de todo el montaje en rack de la infraestructura. Está diseñado para los sitios remotos, las pequeñas y medianas empresas y centros de datos con limitaciones de refrigeración. Este informe proporciona una visión general de tecnología de la HP BladeSystem c3000, el poder Thermal Logic y tecnologías de refrigeración, y opciones de interconexión.

Descripción general de HP BladeSystem c3000 Enclosure

El HP BladeSystem c3000 Enclosure es el nuevo gabinete a cabo utilizando el BladeSystem c-Class arquitectura. Mientras que el gabinete BladeSystem c7000 está optimizado para aplicaciones de centros de datos empresariales, el gabinete c3000 está optimizado para entornos de computación tales como sitios remotos o pequeños negocios. Más información sobre la arquitectura c-Class y el gabinete c7000 está disponible en el sitio web de la tecnología de HP en www.hp.com / servers / tecnología.

El gabinete c3000 está disponible en dos modelos diferentes, el modelo de bastidor c3000 que se ajuste a HP de tamaño estándar y soportes de otros fabricantes, y el modelo C3000 Torre, que funciona bien en sitios sin bastidores. Ambos modelos emplean c-Class con factor de forma blades de servidor, almacenamiento blade y módulos de interconexión. El gabinete c3000 está optimizado para entornos de computación, tales como los sitios remotos, tiendas minoristas, oficinas pequeñas, plataformas petrolíferas, barcos, aviones, camiones o cualquier sitio con las opciones de energía limitados. El gabinete c3000 también está diseñado para los sitios que pueden no tener ninguna capacidad de refrigeración especial, sino que pueden existir en ambientes de hasta 35 grados centígrados. El gabinete c3000 admite el uso de dispositivos de gestión, tales como conmutadores KVM locales para la administración local.

El HP BladeSystem c3000 Enclosure tiene rutas redundantes de la señal entre los servidores y módulos de interconexión. El plano medio de la señal continua en el gabinete c3000 no tiene componentes activos. La carcasa está disponible con un subsistema de alimentación monofásica que puede funcionar tanto con línea baja (120 VAC) o de alta gama (240 VAC) de potencia. Ambos modelos c3000 se puede rellenar con los siguientes componentes:

- Hasta cuatro cuchillas de altura completa (FH) u ocho cuchillas de media altura (HH) del servidor y / o almacenamiento por gabinete
- Hasta cuatro módulos de interconexión al mismo tiempo que apoyan una variedad de fibras de interconexión de red como Ethernet, Canal de fibra (FC), entre otras.
- Los kits de Active Cool Fan para un máximo de seis ventiladores
- Hasta seis fuentes de alimentación, ya sea con el poder bajo la línea o líneas de alta-input1
- Uno o dos BladeSystem Onboard Administrator (OA) módulos de gestión
- Unidad de DVD
- Opción de módulo KVM caja para conectar el C3000 a un conmutador KVM en el rack o HP TFT 7600 de montaje en rack de teclado / monitor

Figura 1: HP BladeSystem c3000 Enclosure - vista frontal

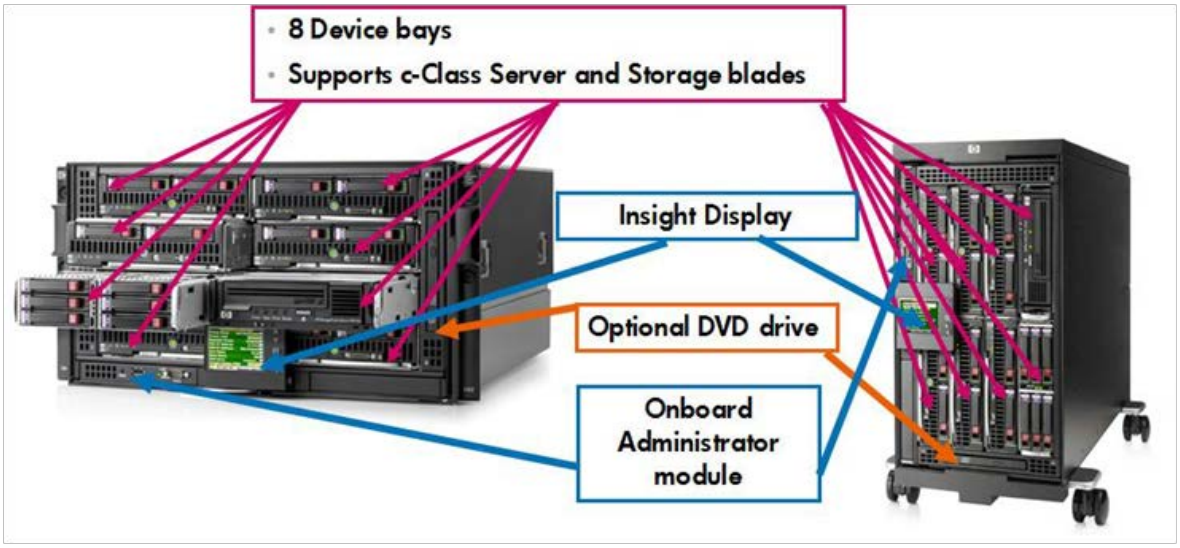
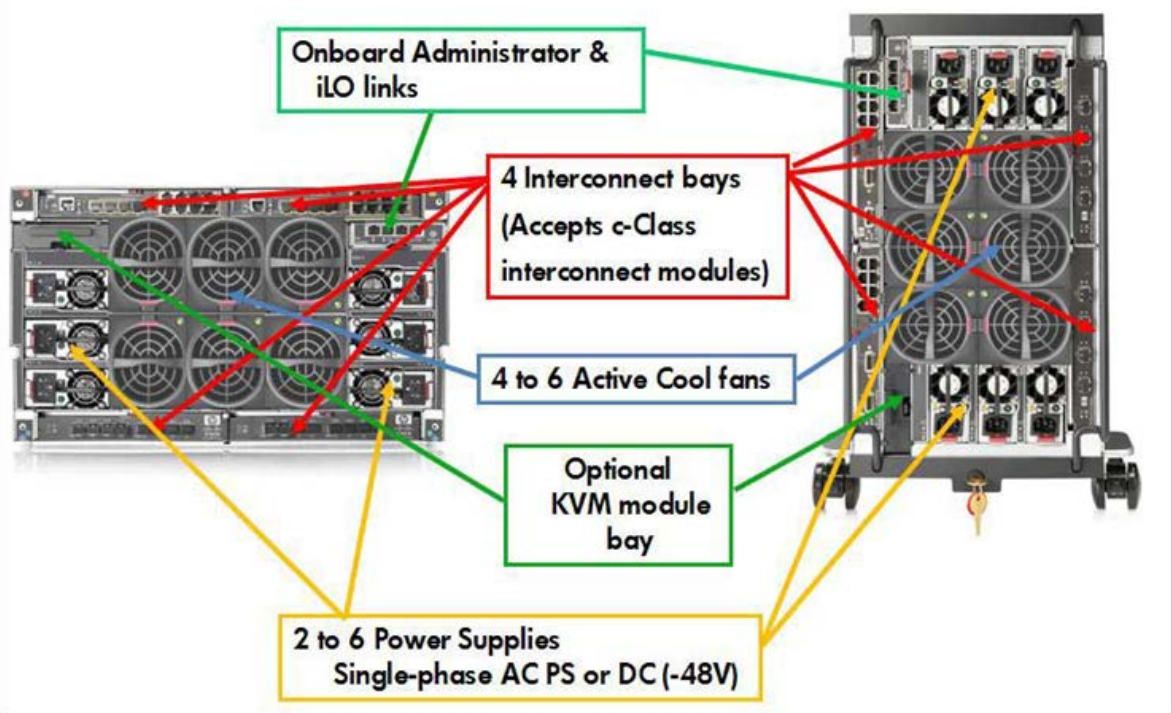


Figura 2. HP BladeSystem c3000 Enclosure – vista trasera



La caja c3000 puede almacenar componentes críticos de la infraestructura, tales como: servidores, las interconexiones, tarjetas intermedias, cuchillas de almacenamiento, fuentes de alimentación y ventiladores. La Tabla 1 enumera los componentes del soporte dos recintos.

Enclosure	c3000
Model	Rack (6U) or Tower
Blade orientation	Horizontal (rack) Vertical (Tower)
Blades supported	8 HH , 4 FH, 6HH/1FH
Interconnect bays	4
Power supplies	6 at up to 1200 watts each
Active Cool fans	6
Enclosure KVM support	Yes
CD/DVD support	Enclosure-based available
OA support	Single or dual
Midplane speed	Tested up to 10 Gbit on Midplane
OA Serial/USB connections	In front

ANEXO C

ACUERDO DE NIVEL DE SERVICIO (SLA)
CNT - CLIENTE

CONTENIDO

SLA Acuerdo de Niveles de Servicio

1.1. Definiciones y Objetivos

El presente acuerdo tiene como finalidad:

- Definir el Acuerdo de Niveles de Servicio (SLA) "Service Level Agreement" entre el CLIENTE y CNT, el cual describe los objetivos de desempeño y disponibilidad.
- Proporcionar una mayor visibilidad y conocimiento de los **Servicios** que demanda el CLIENTE para su negocio.
- Conocer los alcances, limitaciones y responsabilidades tanto del CLIENTE, como de CNT

Los objetivos de desempeño y disponibilidad serán los parámetros medibles de la relación CLIENTE - CNT, y podrán estar sujetos a revisiones continuas.

1.2. Relación CLIENTE – CNT

El SLA descrito en este documento establece un acuerdo entre el CLIENTE y CNT, cuyo sistema servirá para la implementación de los servicios contratados para uso exclusivo del CLIENTE.

1.3. Grupos de Trabajo

Cada una de las partes establecerá un Grupo de Trabajo, cuyas tareas serán:

1.3.1. **Implementar** la solución demandada, lo cual comprende:

- Instalar y configurar el equipamiento para los enlaces contratados.
- Activar los servicios contratados, utilizando la tecnología que mejor relación costo-beneficio ofrezca para cada localidad en particular.

1.3.2. **Administrar** la solución, lo cual comprende:

- Cuidar de que los servicios contratados y equipos de comunicación se hallen trabajando dentro de los parámetros y rangos de utilización apropiados para garantizar el servicio.
- Planificar cambios y crecimientos, de tal forma que cualquier variación a una topología no implique degradación del servicio a los usuarios de la red, no afecte a otras áreas de la red y no genere costos indirectos en otras plataformas tecnológicas.
- Ofrecer soluciones alternas y/o de contingencia, para superar problemas en el o los enlaces contratados o equipos de comunicación.

1.4. Niveles de Servicio

CNT deberá cumplir con los Niveles de Servicio detallados en la siguiente tabla.

Id	Denominación	Niveles de Servicio
1.4.1	Disponibilidad de servicio	Se entiende como "**disponibilidad**" al tiempo medido en horas, que el servicio se encuentra operativo, con los parámetros anotados en este numeral. La disponibilidad será medida mensualmente, considerando los valores de cada servicio en forma independiente. Según el resultado de esta medida se definirá el Valor Mensual a Pagar, conforme a lo expresado en el numeral 1.5.5 de esta tabla. **La disponibilidad (D) mínima mensual contratada se encuentra en la orden de servicio suscrita con el cliente y en el catálogo de productos.** El valor de disponibilidad se calculará con la siguiente expresión: **D = ((TD+TM) / TT) * 100 [%]** Donde:

Id	Denominación	Niveles de Servicio
		D (%) = Disponibilidad mensual del enlace, expresado como un porcentaje. **TD** (horas) = Tiempo Disponible, tiempo que el servicio estuvo disponible en horas durante el mes. **TT** (horas) = Tiempo Total, tiempo total de horas en un mes. Este valor es fijo, y dependiendo del mes, será igual a: 672 horas (28 días). 696 horas (29 días). 720 horas (30 días). 744 horas (31 días). **TM** (horas) = Tiempo en Mantenimiento, tiempo que el enlace estuvo fuera de servicio debido a mantenimientos preventivos planificados por CNT y previamente aceptados por el CLIENTE; o a cualquiera de los motivos que se consideran como causas de fuerza mayor, indicados a continuación: • Desastres naturales, atentados, hurto, vandalismo, accidente, incendio, alteración del orden público, etc, que afecten las instalaciones, equipos y/o facilidades de CNT. • Tiempo de movilización (tm) al sitio de falla (en caso de requerirse), cuyos valores máximos se ajustarán a la siguiente tabla: • Fallas en las instalaciones del CLIENTE tales como acometidas internas, pares aislados, ducterías internas, sistemas de tierra, reguladores, baterías, plantas eléctricas y UPS´s, aplicaciones y protocolos utilizados por el CLIENTE, equipos de cómputo y equipos de comunicación de datos para LAN, falta de permisos apropiados para el acceso de CNT a las instalaciones del CLIENTE. • Tiempo que se genere en otorgar los permisos apropiados para el acceso a las instalaciones del CLIENTE. • Interrupciones autorizadas y/o requeridas por el CLIENTE. No cuenta para el cálculo de la disponibilidad, los problemas en donde se detecte que la falla fue originada en el equipamiento del cliente ó por mala manipulación de los equipos de CNT, sin el consentimiento de su personal técnico. Quedan excluidos además, los problemas que sean originados por fallas en extremos del circuito provistos por otro operador diferente de CNT, a menos de que se trate de: a) un contrato en donde CNT asume la administración y facturación por circuito completo; o, b) la subcontratación de terceros por parte de CNT.

Id	Denominación	Niveles de Servicio
1.4.2	Calidad del Enlace	La Calidad de un servicio contempla anchos de banda (BW), retardos y errores o pérdidas de paquetes. **Ancho de Banda** • Este valor será definido por el CLIENTE de acuerdo al tipo de plan contratado para Internet y Datos. En los casos de servicios diferentes a éstos, éste será definido de acuerdo a las condiciones del servicio. **Retardos** • El retardo se medirá, como referencia, utilizando ICMP a través del servicio "**ping**" (echo request / echo reply) en un canal sin carga. • Según el tipo de enlace, los tiempos promedios de ping, considerando un canal sin carga, un tamaño de paquete de 100 bytes, y 100 pines de prueba, deberán ser los siguientes: Locales < 80 ms (para enlaces terrestres). Interurbanos < 90 ms (para enlaces terrestres). Internacionales < 100 ms (al NAP de las amércias) Satelitales < 1200 ms Internet < 80 ms al primer ruteador del Internet. **Errores** • Todos los servicios que involucren transmisión de datos deberán garantizar una tasa de error de bit inferior a $1x10^{-8}$ (BER), medido durante un período no menor a 24 horas, al momento de la instalación. Para los casos de servicios instalados en capas superiores del modelo OSI, será suficiente las pruebas de pérdida de paquetes. CNT asegurará que los enlaces se encuentren dentro de este rango una vez que han sido implementados. **Pérdida de Paquetes**
1.4.3	Horario de Soporte Técnico.	CNT cuenta con un Centro de Servicio Técnico, en el cual se encuentre laborando el personal con la experiencia y el conocimiento necesario, de tal manera que puedan brindar el soporte apropiado al CLIENTE para superar cualquier inconveniente o problema en los canales. Este horario es de: **7x24x365**.
1.4.4	MTTR Y MTBF	CNT ofrece un tiempo promedio de recuperación ante fallas del servicio (MTTR - mean time to recovery) MTTR del canal de datos de: 3 horas. Los tiempos indicados anteriormente se toman bajo las siguientes consideraciones: • Este tiempo inicia desde el momento del reporte realizado por el personal del CLIENTE, y la recepción del Número de Caso (notar numeral 1.4.8 de este documento). • En este tiempo se contempla el período de diagnóstico y solución del problema. • No está considerado el tiempo de movilización, en caso de ser requerido (ver numeral 1.5.1) • Para asegurar los lapsos mencionados, CNT indicará, en el momento del reporte, el personal que va a dar solución al problema, de tal manera que se generen los permisos apropiados para el acceso a las instalaciones del CLIENTE. El tiempo promedio entre fallas del enlace (MTBF - mean time between failure) es de 90 días.
1.4.5	Valor a pagar	El valor mensual a pagar por el CLIENTE a CNT por cada enlace se

Id	Denominación	Niveles de Servicio
		calculará basándose en la siguiente fórmula: VALOR A PAGAR = VALOR MENSUAL – DESCUENTO VALOR MENSUAL: Pensión básica, sin incluir renta de equipos o consumo. DESCUENTO: Si por causas atribuibles a CNT y salvo caso fortuito o fuerza mayor, existiera una disponibilidad inferior a la ofertada en este SLA, CNT se compromete a descontar del valor mensual contratado, de acuerdo a lo estipulado en el catálogo del producto. En caso de que no exista un tabla dentro de dicho servicio, entonces se aceptará por concepto de multa el valor a describirse a continuación:
1.4.6	Provisión de nuevos servicios	Para nuevos servicios ó ampliaciones solicitados por el CLIENTE, CNT deberá cumplir con las siguientes valores máximos: • Entrega de factibilidad y cotización: 5 días, a partir de la solicitud escrita (aplica el uso de correo electrónico) • Entrega de un nuevo servicio: de 3 a 12 (diez días laborables), a partir de la aceptación escrita de la cotización y dependiendo de la complejidad y tipo de solución. Este enlace deberá estar validado por la Hoja de Aceptación de numeral 1.6 del presente SLA. • Estos tiempos aplican cuando el requerimiento sea estándar. Requerimientos especializados estarán sujetos a factibilidad técnica.

[1] Este descuento es válido para servicios corporativos. En el caso de servicios masivos, el descuento será proporcional al tiempo que el servicio permanezca indisponible, fuera de la disponibilidad ofertada. Descuento
= Valor a pagar x (Tiempo disponible ofertado - Tiempo disponible del servicio) / Tiempo disponible ofertado. En el caso de servicios que incluyan rubros fijos más rubros de consumo, éste descuento será aplicado para el valor fijo y no para el consumo realizado.

ANEXO D

NIVELES DE RIESGO CORTE CONSTITUCIONAL

Según los lineamientos de Cobit 4.1, la evaluación y administración de riesgos se basa en crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar con respecto a variables que analicen al menos un mínimo de probabilidad de que un evento ocurra.

VALORACIÓN DE LOS RIESGOS

Riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento.

En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la concurrencia de una pérdida (por ejemplo el riesgo de perder datos debido a rotura de disco, virus informáticos, entre otros).

Existen varios elementos para determinar un riesgo que son: probabilidad, amenazas, vulnerabilidades, activos e impactos.

Probabilidad: establecer la probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción atenuante, o sea, debe considerarse en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

Amenazas: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, facilidad de acceso a las instalaciones, etc.

Vulnerabilidades: son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevando a esos activos a ser vulnerables.

Activos: los activos a reconocer son aquellos relacionados con sistemas de información.

Impacto: Se habla de un impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Estimar el impacto generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que se considerará parte del daño económico, así como también otros valores por ejemplo daños materiales y emocionales, que causarían perjuicios considerables en el desempeño de labores de la Corte Constitucional. Debido a esto, es que el Departamento de Tecnología ha definido de forma cualitativa el nivel de impacto que sufriría la infraestructura tecnológica de la entidad ante un posible riesgo.

Tabla del nivel de riesgo de la Corte Constitucional se encuentra evaluada según la siguiente tabla a continuación en la Tabla 1:

RIESGO	IMPACTO
Bajo	Tolerable (2)
Medio	Moderado (3)
Alto	Importante (4 – 5)

Tabla 1: Niveles de riesgo

2 – Tolerable.- se debería considerar soluciones más rentables o mejoras que no supongan una carga económica importante, además de comprobaciones periódicas para asegurar que se mantiene la eficacia de las medidas de control.

3 – Moderado.- Se debe proponer un plan para reducir el riesgo, determinando las inversiones precisas. Las medidas para reducir el riesgo deben implantarse en un período determinado. Cuando el riesgo moderado está asociado con consecuencias extremadamente dañinas, se precisará una acción posterior para establecer, con más precisión, la probabilidad de daño como base para determinar la necesidad de mejora de las medidas de control.

4 – Importante.- Se debería implementar políticas de control de seguridad de la información en donde se precisen los recursos considerables para controlar el riesgo. Cuando el riesgo corresponde a un trabajo que se está realizando, debe remediarse el problema en un tiempo inferior al de los riesgos moderados.

5 – Intolerable.- No se debería permitir comenzar, ni continuar el trabajo, hasta que se reduzca el riesgo e implementar un plan de retroalimentación de daños con sus respectivas causas. Si no es posible reducir el riesgo, incluso con recursos limitados, debe prohibirse el trabajo.

Para poder realizar la matriz de riesgos de la infraestructura tecnológica de la entidad se ha tomado en cuenta los equipos que se muestra a continuación en la Tabla 2 sin ningún orden en particular dependiendo de su importancia:

#	EQUIPOS EN RIESGO
1	Blade
2	Servidores
3	Sistema de Almacenamiento
4	Aire Acondicionado
5	UPS Data Center
6	Extintor
7	Dispositivos de interconexión
8	Cámaras de seguridad
9	Grupo electrógeno
10	UTM seguridad perimetral
11	Cableado estructurado
12	Aplicaciones y servicios
13	UPS edificio

Tabla 2: Infraestructura tecnológica de la Corte Constitucional

La matriz de riesgos se encuentra valorada según datos estadísticos sobre amenazas obtenidos de la "IV Estadística Latinoamericana de Seguridad de la Información 2012[109]" realizada por la ACIS (Asociación Colombiana de Ingenieros de Sistemas), organización que se encuentra respaldada por CSIRT.ORG e ISACA para su investigación, una vez concluido su estudio se puede obtener la siguiente información sobre el porcentaje de ataques a nivel latinoamericano como muestra la Tabla 3 a continuación:

Id.	Contingencia	Porcentaje
A	Ataque de aplicaciones web	18%
B	Manipulación de aplicaciones de software	17%
C	Virus	43%
D	Cortes de corriente	9%
E	Monitoreo no autorizado del tráfico	9%
F	Robo de datos	7%
G	Acceso no autorizado	5%
H	Errores de hardware	4%
I	Pharming	4%
J	Otros factores (espionaje)	3%

Tabla 3: Porcentajes de riesgo según ACIS

[109] **IV Estadística Latinoamericana de Seguridad de la Información 2012**, Obtenida en, http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XII_JornadaSeguridad/PresentacionJeimyCano-IVELSI.pdf

Además, en esta encuesta realizada por la ACIS también se encuentran detallados los porcentajes de las medidas de prevención con mayor índice de efectividad para proteger la infraestructura tecnológica de una organización, y esta información se la puede observar a continuación de acuerdo a las medias de control que se encuentran implementadas en la Corte Constitucional, como muestra la Tabla 4:

Protección	**%**
Antivirus	84.16%
Contraseñas	78.33%
Firewalls Hardware / UTM	85.27%
VPN/IPSec	64.72%
Sistemas de IPS e IDS	71.05%
Generador eléctrico y UPS	85.16%
Proxies con filtros web	84.71%
Promedio de Seguridad:	**79.06% Control actual**

Tabla 4: Mecanismos de protección

Como se puede observar en la Tabla 4 de acuerdo a las estadísticas sobre efectividad de medidas de control de la ACIS, la Corte Constitucional posee actualmente un promedio de seguridad de 79.06%, gracias a las medidas de control que se han tomado hasta el momento.

Para este caso y con respecto a los datos estadísticos de la ACSI, los equipos de la Corte Constitucional han sido seleccionados y evaluados con una calificación del 1 al 5 de acuerdo a la Tabla 1 de nivel de riesgos, con las siguientes características según su ubicación:

- En la fila principal se encuentran identificadas 7 amenazas con sus respectivos identificadores que fueron tomadas de la Tabla 3.
- En las columnas siguientes se indican los identificadores para cada uno de los activos a proteger obtenidos de la Tabla 2 y cuál es el importe de la pérdida media estimada que ocasionaría esa amenaza en ese activo.
- Los valores de la fila impacto se han dado de forma cualitativa de acuerdo al nivel de gravedad de que uno de los activos de la Corte quede inoperativo o afectado por un evento.
- Los valores asignados a cada uno de los eventos fueron calculados con la **fórmula: Impacto * % estadístico ACIS**, como por ejemplo, calcular el porcentaje de riesgo de que el Blade enfrente un Ataque de aplicaciones:
  Valor de la celda A1:

  A1= impacto * % ACIS
  A1= 5 * 0.18%
  A1= 0.85

De esta forma se calcularon todos los datos dentro de la matriz de riesgos de la Tabla 5 que se muestra a continuación.

- Finalmente, en la última fila, se indica cuál es el riesgo residual, que resulta de aplicar el porcentaje del promedio de efectividad de control obtenido en la Tabla 4 al riesgo total; como por ejemplo, si se desea calcular el riesgo residual de la celda Riesgo 3 el procedimiento sería el siguiente:

Riesgo columna 3 = 4.5
Efectividad de control = 79%
Riesgo Residual = (1 – 0.79) * 4.5
Riesgo Residual = 0.21 * 4.5
Riesgo Residual = 0.94

Con este proceso se calcularon todos los riesgos residuales de la Tabla 5 que se muestra como matriz de riesgos.

Amenazas	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
A	0.85	0.68	0.85	0.68	0.85	0.85	0.68	0.68	0.51	0.85	0.68	0.85	0.34
C	2	1.5	2	1.5	2	2	1.5	1.5	1.2	2	1.5	2	0.86
D	0.45	0.36	0.45	0.36	0.45	0.45	0.36	0.36	0.27	0.45	0.36	0.45	0.36
E	0.45	0.36	0.45	0.36	0.45	0.45	0.36	0.36	0.27	0.45	0.36	0.45	0.36
F	0.35	0.28	0.35	0.28	0.35	0.35	0.28	0.28	0.21	0.35	0.28	0.35	0.14
G	0.25	0.2	0.25	0.2	0.25	0.25	0.2	0.2	0.15	0.25	0.2	0.25	0.1
H	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.1	0.2	0.2	0.2	0.1
Impacto	5	4	5	4	5	5	4	4	3	5	4	5	2
Riesgo	4.5	3.5	4.5	3.5	4.5	4.5	3.5	3.5	2.7	4.5	3.5	4.5	2.2
Efectividad Control	79%	79%	79%	79%	79%	79%	79%	79%	79%	79%	79%	79%	79%
Riesgo Residual	0.94	0.73	0.94	0.73	0.94	0.94	0.73	0.73	0.57	0.94	0.73	0.94	0.46

Tabla 5: Matriz de riesgos de infraestructura

VALORACIÓN DE PROBABILIDAD DE RIESGO

Se trata de la probabilidad de que un riesgo ocurra. Los factores que se tienen en cuenta para determinar la probabilidad son los siguientes: el origen de la amenaza, el potencial del origen y la respuesta que se dará a la vulnerabilidad detectada, y por otro lado, la existencia de los mecanismos de control que existen actualmente para controlarlos. La probabilidad puede describirse como baja (0.1 – 0.3), media (0.4-0.7) y alta (0.8-1.0).

Baja: el evento puede ocurrir en algún momento

Media: el evento ocurrirá probablemente en muchos casos

Alta: el evento ocurrirá en la mayoría de casos

RIESGO	PROBABILIDAD
Baja	Tolerable (0.1 – 0.3)
Media	Moderado (0.4 – 0.7)
Alta	Importante (0.8 – 1.0)

Tabla 6: Valores de probabilidad de riesgos

Tolerable.- se encuentra valorado de acuerdo a la probabilidad de que un evento se presente aunque sea de forma mínima, sin embargo, se encuentra controlado debido a los mecanismos implementados para mantener este índice bajo.

Moderado.- tiene que ver con la probabilidad de que un riesgo se presente en un rango medio, representando un peligro para la inversión operativa de los activos de la Corte Constitucional, en el que se deberían revisar e incrementar los mecanismos de control de la seguridad.

Importante.- este tipo de probabilidad significaría que no se posee ningún mecanismo de control, o que si existe, es inefectivo para mitigar amenazas y se deberían replantear los controles de seguridad de forma inmediata.

Existen 3 puntos básicos para este tipo de análisis de probabilidad según Cobit que son:

Identificación de Eventos.- identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa aunque sean mínimos, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información registrada

Evaluación.- Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

Respuesta a los Riesgos.- Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

Por estas razones es que este tipo de cálculo se lo realizará en base a una distribución de probabilidades discretas como método cuantitativo, ya que en este

tipo de variables siempre se contempla un rango de error aunque sea el más mínimo, tomando en cuenta que se habla de activos tecnológicos en donde siempre se corre el riesgo de cualquier brecha de seguridad; esto al contrario de la distribución de variables continuas en el cual si pueden tener valores de cero, que para este caso de infraestructura tecnológica serían porcentajes perfectos imposibles de alcanzar.

FACTORES DE RIESGO INSTITUCIONAL Y SU VALOR PONDERADO

A continuación se resumen los principales factores de riesgo de la Corte Constitucional y los pesos ponderados asignados a los mismos.

Riesgos financieros 35%
Riesgos operativos 25%

De acuerdo a estos factores de riesgo institucional, los riesgos operativos que incluyen a las TI se catalogan en un 25% de incidencia, que hacen referencia a la pérdida resultante de procesos, personal o sistemas inadecuados o ineficientes, o de eventos externos. Por estas razones es que para poder calcular la distribución de probabilidad discreta de que un evento se origine dentro de las TI se utiliza la siguiente fórmula:

Probabilidad de riesgo = (Riesgo Total / Impacto Promedio) * 25 riesgo operativo

Siendo:

Riesgo Total: es el rango de daño en porcentaje que recibirá la entidad por la pérdida de cualquier herramienta relacionada con la infraestructura tecnológica.

Impacto Promedio: representa el valor económico para la empresa por la pérdida de cualquier herramienta relacionada con la infraestructura tecnológica.

Riesgo operativo: según factores de riesgo institucional y su valor ponderado.

Considerando estos aspectos, el riesgo total según el impacto que causaría un desperfecto o daño de los equipos de la Corte Constitucional según la Tabla 7 sería:

Impacto	Riesgo Total
5	100 %
4	80 %
3	60 %
2	40 %
1	20 %

Tabla 7: Porcentajes de riesgo total según su impacto

Y considerando la infraestructura que se tiene actualmente el impacto promedio con respecto a los Riesgos Financieros para reponer un equipo o servicio dañado sería:

RIESGO	IMPACTO PROMEDIO $
Blade	$ 10.000
Servidores	$ 4.000 - $ 8.000
Sistema de Almacenamiento	$ 15.000
Aire Acondicionado	$ 11.000
UPS Data Center	$ 10.000
Extintor	$ 11.000
Dispositivos de interconexión	$ 1.000
Cámaras de seguridad	$ 6.000
Grupo electrógeno	$ 20.000
UTM seguridad perimetral	$ 67.000
Cableado estructurado	$ 5.000 - $ 10.000
Aplicaciones y servicios	$ 10.000
UPS edificio	$ 8.000

Tabla 8: Impacto promedio de acuerdo al Riesgo Financiero

Con la utilización de la fórmula y de acuerdo a los datos obtenidos de la Tabla 6 y de la Tabla 7 se puede comprobar por ejemplo, la probabilidad de riesgo (PR) de un servidor:

PR = (Riesgo Total / Impacto Promedio) * 25

PR = (80% / 8000) * 25

PR = 0.24

Con esta información se puede llevar a cabo el cálculo de la probabilidad de riesgo todos los activos tecnológicos de la entidad; las medidas preventivas que se tomen contra posibles riesgos a la infraestructura se encuentran a cargo del Departamento de Tecnología, y debido a su impacto y su naturaleza, es que se ha realizado el siguiente cuadro sobre el riesgo de TI.

RIESGO ACTUAL DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CORTE CONSTITUCIONAL

De acuerdo a toda la información recopilada anteriormente mediante fórmulas y porcentajes se obtiene la Tabla 9 que se muestra a continuación, que es el resultado de la probabilidad e impacto de riesgos que posee actualmente la infraestructura de la Corte Constitucional.

INFRAESTRUCTURA	PROBABILIDAD	IMPACTO	JUSTIFICACIÓN
Cableado estructurado	0.5	4	Su incidencia es mayor puesto que el cableado se encuentra expuesto a posibles cortes o rupturas accidentales debido a que se encuentra visible a todos los usuarios.
Aplicaciones y servicios	0.4	5	Representa un riesgo mayor por el auge en los ataques a aplicaciones y servicios para obtener información, tomando en cuenta la manipulación tanto interna como externa a la que se enfrentan.
UPS Data Center	0.3	5	La única debilidad de este equipo, es que la ausencia de energía eléctrica pueda superar el tiempo de respaldo que pueden brindar las baterías al Data Center.
Dispositivos de interconexión	0.3	4	Los dispositivos de interconexión se encuentran protegidos contra manipulación directa, sin embargo al cortar el cableado se podría afectar la comunicación entre ellos dejando la posibilidad de retardar el paso de información
Cámaras de seguridad	0.3	4	Las cámaras representan una incidencia mayor debido a que se encuentran expuestas en el exterior de pasillos, sin embargo cuentan con vidrio protector y están a cargo de la Policía Nacional.
Blade	0.2	5	Su probabilidad de daño es muy baja debido al UTM de seguridad implementado que lo protege contra ataques, al sistema de extinción del Data Center y a las cámaras de vigilancia.
Extintor	0.2	5	El sistema de extinción se encuentra controlado por la empresa proveedora de la solución, brindando la garantía necesaria para que el sistema funcione a la perfección.
Sistema de Almacenamiento	0.2	5	Su probabilidad de daño es muy baja debido al UTM de seguridad, al sistema de extinción del Data Center y de registro de intrusiones no autorizadas gracias a las cámaras de vigilancia.

Aire Acondicionado	0.2	4	Este sistema posee una baja incidencia debido a que se realiza un mantenimiento continuo, además de informar diariamente al administrador sobre su comportamiento vía mensajes de texto.
Servidores	0.2	4	Su probabilidad de daño es muy baja debido al UTM de seguridad implementado, de posibles incendios gracias al sistema de extinción del Data Center y a las cámaras de vigilancia.
UPS edificio	0.2	2	La incidencia y el impacto de este equipo son tan bajos ya que se tiene el respaldo del generador eléctrico y el UPS del Data Center para mantener con energía todos los componentes tecnológicos de la entidad.
UTM de seguridad	0.1	5	Este equipo posee el índice más bajo de incidencia debido a que fue adquirido recientemente y de acuerdo a su configuración redundante con 2 equipos de las mismas características, es capaz de filtrar, analizar y proteger todo el tráfico de datos de la Corte Constitucional.
Grupo electrógeno	0.1	3	La probabilidad de que se presente un riesgo es muy baja debido a que este equipo se encuentra revisado y garantizado por el proveedor de la solución.

Tabla 9: Probabilidad e impacto de riesgos en la infraestructura

De esta forma se han catalogado los posibles riesgos dentro de la infraestructura de la Corte Constitucional, sin embargo las formas de mitigación podrían ser varias con el objetivo de minimizar la posibilidad de que un riesgo ocurra, algunas de estas opciones de mitigación considerando la infraestructura de la Corte Constitucional podrían ser:

Mitigación:

- La instalación del equipo UTM ayudará a controlar la seguridad de la infraestructura, de la siguiente forma:

Redundancia: instalación de dos equipos de similares características para que si en caso fortuito uno llegara a quedarse sin servicio el otro tomaría su lugar y la seguridad de la Corte Constitucional no se vería afectada.
IDS e IPS: instalación de políticas de análisis de detección y prevención de intrusos, protegiendo así patrones de ataque para las aplicaciones que corren sobre la red.
Firewalls: creación de reglas de seguridad para evitar el ingreso de intrusos tanto a la red como a equipos más sensibles como servidores o Blade.
Filtros Web: reducir el riesgo de que los usuarios ingresen a páginas web potencialmente peligrosas para el rendimiento de la red.
Control de aplicaciones: reducir la instalación y uso de aplicaciones no autorizadas por el Departamento de Tecnología, disminuyendo de esta forma el tráfico sobre la red de aplicaciones innecesarias.
Control de ancho de banda: beneficiará al tráfico que fluye a través de la red priorizando aplicaciones que necesitan un mayor ancho de banda como por ejemplo video conferencia.

- El mantener al día la garantía y cobertura de los equipos por parte de los proveedores de la solución tecnológica certifica que los equipos estarán revisados y actualizados constantemente por personal calificado.
- Ampliar los soportes técnicos autorizados ayudaría a garantizar la revisión tanto de hardware como de software de equipo especial.
- Capacitar al personal para que cuide sus contraseñas, así como también enseñarles las formas de crear una contraseña segura.
- Enseñar al personal normas de seguridad informática básica para crear una cultura de acción preventiva ante posibles riesgos.
- Realizar un mantenimiento continuo de toda la infraestructura aportará en tener en óptimas condiciones los equipos disminuyendo la probabilidad de descompostura de la Corte Constitucional.
- Implementar políticas de creación de contraseñas para servidores y aplicaciones sensibles, para de esta forma garantizar disponibilidad, integridad y confidencialidad de la información en todo momento.

Hay que tomar muy en cuenta la implementación de políticas formales para la seguridad de la información, ya que según la encuesta realizada por la ACIS del presente año, tan solo un 54.62% de todas las entidades a nivel latinoamericano cuentan con este tipo de modelo de seguridad en sus organizaciones, por esta motivo es que a continuación en la Tabla 10 se presentará una propuesta de plan de acción para el Departamento de Tecnología de la Corte Constitucional.

PLAN DE ACCIÓN DE RIESGOS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA CORTE CONSTITUCIONAL								
CODIGO	**OBLIGACIÓN**	**CUMPLIMIENTO**	**PLAN DE ACCIÓN**	**MEDIOS DE VERIFICACIÓN**	**RESPONSABLES**	**PLAZO**	**FECHAS DE INICIO / PRESUPUESTO**	**NORMAS DE CONTROL DE RIESGO PARA EL SECTOR PÚBLICO**
TECNOLÓGICO								
1	**Infraestructura y equipamiento tecnológico**							
	Definir el grado de innovación y tecnología que se pueda implementar para mejorar la seguridad de la información en base a una previa evaluación de riesgos.	**cumplimiento**	Con el objetivo de mejorar la seguridad de la red de datos de la Corte y preservar la información, se ha implementado un UTM, que es un sistema de gestión de seguridad unificado que ayudará a mitigar los posibles riesgos detectados anteriormente gracias a características de configuración que incluyen: redundancia, IDS, IPS, firewalls, filtro web, control de aplicaciones, control de ancho de banda, DLP, entre otras que contribuirán a la preservación de la información.	Documentos técnicos ya sean físicos o digitales que respalden la instalación y configuración del equipo.	Administrador de red	3 meses	Julio de 2012 / 22.000 USD	Según norma 410-08
2	**Nuevas políticas y procedimientos**							
	Utilizar la implementación de la infraestructura para crear nuevas políticas y procedimientos con el propósito de preservar la seguridad de la información.	**cumplimiento**	Con la implementación del UTM se ha visto necesario crear nuevas políticas formales para lograr una mejor gestión de seguridad de la información, debido a esto, se han dividido los privilegios de funcionarios de acuerdo a reglas que contemplan horarios de visita a ciertas páginas y la restricción de instalación y uso de aplicaciones en tiempo laboral. Así como también, se han implementado políticas para proteger la red externamente, activando funciones como el filtrado de paquetes, detección de intrusos, entre otras que están incluidas en el licenciamiento.	Implementación de políticas y procedimientos en la configuración del UTM. Licenciamiento por 1 año.	Administrador de red	1 año	Julio de 2012 / 2.500 USD	Según norma 410-04
3	**Mantenimiento y control del UTM**							
	Estas tareas se encuentran cubiertas por el licenciamiento de 1 año por la adquisición del UTM.	**cumplimiento**	La empresa proveedora del producto es la que brindará el mantenimiento correctivo, preventivo, estabilización y actualizaciones necesarias para garantizar el buen funcionamiento del equipo, con personal capacitado y autorizado para realizar estas operaciones.	De acuerdo a lo solicitado en las Bases Técnicas presentadas a través de la página oficial de Compras Públicas.	Departamento de Tecnología	1 año	Enero de 2013 / 1.500 USD	Según norma 410-09
4	**Plan de contingencia**							
	En base a los requerimientos de control interno se ha implementado un plan de contingencia para el UTM.	**cumplimiento**	Como medida de seguridad para una implementación tan sensible dentro de la infraestructura de la Corte Constitucional se ha visto necesario adquirir otro equipo UTM de las mismas características, con el objetivo de tener configurados ambos equipos de forma redundante, así, si el equipo principal llegaría a quedarse inoperativo el otro entraría en funcionamiento para no dejar desprotegida la red.	Implementación de otro equipo UTM redundante como contingencia a fallos.	Departamento de Tecnología	3 meses	Julio de 2012 / 22.000 USD	Según norma 410-11
5	**Capacitación**							
	La capacitación del personal es fundamental para poder sacar el mejor provecho del UTM implementado.	**cumplimiento**	La correcta administración del equipo UTM dependerá de una debida capacitación por parte de la empresa proveedora de la solución tecnológica con personal capacitado, para que el personal que estará a cargo del equipo pueda sacar el máximo provecho tanto de los servicios como de las configuraciones.	Certificación de los cursos de capacitación ofrecidos por el proveedor para administrar el UTM.	Administrador de red	1 mes	Agosto de 2012 / 8.000 USD	Según norma 410-15

ADMINISTRATIVO								
6	**Análisis de riesgos**							
	Un correcto análisis de riesgos ayuda a valorar los activos de la entidad, aportando una base técnica para la seguridad de las tecnologías de la información.	**cumplimiento**	Realizar continuamente un análisis de riesgos aportará al Departamento de Sistemas una visión más amplia sobre los pobremas que podrían presentarse y las medidas de control que se encuentran implementadas para mitigar los daños, buscando de esta forma dejar en porcentajes mínimos la tolerancia a fallos evaluando todas las medidas de control recomendadas a través de los lineamientos de control interno sobre la seguridad de las Tecnologías de la Información.	Documento de análisis de riesgos actual sobre la infraestructura de la Corte Constitucional.	Departamento de Tecnología	1 mes	Agosto 2012 / 0 USD	Según norma 410-10
7	**Personal dedicado a la seguridad**							
	Ubicar personal que este dedicado 100% a la seguridad de la información aportaría un gran valor a la administración y soporte de la tecnología.	**cumplimiento**	Ver la forma de disminuir la posibilidad de que un riesgo ocurra, implementando personal dedicado exclusivamente a la seguridad de la información, ya sea de manera informal con la asignación de personas o de manera formal con la creación de un equipo de respuesta CSIRT, que en cualquiera de los dos casos tenga como objetivo primordial velar de forma proactiva por la seguridad de la información de la Corte Constitucional, en base a investigación continua de riesgos y creación de planes de acción para mitigarlos.	Tesis sobre Gestión de seguridad de la red de datos de la Corte Constitucional mediante el diseño de un CSIRT.	Departamento de Tecnología	8 meses	Enero 2012 / 0 USD	Según norma 410-12
8	**Seguimiento de los procesos**							
	Realizar un seguimiento de los procesos que se mejoraron a partir de la implementación de las nuevas políticas de seguridad del UTM.	**cumplimiento**	Revisar y presentar periódicamente reportes de gestión sobre las políticas de seguridad implementadas, sin descuidar la comunicación a los funcionarios sobre las nuevas reglas de administración de la seguridad, para de esta forma monitorear y evaluar los procesos.	Generación de reportes a través del equipo NetEnforcer AC-502	Administrador de red	3 meses	Julio 2012 / 9.000 USD	según norma 410-13

Tabla 10: Plan de acción de riesgos

En conclusión, una debida investigación de riesgos aporta para valorar los activos tecnológicos con los que cuenta actualmente la Corte Constitucional, pero sobre todo, para determinar las medidas que se están tomando para preservar tanto los activos como los niveles mínimos de probabilidad para que un evento ocurra, sin embargo, hay que tomar en cuenta que Ecuador en el presente no cuenta con una estadística oficial de ninguna entidad sobre niveles de riesgo, razón por la cual, se ha buscado realidades parecidas a la nuestra para sustentar este estudio de riesgos.

Atentamente,

Ing. Gabriel Novoa
Director de Tecnología
CORTE CONSTITUCIONAL

ANEXO E

LIBRO NARANJA

Cuál es el Propósito del Libro Naranja.

De acuerdo con el texto mismo, el criterio de evaluación se desarrolla con 3 objetivos básicos:

Medición: Para proporcionar de elementos cuantificables al Departamento de Defensa (DoD) con los cuales poder evaluar el grado de confianza que se puede tener en los sistemas informáticos seguros, para el proceso de clasificación de información sensitiva.

El proveer a los usuarios con un criterio con el cual se evalúe la confianza que se puede tener en un sistema de cómputo para el procesamiento de la seguridad o clasificación de información sensitiva. Por ejemplo, un usuario puede confiar que un sistema B2 es más seguro que un sistema C2.

Dirección: Para proporcionar un estándar a los fabricantes en cuanto a las características de seguridad que deben de implementar en sus productos nuevos y planearla con anticipación, para aplicarla en sus productos comerciales y así ofrecer sistemas que satisfacen requisitos de seguridad (con énfasis determinado en la prevención del acceso de datos) para las aplicaciones sensitivas.

Adquisición: Para proporcionar un estándar a los fabricantes en cuanto a las características de seguridad que deben de implementar en sus productos nuevos y planearla con anticipación, para aplicarla en sus productos comerciales y así ofrecer sistemas que satisfacen requisitos de seguridad (con énfasis determinado en la prevención del acceso de datos) para las aplicaciones sensitivas. Las categorías de seguridad del DoD van desde D (Protección Mínima) hasta A (Protección Verificada como la máxima categoría). A continuación se presenta un breve resumen las características de cada una de estas categorías y los niveles que tiene cada una.

D- Protección Mínima

Esta división contiene solamente una clase. Esta reservada para los sistemas que han sido evaluados que pero que no pueden cumplir los requisitos para una clase más alta de la evaluación.

Cualquier sistema que no cumple con cualquier otra categoría, o ha dejado de recibir una clasificación más alta. El sistema DOS para PCs se cae en esta categoría.

C- Protección Discrecional

Las clases en esta división proporcionan una Protección discrecional (necesidad – de - identificación) y, a través de inclusión de capacidades de auditoría, exige la responsabilidad de los usuarios de las acciones que realiza.

La protección discrecional se aplica a una Base de Computadoras Confiables (TCB) con protección de objetos optativos (archivos, directorios, dispositivos, etc.).

C1- Protección de Seguridad discrecional

Las TCB de un sistema de la clase C1, deben cubrir los requisitos de seguridad discrecional proporcionando la separación de usuarios y de datos. Incorporar algún mecanismo de control y acreditación, así como la capacidad de hacer cumplir las restricciones de acceso de una base individual, es decir, garantizar de una forma convincente a los usuarios de que sus proyectos o información privada está protegida y evitar que otros usuarios accidentalmente puedan leer o destruir sus datos. Se supone que en el ambiente de la clase C1 existe cooperación entre los usuarios y además todos ellos procesan datos en el mismo nivel(es) de sensitividad.

Los requisitos mínimos para los sistemas con asignación de la clase C1 son:

- Protección de archivos optativa, por ejemplo Control de Listas de
- Acceso (ACLs), Protección a Usuario/ Grupo/Público.

- Usualmente para usuarios que están todos en el mismo nivel de seguridad.
- Protección de la contraseña y banco de datos seguro de autorizaciones (ADB).
- Protección del modo de operación del sistema. Verificación de Integridad del TCB. Documentación de Seguridad del Usuario.
- Documentación de Seguridad del Administración de Sistemas. Documentación para Comprobación de la Seguridad.
- Diseño de documentación de TCB.
- Típicamente para usuarios en el mismo nivel de seguridad.

C2- Protección de Acceso Controlado.

Los sistemas en esta clase hacen cumplir más fielmente un control de acceso discrecional más fino que los sistemas C1, haciendo responsable individualmente a los usuarios de sus acciones a través de procedimientos de conexión, revisión de eventos relevantes de seguridad, y el aislamiento de recursos.

Los siguientes son requisitos mínimos para los sistemas con asignación de clase (C2):

- La protección de objetos puede estar con base al usuario, ej. De un
- ACL o una base de datos del administrador.
- La autorización para acceder sólo puede ser asignada por usuarios autorizados.
- Protección de reutilización de objetos (ejemplo: para evitar reasignación de permisos de seguridad de objetos borrados).
- Identificación obligatoria y procedimientos de autorización para los usuarios, ejemplo: contraseñas.
- Auditoria de eventos de seguridad.
- Protección del modo de operación del sistema.
- Agrega protección para autorizaciones y auditoría de datos. Documentación de la información como C1 plus al examinar la auditoría de la información.

B- Protección Obligatoria

La división B especifica que el sistema de protección del TCB debe ser obligatorio, no solo discrecional.

La noción de un TCB que preserve la integridad de etiquetas de sensibilidad de la información y se utilizan para hacer cumplir un conjunto de reglas obligatorias del control de acceso, es un requisito importante en esta división. Los sistemas en esta división deben llevar las etiquetas de sensibilidad en las estructuras de datos importantes del sistema. El desarrollador del sistema también debe proporcionar un modelo de política de seguridad en el cual se basa el TCB y equipar por medio de una serie de especificaciones al TCB. Evidentemente debe ser proporcionada una demostración que sirva para aclarar el concepto del monitor de referencia y su forma de implementarlo.

B1- Protección de Seguridad por Etiquetas

Los sistemas de la clase B1 requieren todas las características solicitadas para la clase C2. Además una declaración informal del modelo de la política de seguridad, de las etiquetas de los datos, y del control de acceso obligatorio sobre los eventos y objetos nombrados debe estar presente. Debe existir la capacidad para etiquetar exactamente la información exportada. Cualquier defecto identificado al hacer las pruebas debe ser eliminado.

Los siguientes son los requisitos mínimos para los sistemas con asignaron de grado de la clase B1:

- Seguridad obligatoria y acceso por etiquetas a todos los objetos, ej. archivos, procesos, dispositivos, etc.
- Verificación de la Integridad de las etiquetas. Auditoria de objetos Etiquetados.
- Control de acceso obligatorio.
- Habilidad de especificar el nivel de seguridad impreso en salidas legibles al humano (ej. impresiones.).

B2- Protección Estructurada

En los sistemas de clase B2, los TCB deben estar basados en una documentación formal clara y contar con un modelo de política de seguridad bien definido que requiera un control de acceso discrecional y obligatorio, las imposiciones a los sistemas encontradas en la clase B1, se deben extender a todos los eventos y objetos en sistemas ADP. Además, los canales secretos son direccionados. El TCB se debe estar cuidadosamente estructurado en elementos de protección críticos y elementos de protección no críticos. La interfaz de TCB deberá estar bien definida así como el diseño y la activación de la implementación del TCB le permiten ser sujeto de prueba y revisión más completa. Se consolidan los mecanismos de autentificación, el manejo de recursos seguros se proporciona en forma de ayuda para las funciones del administrador y del operador del sistema, y se imponen controles rigurosos de la administración de configuración. El sistema es relativamente resistente a la penetración.

Los siguientes son requisitos mínimos para los sistemas con asignación de grado de la clase B2:

- Notificación de cambios del nivel de seguridad que afecten interactivamente a los usuarios.
- Etiquetas de dispositivos jerárquicas.
- Acceso obligatorio sobre todos los objetos y dispositivos. Rutas Confiables de comunicaciones entre usuario y sistema. Rastreo de los canales secretos de almacenamiento.
- Modo de operación del sistema más firme en multinivel en unidades independientes.
- Análisis de canales seguros. Comprobación de la seguridad mejorada. Modelos formales de TCB.
- Versión, actualización y análisis de parches y auditoria.
- Un ejemplo de estos sistemas operativos es el Honeywell Multics.

B3- Protección por Dominios

En la clase B3 los TCB debe satisfacer los requisitos de herramientas de monitoreo como un "monitor de referencia" que Interviene en todos los accesos de usuarios a los objetos, a fin de ser comprobada, y que sea lo bastante pequeña para ser sujeta al análisis y pruebas. Al final, el B3 TCB debe estar estructurado para excluir el código no esencial para aplicar la política de seguridad, mediante ingeniería de sistemas durante el diseño y la implementación del TCB, orientada hacia la reducción de su complejidad al mínimo.

Debe de contar también con un Administrador de Seguridad, los mecanismos de auditoría se amplían para señalar acontecimientos relevantes de la seguridad, y se necesitan procedimientos de recuperación del sistema. El sistema es altamente resistente a la penetración.

Los siguientes son requisitos mínimos para los sistemas con asignación de un grado de clase B3:

- ACL's adicionales basado en grupos e identificadores.
- Rutas de acceso confiables y autentificación.
- Análisis automático de la seguridad.
- Modelos más formales de TCB.
- Auditoría de eventos de seguridad.
- Recuperación confiable después de baja del sistema y documentación relevante.
- Cero defectos del diseño del TCB, y mínima ejecución de errores.

A- Protección Verificada

Esta división se caracteriza por el uso de métodos formales para la verificación de seguridad y así garantizar que los controles de seguridad obligatoria y discrecional empleados en el sistema pueden proteger con eficacia la información clasificada o sensitiva almacenada o procesada por el sistema. Se requiere de amplia

documentación para demostrar que el TCB resuelve los requisitos de seguridad en todos los aspectos del diseño, desarrollo e implementación.

Se deben de cubrir todos los requisitos de B3 más otros criterios adicionales:

A1 – Diseño verificado

Los sistemas en la clase (A1) son funcionalmente equivalentes a los de la clase B3 en que no se agrega ningunas características o requisitos arquitectónicos adicionales de la política de seguridad. La característica que distingue los sistemas en esta clase es el análisis derivado de técnicas formales de especificación y la verificación del diseño, y el alto grado de confiabilidad que resulta de la correcta implementación del TCB. Este garantia se desarrolla naturalmente, comenzando con un modelo formal de la política de la seguridad y una especificación formal de alto nivel (FTLS Especificación Normal de Alto Nivel) del diseño. Independiente del lenguaje determinado de la especificación o sistema de la verificación usado, hay cinco criterios importantes para la verificación del diseño de la clase (A1).

Un modelo formal de la política de seguridad debe ser claramente identificado y documentar, incluyendo una prueba matemática que el modelo es constante con sus axiomas y es suficiente para soportar la política de la seguridad.

Un FTLS debe ser proporcionado que incluya las definiciones abstractas de las funciones que el TCB se realiza y de los mecanismos de la dotación física y/o de los firmwares que se utilizan para utilizar dominios separados de la ejecución.

Se debe demostrar que el FTLS del TCB es constante y consistente con el modelo por técnicas formales en lo posible (es decir, donde existen las herramientas de verificación) y las informales de otra manera.

La implementación del TCB (ejemplo, en Hardware, firmware, y software) debe mostrar informalmente que es consistente con el FTLS. Los elementos del FTLS

deben ser mostrados, usando técnicas informales, que correspondan a los elementos del TCB. El FTLS debe expresar un mecanismo unificado de protección, necesario para satisfacer la política de seguridad, y todos los elementos de este mecanismo de protección deben estar asociados a los elementos del TCB.

Deben de utilizarse técnicas de análisis formal para identificar y analizar los canales secretos. Las técnicas informales se pueden utilizar para identificar los canales secretos de sincronización. La continua existencia de canales secretos identificados en el sistema debe ser justificada.

ANEXO F

SERVICIOS DEL EQUIPO DE SEGURIDAD UTM

A continuación se detallan los servicios que podrán disponer tanto los usuarios finales como el departamento de tecnología con la implementación del nuevo sistema de seguridad:

FIREWALL

FUNCIONARIOS	TECNOLOGÍA
La nueva seguridad perimetral de la Corte proveerá de una mayor velocidad de la red, así como un monitoreo y reporte de posibles atacantes de la red, obteniendo las direcciones desde donde se intentó propiciar el ataque.	Velocidad de análisis de paquetes y nuevas políticas de administración.

VPN

FUNCIONARIOS	TECNOLOGÍA
Con las 9 licencias de VPN incluidas en el sistema de seguridad se podría dar servicio a 9 funcionarios para que en caso de que necesiten, tengan la facilidad de conectarse desde un lugar externo a la red de la corte y poder realizar tareas como imprimir, abrir archivos y hasta realizar llamadas telefónicas.	Conectividad externa a la red para 10 funcionarios.

CALIDAD DE SERVICIO

FUNCIONARIOS	TECNOLOGÍA
Con la capacidad de regular la calidad de servicio se tendrá la posibilidad de priorizar el ancho de banda dependiendo del departamento, área o funcionario y de esta forma mejorar sus niveles de productividad.	Dividir trafico según su prioridad y de esta manera regular el ancho de banda

ANTIVIRUS

FUNCIONARIOS	TECNOLOGÍA
Disminuir la posibilidad de que un virus infecte los servidores, los correos o la información digital adjunta de la Corte. Todo archivo detectado como virus podrá ser recuperado posterior a su desinfección, de esta forma no existirá perdida de información.	Proveer antivirus perimetral, a parte del servidor que ya se tiene localmente.

FILTRAJE DE DIRECCIONES WEB

FUNCIONARIOS	TECNOLOGÍA
Denegar el acceso a direcciones no permitidas, y en caso de que un funcionario quisiera obtener una conexión a ésta, no solo le saldrá un "error", sino que habrá la posibilidad de personalizar el mensaje para informar al usuario de que no está permitido el ingreso a dicha página.	Manejo de restricción de visitas a páginas web inapropiadas sin tener la necesidad de bloquear puertos.

PREVENCIÓN CONTRA INTRUSOS (IPS)

FUNCIONARIOS	TECNOLOGÍA
Todas las entidades privadas o públicas tienen el riesgo de sufrir ataques externos, por esta razón con el nuevo sistema de seguridad se obtendrá el servicio de prevención de intrusos, que monitoreará constantemente, informando y bloqueando, si algún ente externo desea ingresar a la red de la Corte y robar información.	Detectar y prevenir intrusiones externas e internas a los servidores.

MECANISMOS DE DETECCIÓN DE ATAQUES

FUNCIONARIOS	TECNOLOGÍA
Trabaja junto la prevención de intrusos para que la página web de la Corte no sea vulnerada ni alterada externamente, considerando que el portal web es el medio informativo no solo para usuarios locales sino para el exterior.	Detectar secuencias de ataques con algún fin específico en la red de la Corte.

OPTIMIZACIÓN DE RED

FUNCIONARIOS	TECNOLOGÍA
Mejora la velocidad de navegación de los usuarios finales.	Incrementa la velocidad de navegación al poder almacenar en cache las páginas visitadas por los usuarios.

CONTROL DE APLICACIONES

FUNCIONARIOS	TECNOLOGÍA
Controlar aplicaciones que utilizan los funcionarios y de esta manera mejorar su productividad, y además, tener la capacidad de habilitar las mismas solo en horas de almuerzo u otros horarios a convenir.	Poder dar prioridades de utilización de distintas aplicaciones según horario y privilegios.

ALTA DISPONIBILIDAD

FUNCIONARIOS	TECNOLOGÍA
Garantiza la continuidad del negocio.	Al contar con 2 equipos UTM en clúster se dispone de redundancia ante posibles fallos.

CARACTERÍSTICAS DE GERENCIA

FUNCIONARIOS	TECNOLOGÍA
Tener la posibilidad de presentar informes a nivel gerencial y por categorías.	Presentación de informes sobre los acontecimientos detectados por el equipo.

VIRTUALIZACIÓN

FUNCIONARIOS	TECNOLOGÍA
Creación de una Intranet que facilite la navegación institucional. Obtención de información del portal web sin la necesidad de salir a través de Internet.	Disminución del uso de Internet institucional con el uso de la virtualización para crear una Intranet de la Corte.

ANEXO G

BASES TÉCNICAS UTM

ITEM	DESCRIPCION	EMPRESA
Marca	Especificar	
Modelo	Especificar	
Cantidad	2	
Año de fabricación	>= 2011	
Características del dispositivo	El dispositivo debe ser una Appliance de propósito específico	
	Basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection".	
	Soportar la funcionalidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido.	
	El equipo deberá poder ser configurado en modo Nat o en modo transparente en la red.	
	En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.	
	Sistema operativo pre-endurecido específico para seguridad que sea compatible con el appliance.	
	Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos	
Firewall	**Requerido**	
	Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs	
	Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino.	
	Las reglas del firewall deberán tomar en cuenta dirección IP fuente, dirección IP destino y servicio de la comunicación que se está analizando	
	Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación	
	Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo	
	Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)	
	Capacidad de hacer traslación de direcciones estático, uno a uno, NAT	
	Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.	
	Deberá soportar reglas de firewall enIPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario)	
	Deberá soportar reglas de firewall que soporten autenticación por usuarios mediantes repositorios locales o remotos (LDAP, RADIUS, TACACS+).	
	Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.	
Conectividad y sistema de ruteo	**Requerido**	
	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP	
	Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs	
	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas	
	Soporte a políticas de ruteo (policy routing)	
	Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP	
	Soporte a ruteo de multicast	
VPN IPSec	**Requerido**	
	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)	
	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.	
	Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits	
	Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site	
	La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)	
	En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.	

VPN SSL	Requerido	
	Capacidad de realizar SSL VPNs	
	Soporte a certificados PKI X.509 para construcción de VPNs SSL	
	Soporte a asignación de aplicaciones permitidas por grupo de usuarios	
	Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet	
	Deberá poder verificar la presencia de antivirus y de un firewall personal en la máquina que establece la comunicación VPN SSL	
	Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)	
	La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS	
	Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL	
	Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente	
	Debera permitir la creacion de portales personalizables y que sean asignados a diferentes tipos de usuarios	
Traffic Shapping / QoS	**Requerido**	
	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall	
	Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo	
	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo	
	Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia	
Autenticación y Certificación Digital	**Requerido**	
	Capacidad de integrarse con Servidores de Autenticación RADIUS	
	Capacidad nativa de integrarse con directorios LDAP	
	Capacidad incluida, al integrarse con Microsoft Windows Active Directory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”	
	Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet	
	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)	
	Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos	
Antivirus	**Requerido**	
	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP, HTTPS, SMTPS, POP3S e IMAPS	
	Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido	
	La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3, FTP, HTTPS, SMTPS, POP3S e IMAPS deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso	
	Por desempeño y eficiencia, el antivirus deberá funcionar bajo el esquema “Wild list” (Virus en activo solamente) en el cual los virus conocidos que están activos en el Internet son los que se detectan y se detienen	
	El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List)	
	El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos HTTP, SMTP, IMAP, POP3, FTP, HTTPS, SMTPS, POP3S e IMAPS	
	El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red	
	El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger	
	El antivirus deberá ser capaz de filtrar archivos por extensión	
	El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo	

AntiSpam	Requerido	
	La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje	
	La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)	
	La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM	
	En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje	
Filtraje de URLs	**Requerido**	
	Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido	
	Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso	
	Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida	
	Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables	
	Capacidad de filtrado de scripts en páginas web (JAVA/Active X)	
Protección contra intrusos IPS	**Requerido**	
	Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas)	
	Estar orientado para la protección de redes	
	Deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.	
	La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance	
	Deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detección).	
	Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo	
	Tecnología de detección tipo Stateful basada en Firmas (signatures)	
	Actualización automática de firmas para el detector de intrusos	
	Deberá mitigar los efectos de los ataques de negación de servicios	
Mecanismos de detección de ataques	**Requerido**	
	Reconocimiento de patrones, Análisis de protocolos,	
	Detección de anomalías	
	Detección de ataques de RPC (Remote procedure call)	
	Protección contra ataques de Windows o NetBios	
	Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol), Sendmail o POP (Post Office Protocol)	
	Protección contra ataques DNS (Domain Name System)	
	Protección contra ataques a FTP, SSH , Telnet y rlogin	
	Protección contra ataques de ICMP (Internet Control Message Protocol)	
Métodos de notificación	**Requerido**	
	Alarmas mostradas en la consola de administración del appliance.	
	Alertas vía correo electrónico	
Filtraje de tráfico VoIP, Peer to Peer y mensajería instantanea	**Requerido**	
	Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP)	
	El dispositivo deberá tener técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer	
	En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual	

Optimización de enlaces WAN y Cache	**Requerido**	
	Soporte para optimizar enlaces WAN mediante la implantación de dos dispositivos en cada canal de datos WAN	
	La solución debe contar con la capacidad de realizar caching sobre http para ahorro y optimización de tráfico.	
	La solución debe estar en la capacidad de optimizar tráfico SMTP, CIFS, HTTP y FTP a nivel de enlaces WAN.	
	La solución debe permitir a los usuarios la configuración de un proxy explicito de http.	
	La solución debe permitir la integración con plataformas que soporten estándar WCCP	
Control de aplicaciones	**Requerido**	
	Soporte para identificar aplicaciones independientes del puerto tcp/udp utilizado.	
	Capacidad de asignar perfiles de autenticación asociados al uso de aplicaciones.	
	Capacidad de almacenar información sobre el tráfico generado por la aplicación	
Alta Disponibilidad	**Requerido**	
	Soporte de Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.	
	Alta Disponibilidad en modo Activo-Pasivo	
	Alta Disponibilidad en modo Activo-Activo	
	Posibilidad de definir al menos dos interfaces para sincronía	
	El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red	
Características de gerencia	**Requerido**	
	Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS)	
	La interfaz gráfica de ususario (GUI) vía web deberá poder estar en español y en inglés configurable por el usuario	
	Interfaz basada en línea de comando (CLI) para administración de la solución.	
	Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o Telnet)	
	El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales	
	Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.	
	El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o HTTPS.	
	El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.	
	Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.	
Virtualización	**Requerido**	
	El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”	
	La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus	
	Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer	
	Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red	
Estándares	Soporte documentado de los siguientes RFCs: RFC 0768, RFC 0791	
	Soporte documentado a los siguientes estándares de criptografía: PKCS #7 (RFC 2315), PKCS #10 (RFC 2986), PKCS #12	
Licenciamiento y actualizaciones	Tamaño de la licencia: El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través del equipo	
CARACTERÍSTICAS TÉCNICAS	**Requerido**	
Numero de Interfaces Requeridas 10/100/1000	10	
Capacidad de disco para almacenamiento	64GB SSD	
Throughput de Firewall	8 GB	
Throughput de VPN IPSec	6 GB	
Throughput de Antivirus Proxy	160 MBPS	
Throughput IPS (http)	800 MBPS	
Throughput SSL-VPN	200MBPS	
Sesiones Concurrentes	600000	
Nuevas sesiones / Segundo	20000	
Usuarios concurrentes SSL-VPN	300	
Políticas Firewall	8000	
Dominios Virtuales	10	

ANEXO H

RESUMEN EJECUTIVO DISEÑO CSIRT

OBJETIVO

Crear el modelo de un CSIRT, equipo de respuesta a incidentes de seguridad, que ayude a precautelar la confidencialidad, integridad y disponibilidad de la información en todo momento, en base a investigación continua y a la creación de procesos tanto reactivos como proactivos con el fin de resguardar la seguridad de la red de datos de la Corte Constitucional.

Por esta razón y según el diseño del CSIRT del presente trabajo de investigación, a continuación se detalla la misión y visión propuestas, ya que reforzarán el objetivo de la propuesta:

Misión

Brindar seguridad proactiva a los equipos y aplicaciones en base a investigación continua, con el fin de precautelar los servicios de los usuarios y funcionarios de la Corte Constitucional.

Visión

Ser el punto de partida para que en un futuro se puedan implementar más equipos CSIRTs en las entidades públicas, logrando de esta forma, aumentar la difusión de información entre equipos y disminuir los riesgos de los posibles ataques.

En resumen esto es lo que se desea lograr con el diseño de un equipo de respuesta que siempre esté al tanto de la seguridad de red y de la información que fluye a través de ésta.

SERVICIOS

Los servicios que brindará el desarrollo del equipo de respuesta en la Corte Constitucional podrían ser los siguientes, como se aprecia en la tabla a continuación:

#	Actividades Proactivas	Actividades Reactivas
1	Analizar el soporte de concurrencia de los servidores para evitar ataques de DoS.	Atención a infección de virus en estaciones de trabajo
2	Realizar análisis periódicos de vulnerabilidades, generando alertas sobre los peligros detectados.	Instalación de infraestructura tecnológica para cubrir falencias de seguridad encontrada, como UTMs, Firewalls, etc.
3	Coordinar respuestas y recuperación después de que se presente un posible incidente.	Instalación de equipos de prevención y detección de intrusos a la red.
4	Investigación sobre ataques a otras entidades públicas para prevenir el mismo patrón de amenaza.	Poseer personal para poder reaccionar contra ataques que se presenten en tiempo real
5	Comunicar a los funcionarios sobre los peligros de infección con virus que existen en internet, como publicidad engañosa, correos de destinatarios desconocidos, etc.	Soporte técnico presencial en el momento en que se reporte algún incidente ya sea de un funcionario como de un usuario.

Posibles Metas

Conformar un grupo de respuesta a incidentes que se encargue de analizar, identificar y brindar soluciones proactivas a los incidentes que se presenten en la institución, haciendo uso de políticas y metodologías de resolución de incidentes.

Además de crear conciencia en los diferentes funcionarios acerca de la importancia de implementar un CSIRT.

Resultados que se espera lograr

Equipo de personas capacitado para responder a incidentes, haciendo uso de metodologías para el manejo de incidentes y políticas internas para el grupo.

Reducir el número de posibles ataques y tomar medidas para disminuir el número de vulnerabilidades encontradas.

PUNTOS A TOMAR EN CUENTA PARA UNA POSIBLE IMPLEMENTACIÓN

Hay algunos aspectos que deben ser tomados en cuenta ante una posible implementación del CSIRT, como puede ser:

- Contar con el personal necesario.
- Realizar una correcta definición de riesgos sobre la red.
- Crear una debida retroalimentación y corrección de incidentes detectados
- Realizar una investigación constante de los posibles riesgos y vulnerabilidades que existen en la infraestructura.
- Investigar la resistencia de funcionarios a aprender sobre temas de seguridad de la información.
- Creación de estadísticas y reporte de eventos para informar sobre el funcionamiento del equipo de respuesta.
- Capacitación continua tanto de funcionarios como del personal involucrado.
- Debida creación de políticas y procedimientos de acuerdo a las necesidades de la Corte Constitucional.

Estos serían algunos de los detalles que se deberían tomar en cuenta antes de una implementación dentro de la entidad.

CRONOGRAMA TENTATIVO DE IMPLEMENTACIÓN DEL CSIRT CORTE CONSTITUCIONAL

A continuación en la siguiente tabla se detalla un estimado de tiempo para la implementación del CSIRT de la Corte Constitucional:

Fase del Proyecto	Tarea	Tiempo estimado
Definición Organización	Tipo CSIRT	2 días
	Modelo de estructura	1 semana
	Servicios	2 semanas
Proceso de Planificación	Definición de Políticas y Procedimientos	4 semanas
Ejecución	Comunicación al personal	1 semana
	Puesta en marcha de nuevas políticas y procedimientos	1 semana
Cierre	Presentación formal del CSIRT Corte Constitucional	1 día
	Realizar pruebas de estabilización	2 semanas