# ANÁLISIS DE SEGURIDAD A LA RED DE DATOS DE LA EMPRESA ASISTIR COMPUTADORES DE LA CIUDAD DE BOGOTÁ

RAÚL GARCÍA GUACANEME

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA D.C.

2017

# ANÁLISIS DE SEGURIDAD A LA RED DE DATOS DE LA EMPRESA ASISTIR COMPUTADORES DE LA CIUDAD DE BOGOTÁ

RAÚL GARCIA GUACANEME

Trabajo de grado para optar por el título:

Especialista En Seguridad Informática

Directora de Proyecto:
Ing. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C

2017

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C, 24 de Julio de 2017

Dedico de manera especial este trabajo de grado de especialización, a mi familia, ya que gracias a su apoyo he logrado culminar este proyecto con éxito.

**AGRADECIMIENTOS**

A los tutores y profesores de la Universidad que me brindaron su constante guía para el desarrollo de este proyecto.

**CONTENIDO**

Pág.

## LISTA DE FIGURAS

Pág.

## LISTA DE ANEXOS

Pág.

# INTRODUCCIÓN

El Crecimiento de las Telecomunicaciones, el auge de internet y todo lo que tiene que ver con el manejo de datos en la red, han tenido un constante desarrollo significativo en la actualidad, provocando la aparición de vulnerabilidades y además poniendo en riesgo la información sensible de la organización.

Para que la entidad controle estas vulnerabilidades es necesario tener como base muchos de los conceptos de seguridad informática en redes de telecomunicaciones. Es por ello que el tema de seguridad se debe asimilar como un engranaje en el que intervienen todas las áreas de la organización, para así lograr proteger adecuadamente la integridad de la información y la privacidad de los datos.

Por esta razón se realizó un análisis de seguridad a la red de datos de la empresa ASISTIR COMPUTADORES para detectar vulnerabilidades, tanto en el exterior como en el interior de la entidad, para evitar cualquier robo o pérdida de información.

# 1 DESCRIPCIÓN DEL PROBLEMA

La empresa ASISTIR COMPUTADORES ha experimentado transformaciones en algunos aspectos de seguridad informática, en la actualidad los sistemas informáticos son el activo más valioso y al mismo tiempo el más vulnerable de la empresa, el cual puede ser accedido por personal no autorizado para modificar o hurtar su información.

Debido a que posiblemente la red está expuesta a riesgos que se pueden materializar por las vulnerabilidades de los sistemas de red y además teniendo en cuenta que la empresa ASISTIR COMPUTADORES no conoce el estado de seguridad de la red de datos porque a la fecha no han realizado un análisis de esta, les preocupa que puedan sufrir daños que tengan un impacto económico, a su imagen o que afecten la confidencialidad, integridad y disponibilidad de la información y los servicios.

La empresa invierte poco en la parte de seguridad informática en sus sistemas de red para prevenir el daño y pérdida de la información confidencial, a raíz de ello han surgido muchos problemas relacionados con el aumento de tecnología en la empresa, la cual cuenta con un mayor número de dispositivos conectados a internet y a redes locales empresariales, esta proliferación de conexiones le está representando un riesgo de seguridad para la empresa, teniendo en cuenta que en la mayoría de los casos los dispositivos que se conectan no son configurados adecuadamente, por tal motivo se realizaron pruebas de seguridad a la red para que la empresa tome las medidas necesarias.

## 1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es el estado de seguridad de la red de datos de la empresa ASISTIR COMPUTADORES?

## 1.3 OBJETIVOS

### 1.3.1 Objetivo general

Realizar un análisis de seguridad a la red de datos de la empresa ASISTIR COMPUTADORES de la ciudad de Bogotá, para conocer el estado de la red y realizar las recomendaciones de mejora pertinentes.

### 1.3.2 Objetivos específicos

• Levantar información pertinente que sirva de insumo para llevar a cabo la ejecución del presente proyecto.

• Identificar los activos de información que conforman la red de datos de ASISTIR COMPUTADORES.

• Instalar herramientas de gestión de seguridad y realizar las pruebas de detección de vulnerabilidades acordadas.

• Realizar el informe sobre las vulnerabilidades encontradas y las recomendaciones de mejora relacionadas con la seguridad de información de la red para la empresa ASISTIR COMPUTADORES.

## 1.4 JUSTIFICACION

El proyecto se desarrolló en la empresa ASISTIR COMPUTADORES, con una de sus sedes ubicada en la ciudad de Bogotá, consultora e interventora de sistemas de información desarrollados bajo plataformas tecnológicas que involucra el uso de hardware, software y módulos de integración. En la empresa se realizaron entrevistas y charlas a los empleados, dando como resultado el poco conocimiento por parte de ellos a nivel de seguridad informática y sus implicaciones.

Se realizaron pruebas al esquema de seguridad de la red de datos de la organización, para comprobar si es posible penetrar los sistemas de seguridad implementados por la entidad, por personal no autorizado, tanto interno como externo, que puedan ocasionar daños, robó y sustracción de la información confidencial al interior de la entidad.

La empresa tiene una proyección de crecimiento alto en cuanto a infraestructura, dicho crecimiento ha creado necesidades de mejorar la seguridad de la red, lo cual conlleva necesariamente a que actualicé y difunda a sus empleados la importancia de la seguridad en sus sistemas de red para que no se presenten vulnerabilidades informáticas. Con el fin de asegurar la autenticidad y seguridad de la información, al igual que garantizar la confiabilidad y control de acceso a la información suministrada, la empresa debe implementar las recomendaciones y las nuevas políticas de seguridad que se encontraron con las pruebas realizadas durante la investigación del proyecto, si así lo considera para mejorar la seguridad en su sistema de red.

La empresa puede conocer los riesgos informáticos a los que está expuesta su información y puede minimizarlos o controlarlos mediante una metodología definida y documentada, que se puede revisar y mejorar constantemente, con esta información la empresa identifica fácilmente los dispositivos conectados a sus redes que cuentan con la vulnerabilidad, los cuales constituyen un riesgo potencial para la seguridad de la red y la información que en ella circula.

La seguridad informática juega un papel muy determinante en la organización, por lo cual, es importante realizar periódicamente unas buenas prácticas en el diseño e implementación de protocolos de seguridad, para así mantener un alto estándar de protección de la información.

# 2 MARCO REFERENCIAL

## 2.1 ANTECEDENTES

La preocupación interna de la compañía en proteger la información, la cual cobra fuerza debido al creciente desarrollo tecnológico, dadas las cambiantes condiciones y las nuevas plataformas de sistematización disponibles que posibilitan interconectarse a través de redes.

Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas de información de la empresa. Por ello se hace más necesario proteger la información relevante de la compañía, para lo cual debe estar sincronizado, armonizado y con un plan de seguridad entre los procesos de una compañía con el fin de brindar confianza.

La Seguridad Informática (IT Security) se describe como la distinción táctica y operacional de la Seguridad, es decir, es la forma como se detallan las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos.[1]

Los funcionarios y empleados deben tener claro en qué consisten los atributos de seguridad informática como:

- ✓ **La integridad:** garantizara que los datos sean los reales y que el activo no ha sido alterado de manera no autorizada.
- ✓ **Confidencialidad:** garantizara que la información sea accedida solo por personal debidamente autorizado y tengan acceso a los recursos que se intercambian.
- ✓ **Disponibilidad:** garantizara que la información siempre esté disponible para el usuario que lo requiere.
- ✓ **Privacidad:** los componentes del sistema son accesibles solo para el personal debidamente autorizado.

---

[1] J. J. Cano, "La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes," ISACA Journal Online, vol. 5, 2011

- ✓ **No repudio,** garantizara de que no puedan negar una operación realizada o no pueda alegar desconocer el hecho.
- ✓ **Política de Autenticación:** asegurar que el acceso a los recursos del sistema informático, solo se realice por personal autorizado y asegura el origen y destino de la información.
- ✓ **Control:** asegurar su conformidad con la estructura de seguridad informática y procedimientos establecidos por la compañía en cuanto al acceso a la información y el monitoreo de los usuarios autorizados.

**2.1.1 Sistema de Gestión de la Seguridad de la información**. El Sistema de Gestión de la Seguridad de la Información (SGSI) es la herramienta estratégica que ayuda a la compañía a implementar políticas de seguridad informática, procedimientos y controles de seguridad informática alineados con los objetivos del negocio, con el fin de evaluar y tener una visión global sobre el estado de los riesgos y estos sean conocidos, asumidos, minimizados y gestionados por la compañía de una forma documentada, eficiente y adaptada a los cambios que se produzcan en la compañía, en cuanto a los riesgos, el entorno y las tecnologías a lo largo del tiempo.

El SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.[2]

Los factores que se deben tener en cuenta para el sistema de gestión de la seguridad de la información de la empresa son:

- **Compromiso de la alta dirección.** Para que la iniciativa entregue los resultados esperados es un requisito necesario el apoyo e involucramiento de la alta dirección, sin su apoyo formal real es casi imposible desarrollarlo y demostrar el logro de la conformidad en la implementación del SGSI. Aquellos proyectos que provienen de los sectores operativos o tácticos y no cuentan con el respaldo de la alta dirección tienen mayor posibilidad de fracaso.

- **Cada organización es un mundo diferente.** Aun perteneciendo al mismo sector económico o a un mismo grupo empresarial, cada empresa tiene su ambiente de control y un riesgo de seguridad de la información particular. Lo que es bueno para una, puede que no lo sea para otra, por ello copiar tal cual no es procedente. Se

---

[2] WWW.ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, Madrid, 2012.

debe considerar un entendimiento de los requerimientos de seguridad y gestión de riesgos de cada organización.

- **Definición apropiada del alcance**. Es importante definir un alcance del SGSI que sea viable. El esfuerzo para implementar el sistema de gestión no es el mismo cuando el alcance incluye todos los procesos de la organización, a uno que incluya sólo uno o dos procesos relevantes. En este sentido es mejor iniciar con pocos procesos y paulatinamente ir creciendo la cobertura del SGSI, a medida que se obtiene mayor madurez en seguridad de la información.

- **El SGSI es de la empresa**. En ocasiones, las organizaciones contratan el servicio de consultoría para apoyar la definición y puesta en marcha del sistema de gestión, cometiendo el error de delegar todo el trabajo al grupo consultor sin involucrarse en el desarrollo del proyecto. Debemos tener en cuenta que el SGSI no es de la consultora, es de la organización. La consultora algún día se irá, y si la organización no se compromete desde el inicio del proyecto no aprenderá a implementar y mantener adecuadamente su sistema de gestión. En muchos casos las empresas consultoras entregan a los clientes manuales, procedimientos, formatos, etcétera, y el cliente no sabe cómo aplicarlos.

- **Evaluar el desempeño.** Una forma de saber si el SGSI está operando adecuadamente, no es a través del uso de métricas e indicadores, es aplicable también a un sistema de gestión. Luego entonces, hay que definir métricas e indicadores relevantes.

- **Sensibilicemos.** En la implementación del SGSI no debemos dejar de lado el recurso humano y sus responsabilidades frente a la seguridad de la información. A los empleados, se puede llegar a través de diversos medios para sensibilizarlos: por medio de afiches, pendones, protectores de pantalla, videos, juegos, obras de teatro, entre otros.

- **Importante es llegar, pero mantenerse también**. La definición e implementación de la Norma ISO-27001 no es el fin, es apenas el inicio de un largo y sinuoso camino por la seguridad de la información. Recordemos que un SGSI debe operarse día a día, no una semana antes de la auditoría de certificación o mantenimiento. El sistema debe ser sostenible en el tiempo y eso se logra solamente con el involucramiento del personal y su operación diaria.

- **Mejora continua**. Si se hace adecuadamente, se realimenta y hace que el SGSI se nutra y enriquezca. Es vital establecer acciones correctivas y preventivas para que el sistema reaccione ante eventos desfavorables y evolucione hacia una mayor eficacia.

- **Automatización del SGSI**. Tradicionalmente estas iniciativas se ejecutan con el apoyo de herramientas de ofimática. El uso de una herramienta automatizada que cubra todo el ciclo de vida del SGSI (planear-hacer-verificar-actuar) sin lugar a dudas ha sido factor crítico de éxito, ya que ha reducido la duración de las actividades de inventario de activos, gestión de riesgos y establecimiento de métricas e indicadores. Además, ha permitido que la empresa se involucre directamente en el uso de la herramienta conservando todos los registros y documentos del SGSI en un solo repositorio de información y, sobre todo, le ha permitido dar sostenibilidad al SGSI, sin dependencia directa del equipo de consultoría.

  La seguridad informática, surge como una herramienta organizacional que propende entre otras cosas por crear conciencia en los integrantes de la organización, de los peligros latentes e inherentes a todo sistema de información, los datos del sistema y los medios que se involucran para la transmisión y gestión en general de esa información.

  Los planes de seguridad, tienen que estar soportados por políticas, procedimientos y documentos que indiquen:

1. El por qué se debe proteger un recurso
2. Que se puede hacer para protegerlo
3. Las actividades que se deben llevar a cabo para lograr dicha protección.
   El Sistema de Gestión de Seguridad de la Información (SGSI), debe soportarse en un proceso sistémico y conocido por la totalidad de los integrantes de la organización y ser análogo a un sistema de calidad para la seguridad de la información.

**Seguridad de la información y seguridad informática**

Al involucrarse la empresa en el mundo de la ISO 27000, una de las situaciones más recurrentes se presenta cuando se trata de diferenciar seguridad informática con seguridad de la información. Aunque su significado e implicaciones no es el mismo, ambas persiguen un fin común: proteger la información; pero lo hacen de manera diferente.

- Seguridad Informática:

  Se centra en proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de la empresa, se centra básicamente en hardware y software, y que estas sean utilizadas de la manera indicada por la Organización.

  Su análisis de riesgos se centra en vulnerabilidades del hardware o software, y llevar el nivel de riesgo a nivel aceptable por la organización.

- Seguridad de la Información:

  La seguridad de la información tiene como propósito proteger la información de la Organización, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen.
  La Seguridad de la Información tiene tres principios fundamentales: Confidencialidad, Integridad y Disponibilidad de la información.
  Su radio de acción cubre Análisis de Riesgos, Seguridad del Personal, Seguridad física y del entorno, Gestión de comunicaciones, Desarrollo y Mantenimiento de Sistemas, Control de Accesos, Gestión de Incidentes, y Continuidad de Negocio entre otros (de acuerdo a la ISO 27000)

  Busca mantener el riesgo en la gestión de la información por debajo del nivel asumible por la propia organización. Todas las áreas se encuentran dentro del alcance de la seguridad de la información de acuerdo a la ISO 27000.

  **2.1.2 Seguridad informática en la bases de datos.** La seguridad informática en la base de datos es crítica, debido a que se podría considerar como la caja fuerte de la compañía, en donde la mayoría de la información es sensible y de mucha importancia por guardarse las transacciones de la compañía. La base de datos de la empresa es la recopilación de información sobre diversos aspectos tales como: personas, productos, pedidos, contabilidad, transacciones, etc. Por lo cual se debe contemplar un buen plan de seguridad informática para que sea efectiva, para ello necesita contar con elementos indispensables de apoyo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas.

  La gran mayoría de los datos sensibles de la organización están almacenados en sistemas gestores de bases de datos comerciales tales como Oracle, Microsoft SQL Server entre otros, y atacar una bases de datos es uno de los objetivos favoritos para los criminales.

  Esto puede explicar por qué los ataques externos, tales como inyección de SQL, están subiendo año tras año. Esta tendencia es prueba adicional de que los agresores tienen éxito en hospedar páginas Web maliciosas, y de que las vulnerabilidades y explotación en relación a los navegadores Web están conformando un beneficio importante para ellos. La atención generalmente se ha centrado en asegurar los perímetros de las redes por medio de, firewalls, IDS / IPS y antivirus, cada vez más las organizaciones se están enfocando en

la seguridad de las bases de datos con datos críticos, protegiéndolos de intrusiones y cambios no autorizados.

**2.1.3 Seguridad informática en la red.** La Seguridad informática en la red, surgido de la integración de las tecnologías de las comunicaciones y la computación, propiciado por el rápido desarrollo de las tecnologías de la información y con ello el tema de seguridad informática de las redes de comunicación que permiten el funcionamiento armónico de diferentes procesos de los sitios de trabajo.

Los principales aspectos de seguridad informática en la red son: disponibilidad, desempeño, confidencialidad, integridad y control de acceso físico y lógico, considerando junto a los componentes de la red como: Switches, Routers, firewall, IPS/IDS, Gateway Antivirus, etc. Que combinados e integrados de una forma estratégica y efectiva aseguran la red y por ende la seguridad de la información.

La seguridad informática de la red es una responsabilidad de los administradores, de mantener actualizada las aplicaciones, el equipo de trabajo incluido el usuario final, actualización de Antivirus y configuración correcta del sistema operativo, por el cual se puede dejar el sistema vulnerable a cualquier intruso. Porque si identificamos quién tienen acceso a las bases de datos, podemos determinar el riesgo de los datos, al sufrir un daño causado por un acceso no autorizado.

Uno de los aspectos a los que hay que prestar atención al crear una red informática en la empresa es la seguridad. Debemos tener en cuenta que va a haber diferentes dispositivos interconectados. Un problema de seguridad en uno de los dispositivos podría afectar a los demás, como cuando un programa malicioso se propaga o un software espía obtiene datos de nuestros servidores para utilizarlos a su favor.

Por tanto, hemos de preocuparnos por mejorar la seguridad de nuestras redes informáticas, y no nos referimos sólo a las redes inalámbricas, sino al conjunto de nodos que conforman una red y están compartiendo información entre sí.

**Combatiendo la aparición de intrusos en la red informática**

En las redes inalámbricas es donde más comúnmente puede aparecer un intruso que nos resta velocidad y ancho de banda, ya que ha logrado conectarse o deshabilitar nuestra red Wifi. Sin embargo, en las redes por cable también pueden producirse intrusiones a través de distintos malware.

Por ejemplo, si instalamos algún tipo de software espía en uno de los ordenadores del sistema, puede que no sólo se monitorice la actividad de ese sistema, sino del conjunto de los dispositivos conectados a la red. Por tanto, deberemos proteger cada uno de los equipos de la red informática de todo ataque informático, utilizando un buen firewall, cortafuegos y un antivirus.

**Copias de seguridad centralizadas**

En las redes informáticas es conveniente que nuestra estrategia y planificación de copias de seguridad se encuentre centralizada. De lo contrario, tendríamos que llevar un control exhaustivo de las copias de cada uno de los equipos, lo que a veces conllevaría además una duplicación innecesaria de programas o archivos de uso común en la red.

Es conveniente, por tanto, que se hagan copias de seguridad periódicas, que no ocupen demasiado espacio y que estén centralizadas en un mismo espacio. Como complemento de seguridad, se puede crear redundancia teniendo la última copia de seguridad en un espacio completamente ajeno a la red informática.

**Manteniendo los equipos actualizados**

Un gran error es no prestar el debido mantenimiento informático a cada uno de los equipos que forman parte de la red. El paso del tiempo favorece que el software se quede antiguo y se detecten nuevas vulnerabilidades o agujeros de seguridad, tanto en el sistema operativo, los programas, los navegadores, etc.

La falta de actualización de los equipos en las redes informáticas, aparte de resultar incómodo a la larga para los usuarios, aumenta las probabilidades de infección y propagación de virus en nuestros ordenadores.

El Uso de herramientas que comprometen la seguridad. Hacer o intentar hacer, sin permiso del dueño o del anfitrión del sistema o de la Dirección de Gestión de Tecnología, cualquiera de los siguientes actos:

- Acceder al sistema o red.
- Monitorear datos.
- Sondear, copiar, probar firewalls o herramientas de hacking.
- Atentar contra la vulnerabilidad del sistema, redes.
- Violar las medidas de seguridad, las rutinas de autenticación del sistema o de la red.

Gracias al avance vertiginoso de la tecnología, con el objeto de brindar eficiencia y agilizar la administración y los procesos, se incorporan sistemas automatizados de procesamiento de información. Las organizaciones se ven expuestas a una serie de peligros, que se han incrementado por las nuevas amenazas surgidas por uso de las tecnologías de la información y las comunicaciones.[3]

**2.1.4 Identificación de activos.** El objetivo de la empresa es buscar Estrategias de Seguridad para proteger la Información y los activos de información. En la actualidad, las actividades, servicios o procesos del negocio desarrollados, dependen de la información y los medios empleados para su procesamiento, almacenamiento o trasmisión y cuando uno falla, supone un impacto en las actividades de la empresa.

El modelo de análisis y gestión de vulnerabilidades tiene como objetivo identificar los riesgos a los que se encuentran sometidos los activos de información, para ello debe realizarse un inventario de los servicios de seguridad informática, los procesos implicados y los activos de información que dan soporte a dichos procesos, de forma que la empresa pueda priorizar los mismos y adoptar las medidas adecuadas para protegerlos de acuerdo al mapa de activos sobre el cual se desarrollará el posterior análisis de riesgos.

La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad, con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la compañía, la información deberá estar clasificada como secreta, restringida o general. La información secreta y restringida debe estar soportada por un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros.

Para asegurar que los activos de información reciban el nivel de protección adecuado, la Dirección de Gestión de Tecnología es responsable de definir la metodología de clasificación de activos de información, estos se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de los mismos.

---

[3] Universidad Nacional de Luján, "seguridadinformatica," [Online]. Available: http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf. [Accessed Marzo 2016].

Todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de la organización, son responsables de cumplir y acoger con integridad la Política de Uso Aceptable para dar un uso racional y eficiente los recursos asignados.

El hardware, software y periféricos, así como la información en él contenida es propiedad de la empresa y su uso está restringido únicamente para propósitos de su negocio, reservándose el derecho de monitorearlo en cualquier momento. Cualquier utilización, modificación o acceso no autorizado a este sistema dará lugar a las acciones disciplinarias y/o legales que correspondan.

**2.1.5 Plan de Contingencia.** El plan de contingencia es un procedimiento alternativo para el desarrollo normal de las actividades de la empresa, aunque algunas de sus funciones se hubiesen dañado por accidentes internos o externos, tener un plan de contingencia no significa que reconozca la ineficiencia de la compañía, por el contrario es estar preparados, para superar cualquier eventualidad que pueda acarrear pérdidas materiales, de información y personales, con el fin de hacer frente a futuros acontecimientos para lo cual se debe estar preparados con el único fin de dar continuidad a las actividades de la empresa.

Para la elaboración de un buen Plan de Contingencia se debe dividir en cuatro etapas, las tres primeras hacen referencia al componente preventivo y la última a la ejecución del plan una vez ocurrido el siniestro.

**Evaluación.** Los responsables de la Planificación, deben evaluar constantemente los planes creados, del mismo modo deberán pensar en otras situaciones que se puedan presentar.

**Planificación.** Teniendo en cuenta la probabilidad y el impacto de los riesgos existentes en la compañía, los cuales pueden causar un siniestro, sirviendo este como punto de partida para planificar las respuestas en caso de emergencia, se debe trabajar con hipótesis y desarrollar los posibles escenarios de solucionar la emergencia.

**Pruebas de viabilidad.** Se trata de demostrar cada uno de los procedimientos que se están utilizando que estén completos y de acuerdo a lo establecido, los recursos materiales están disponibles, para cuando estos se vayan a utilizar; las copias sean actualizadas y estén disponibles, y cada uno de los empleados participantes del grupo se encuentren preparados. Además, se debe documentar cada una de las pruebas que se realice y se tenga planeado, determinar el procedimiento de cada prueba, ejecutar cada una de las pruebas documentadas en base a los resultados

obtenidos, actualizar el plan de contingencia de acuerdo a los procedimientos y calendarios de mantenimiento establecidos.

**Ejecución.** Cuando un siniestro se materializa, el grupo de contingencia, debe realizar el plan de contingencia diseñado y los procesos planeados y validados, dando respuesta inmediata para dar continuidad a los servicios informáticos.

## 2.2 MARCO TEÓRICO CONCEPTUAL

• Seguridad informática: Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable.

• Seguridad de la información: Es un término que hace referencia a la seguridad de activos de forma general, incluyendo la seguridad informática, la seguridad TIC y la seguridad de los datos. Además la Seguridad de la Información (Information Security) es la línea estratégica de la Seguridad , La seguridad de la información es la disciplina que nos habla de los riesgos, de las amenazas de los esquemas normativos para minimizar los riesgos en el manejo de los activos, es decir information Security sería, la disciplina que se encargaría de proporcionar evaluar el riesgos y las amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo normativa o buenas practicas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad en el manejo de la información (activos).[4]

• Seguridad Pasiva: Son el conjunto de medidas o estrategias que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema.

• Seguridad Activa: Son todas las acciones enfocadas a prevenir y detectar los riesgos para la seguridad de la información.

• Seguridad Lógica: Su enfoque se fundamenta en las estrategias encaminadas a proteger los programas (Software), de un sistema informático.

• Información: Es el conjunto organizado de datos procesados que constituyen un mensaje ya sea a nivel impreso, almacenada digitalmente.

---

[4] J. J. Cano, "La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes," ISACA Journal Online, vol. 5, 2011.

En la actualidad la información es considerada como uno de los activos más importantes dentro de las compañías, y de vital importancia su protección.

• Riesgo: Se define como cualquier impedimento, obstáculo, amenaza que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia.

• Políticas de Seguridad: Buscan establecer las reglas para proporcionar los lineamientos generales y el soporte para la seguridad de la información, se constituye en uno de los ejes principales del SGSI.

• Usuario: Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por las empresas, ya sean equipos de cómputo, redes de comunicación, teléfonos, etc.

## 2.3 MARCO CONTEXTUAL

**2.3.1 Descripción de la Empresa.** Es una de las firmas líderes, trabaja con los sectores público y privado, a través del suministro de soluciones integradas en ingeniería. Así mismo, provee servicios de consultoría a clientes en las áreas de tecnología, energía, infraestructura, servicios ambientales, edificaciones, minería, transporte, telecomunicaciones e hidrocarburos, presta servicios para transformar el entorno y restaurar el medio ambiente.

Su experiencia abarca desde la mitigación de impactos ambientales en proyectos de infraestructura, hasta la planificación urbana, la ingeniería de edificios emblemáticos, el diseño de redes de transporte sostenible y el desarrollo de fuentes de energía para el futuro.

Tiene una planta de empleados de ingenieros, técnicos, científicos, arquitectos, planificadores, inspectores, profesionales en gestión de la construcción y de proyectos tecnológicos, así como diversos expertos en medio ambiente en una sede ubicada en la ciudad de Bogotá.

**2.3.2 Misión.** Desarrollar, impulsar y continuar ofreciendo soluciones de nuevos proyectos para que la empresa continúe como una de las principales líderes en soluciones de tecnología de comunicaciones.

**2.3.3 Visión.** Ser siempre la primera opción para los clientes, asociados y empleados. Miramos constantemente hacia adelante, para prever y responder a los cambios con agilidad. Solucionamos problemas, exploramos nuevas ideas y procuramos siempre encontrar la solución ideal. Además, desafiamos lo ya establecido, pensamos de manera no convencional y aprendemos de nuestras experiencias. Nosotros impulsamos y valoramos la toma de iniciativas bien sustentadas.

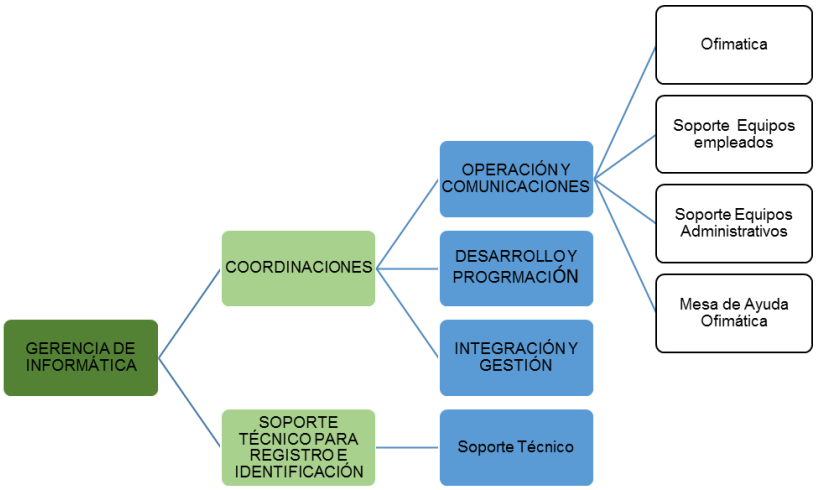
**2.3.4 Valores.**

- Serviciales
- Confiables
- Solidarios
- Apasionados
- Innovadores

**2.3.5 Propósito.** Trabajar en equipo para suministrar soluciones más efectivas y sostenibles a nuestros clientes. Nuestros valores nos sirven de soporte y crean un entorno donde nuestro capital humano puede desarrollarse.

**2.3.6 Organigrama.** En la siguiente figura se observa el organigrama del área de tecnología.

Figura 1. Organigrama del área de tecnología

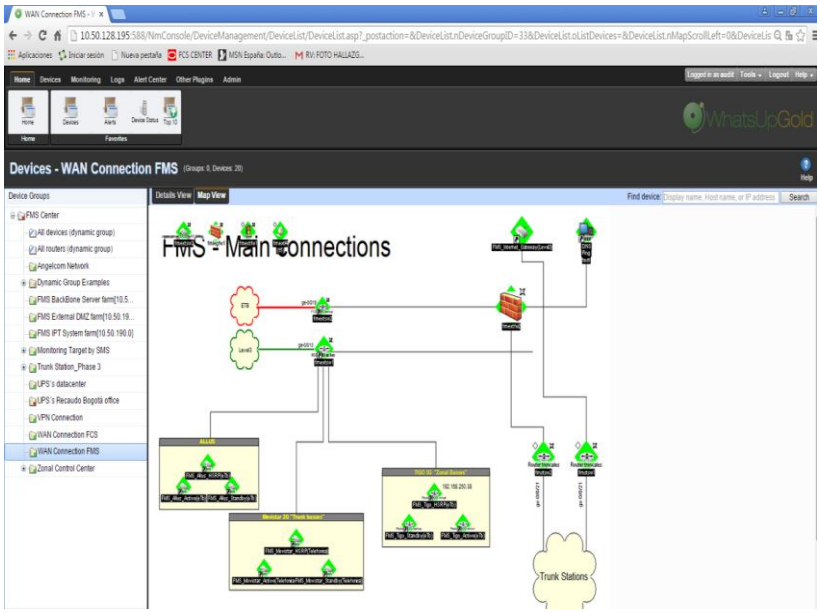



Fuente: El autor

**2.3.7 Mapa de red.** En el plan de configuración se propone una VPN/Firewall para prevenir que los usuarios no autorizados conectados a la intranet accedan a los sistemas centrales, para poder garantizar la comunicación segura entre los sistemas centrales con los demás sistemas del ambiente. A continuación se menciona el plan básico de configuración de VPN/Firewall:

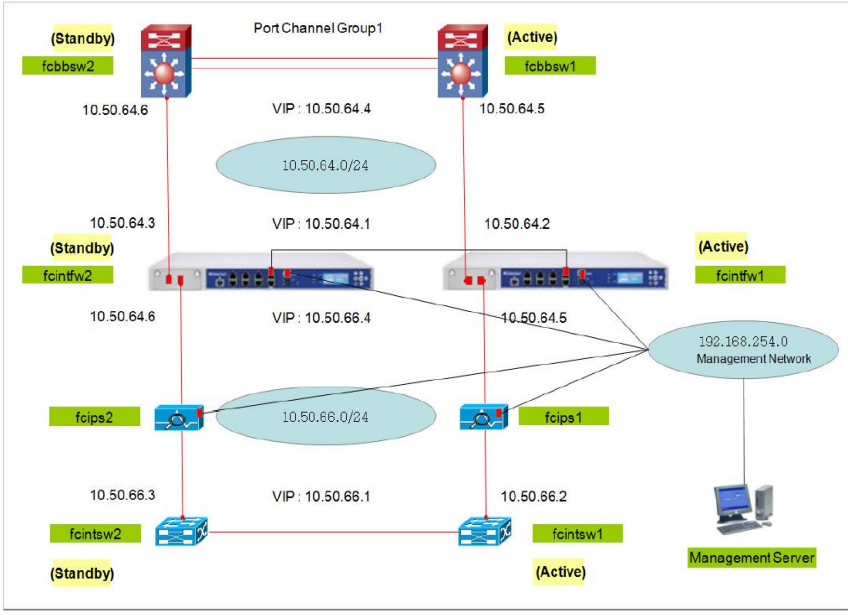
- Configuración de la VPN/firewall que restrinja las conexiones entre las redes en las que no haya confianza y cualquier componente de los sistemas del ambiente de datos.
- El tráfico de entrada y salida que esté restringido y autorizado, así como el tráfico alterno se podrá negar. Prohibir directamente el acceso público entre la Internet y cualquier componente del sistema en el ambiente de datos.
- Implementar el DMZ para limitar el tráfico de ingreso y salida únicamente a protocolos que se necesiten en el ambiente de datos.
- El firewall respalda las fallas sin cerrar las sesiones y filtra los paquetes según las políticas.
- La conexión LAN - LAN y la VPN cliente se pueden respaldar mediante el sistema central y el sistema de la sub-red, como se observa en las Figuras.

Figura 2. Sistema de red




Fuente: El autor

Figura 3. Configuración del firewall VPN.




Fuente: El autor

Los indicadores de confiabilidad y disponibilidad de los equipos que se pueden monitorear del sistema de comunicaciones de la empresa, son un buen indicativo de la seguridad en la transmisión de datos, garantizando que la información recibida es idéntica a la enviada.

## 2.4 MARCO LEGAL

La normatividad vigente en Colombia en las que se enmarcan las obligaciones que debe cumplir la empresa en referencia a delitos informáticos, protección de la información, modificación y robo de información es un hecho penalmente castigable por la ley colombiana, este proyecto se enmarcar en las siguientes regulaciones:

- Ley 1273 de 2009: Modifica el código penal en relación con la seguridad de la información y delitos informáticos. En ella se clasifican los atentados contra la confidencialidad, integridad y disponibilidad de los datos y sistemas de información, los atentados informáticos y otras infracciones.[5]

Haciendo especial énfasis en los siguientes artículos:

Artículo 269A (Acceso abusivo a un sistema informático), dado que el sistema de información de una empresa puede ser accedido sin autorización.

Artículo 269C (Interceptación de datos informáticos), en el caso que la comunicación de la red de la empresa sea interceptada para extraer información.

Artículo 269F (Violación de datos personales), en la situación que la información personal de los clientes sea divulgada sin autorización del mismo.

Artículo 269G (Suplantación de sitios web para capturar datos personales), para el caso de los ataque conocidos como Phishing donde una página impostora engaña al cliente presentándose como un portal web original.

- Ley 527 de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales, y establece las entidades de certificación.[6]

- Ley 1581 de 2012: La ley de protección de datos personales, complementa la regulación vigente para la protección del derecho fundamental que tienen todas

---

[5] EL CONGRESO DE COLOMBIA, "Alcaldia Bogotá," 2009. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [Accessed 2016].

[6] E. C. d. Colombia, "alcaldiabogot," 1999. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. [Accessed 2016].

las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.[7]

[7] EL CONGRESO DE COLOMBIA, "alcaldiabogotá," 2012. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Accessed 2016].

# 3 METODOLOGIA

## 3.1 METODOLOGÍA DE INVESTIGACIÓN

Se realizaron pruebas en sitio en la empresa, detectándose que los procedimientos de identificación y autenticación de usuarios a las terminales establecidas por la empresa no son suficientes, se identificaron vulnerabilidades que se notificaron a la empresa para que tome las medidas necesarias.

Se verificaron las políticas de seguridad implementadas por la organización para el acceso a las terminales, se identificaron algunos riesgos a las que están expuestas las terminales, además se comprobó que hay la necesidad de implementar nuevas políticas de seguridad al interior de la entidad.

Las políticas de seguridad implementadas, garantizan en gran medida la seguridad en la transmisión de datos. En la empresa se verifico la seguridad de la red implementada y se notificó a la entidad de las vulnerabilidades que se encontraron para mejorar su seguridad.

Durante la fase de desarrollo del proyecto, se identificaron algunas vulnerabilidades a las que está expuesta la red, en gran medida cuenta con dispositivos de seguridad adecuados.

## 3.2 METODOLOGÍA DE DESARROLLO

La metodología para el proyecto es la siguiente.

### Levantamiento de información

A los funcionarios y empleados se les realizaron entrevistas, charlas, reuniones etc., a fin de establecer como utilizan los equipos, contraseñas, periféricos, software, etc., asignado a cada empleado, identificando las vulnerabilidades informáticas.

### Identificación de activos

Se identificaron para valorar el grado de vulnerabilidad a la cual están expuestos los activos.

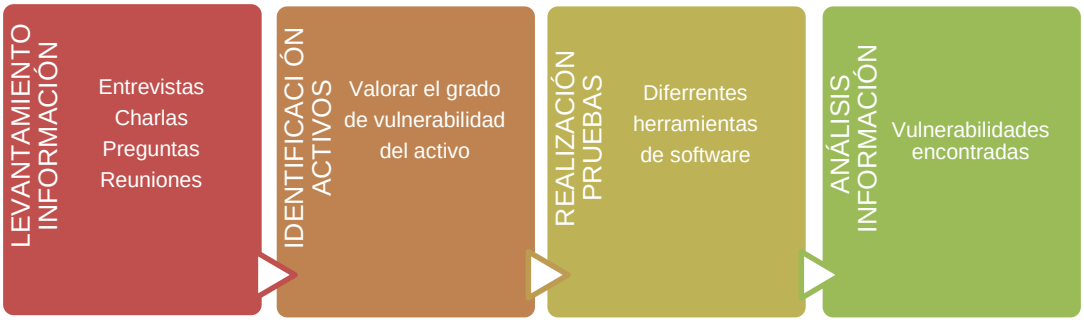
**Realización de  pruebas**

Se realizaron pruebas de vulnerabilidad con diferentes herramientas de software a la red de la entidad para identificar los riesgos informáticos.

**Análisis de la información**

Se entregó a la entidad en un informe de las recomendaciones y vulnerabilidades encontradas en la red, a fin de mejorar su seguridad.

Figura  4. Metodología de desarrollo




Fuente: El autor

En la figura se describe la metodología de desarrollo para el análisis de la red de datos de la organización.

# 4 RESULTADOS

## 4.1 IDENTIFICACIÓN DE LA INFORMACIÓN PARA EL DESARROLLO DEL PROYECTO

Se realizaron entrevistas, charlas, reuniones e inspección visual en los puestos de trabajo con los ingenieros que administra la red y demás personal de la empresa para identificar las posibles vulnerabilidades a las que esta es puesta la red de datos de la organización.

Además se identificaron algunas de las políticas de seguridad:

1. Seguridad de la Información: realiza la creación de usuarios donde se definen las acciones permitidas para cada usuario, tipo de acceso a que objetos y sobre que esquema.

2. Seguridad de Usuarios: Cada usuario tiene un nombre de usuario definido, con rol y/o perfil específico definido para cada sistema. De acuerdo al rol y/o perfil de cada usuario se asigna la respectiva política a regir en él; Cada usuario es responsable de su contraseña ya que esta es personal e intransferible.

   Los usuarios están divididos en los siguientes grupos:

- Usuario de Consulta.
- Usuario Administrado.
- Usuario Desarrollador – Pruebas.

3. Listado de usuarios con su respectivo estado, rol y permisos asignados.

4. Administración de Contraseñas: Para la asignación de usuarios y contraseñas tiene un procedimiento general, donde el jefe de área tiene conocimiento de todo el personal con perfil.

## 4.2 IDENTIFICACION DE LOS ACTIVOS DE INFORMACIÓN QUE CONFORMAN LA RED DE DATOS DE LA EMPRESA.

En Bogotá se encuentra una de las sedes administrativas, en la cual se encuentra una oficina para el departamento de sistemas y de seguridad informática, encargada de mantener el sistema de red funcionando, en ella se identificaron los activos de información de la red de datos de la entidad.

### Identificación de activos de información

Activos de información

| ACTIVO | TIPO DE ACTIVO |
|---|---|
| Terminales de usuario | Hardware |
| Base de datos | Software |
| Portátiles | Hardware |
| Puestos de trabajo | Hardware |
| Router | Red |
| Servidores | Hardware |
| Swicth | Red |
| Funcionarios y empleados | Personal |
| Anti virus | Software |
| Módems | Hardware |
| Fuentes de alimentación | Hardware |
| Programas de aplicación | Software |

Fuente: Autor del proyecto

## 4.3 HERRAMIENTAS DE SOFTWARE UTILIZADAS PARA EL ANALISIS DE LA RED DE DATOS

### 4.3.1 HERRAMIENTAS DE SOFTWARE UTILIZADAS

Para la realización de las pruebas de seguridad se utilizaron las siguientes herramientas:

**Herramienta WhatsUp Gold**: Es una poderosa herramienta de monitoreo de redes, servicios, servidores y aplicaciones.

**Herramienta de gestión OTRS**: Es una herramienta de gestión integral de TI, en la cual la información y los datos se almacenan de forma segura.

**Herramientas de software Pentesting**: Es una herramienta que sirve para evaluar la seguridad de las redes, sistemas de computación y aplicaciones involucradas en los mismos, para poder descubrir las vulnerabilidades en el sistema estudiado.

**Suite de Backtrack**; Es una extensión de Linux que sirve para realizar un test de seguridad a los sistema.as de red para descubrir las vulnerabilidades.

**Programa NMAP**: Es un software de uso libre de código abierto que se utiliza para detectar puertos abiertos.

**Herramienta Hydra**: Permite realizar ataques para intentar adivinar las contraseñas, la cual funciona en paralelo con soporte de diversos protocolos. Actualmente soporta Asterisk, Cisco auth, FTP, HTTP, IMAP, MS-SQL, MYSQL.

**Herramienta SQLMAP**: Esta herramienta se utiliza en inyección de SQL, para obtener listas y registros de las bases de datos.

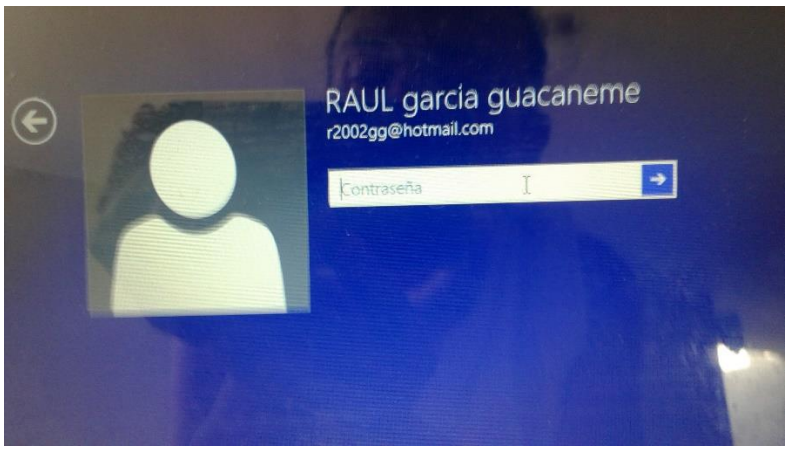
**Herramienta W3AF:** Esta herramienta que permite realizar actividades de auditoria y detectar vulnerabilidades Web, sencilla de utilizar y útil para automatizar deferentes análisis en un proceso.

## 4.4 PRUEBAS DE DETECCIÓN DE VULNERABILIDADES A LA RED DE DATOS

### 4.4.1 Pruebas de contraseña valida y nombre de usuario incorrecto.

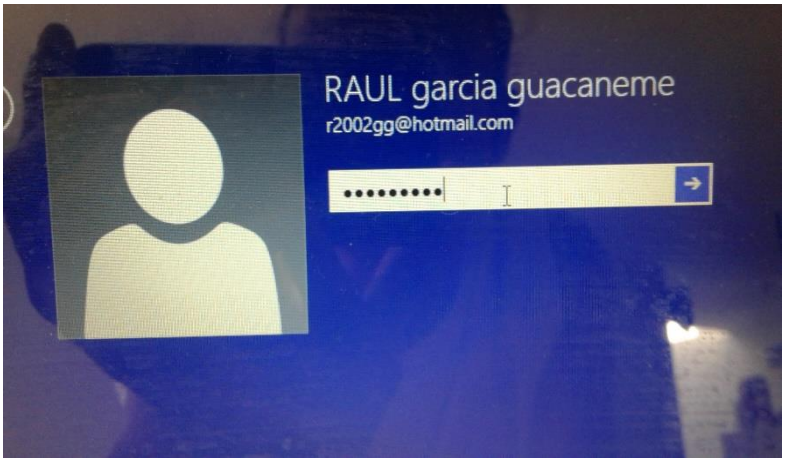
- Contraseña valida
  En las figuras se puede visualizar que al escribir la contraseña correcta la terminal permite el acceso a los programas y aplicativos del sistema.

Figura 5. Terminal de usuario.




Fuente: El autor

Figura 6. Contraseña de usuario.




Fuente: El autor

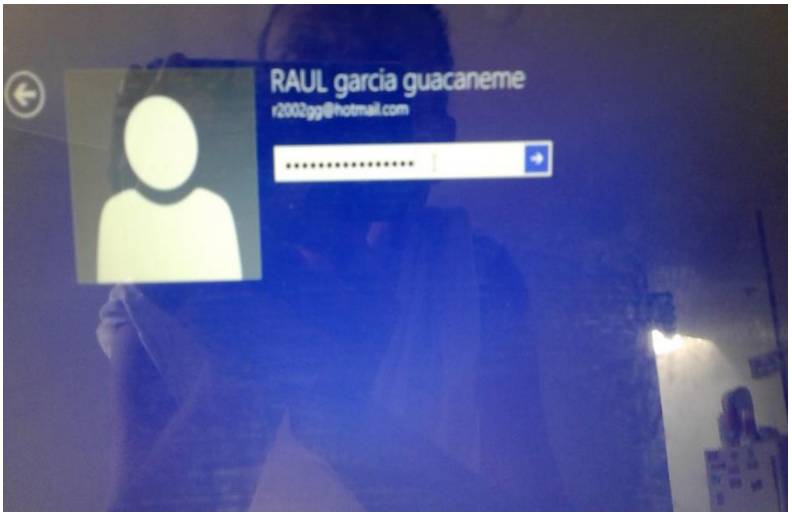
Figura 7. Acceso a la plataforma.

Fuente: El autor

En las figuras se puede observar que la contraseña tiene más de 8 caracteres, numéricos, letras y alfanuméricos lo cual determina que las contraseñas son fuertes y difíciles de descifrar.

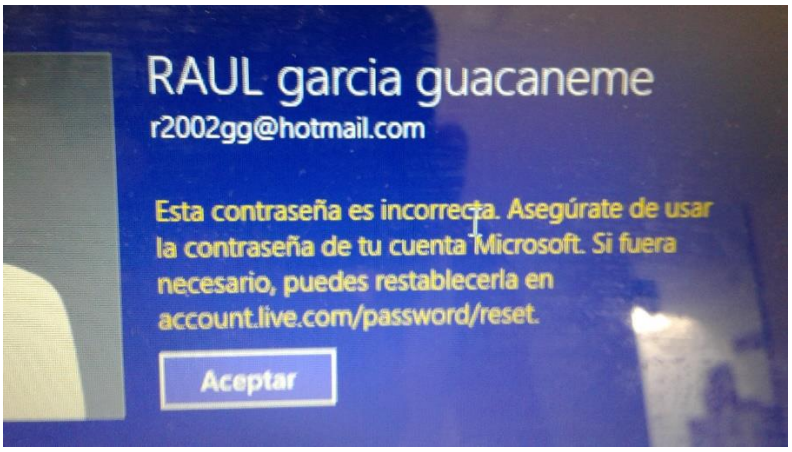
- Contraseña incorrecta

Figura 8. Ingreso de contraseña.




Fuente: El autor

Figura 9. Contraseña incorrecta.




Fuente: El autor

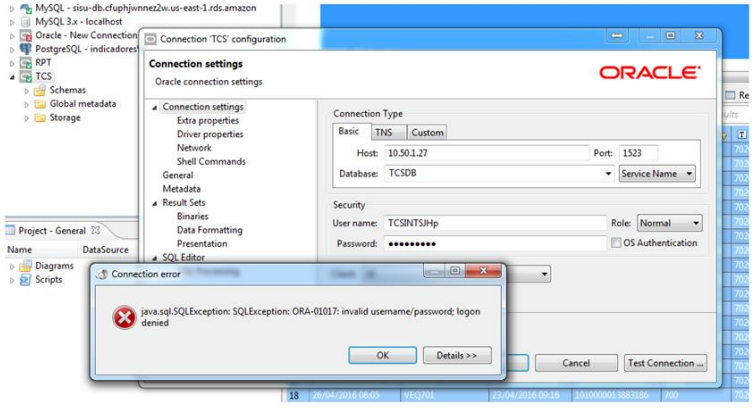
En las figuras se puede observar que al escribir la contraseña de usuario incorrecta la terminal no permite el acceso a los aplicativos.

La contraseña tiene más de 8 caracteres, numéricos, letras y alfanuméricos lo cual determina que las contraseñas son fuertes y difíciles de descifrar.

### 4.4.2 Pruebas de acceso a la base de datos TCS

Intento de acceder a la base de datos TCS, el intento es fallido, no podemos conectarnos a la base de datos TCS., como se observa en la figura.

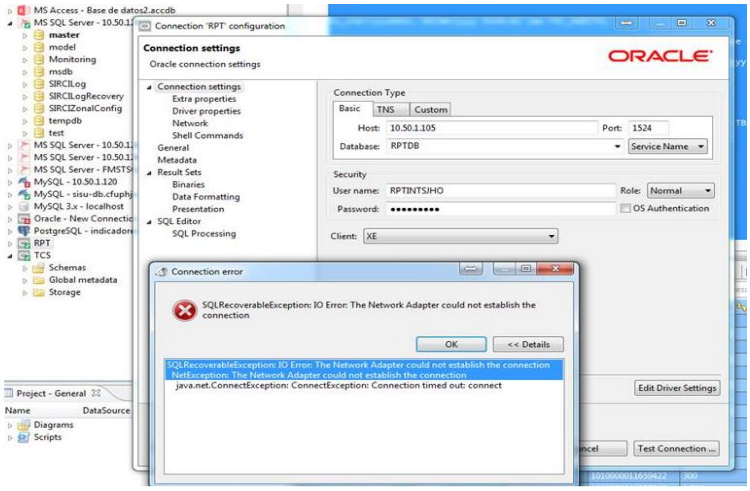
Figura 10. Base de datos TCS.




Fuente: El autor

Al tratar de acceder a la base de datos  por medio de la IP 10.50.1.105  me arroja un error y no me deja acceder a la base de datos rpt y tcs., como se observa en la figura.

Figura  11. Base de datos RPT y TCS.



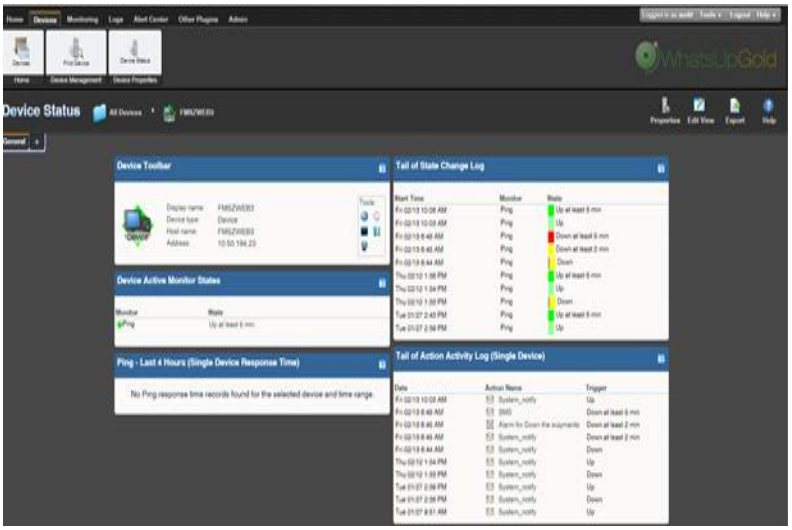

Fuente: El autor

### 4.4.3  Pruebas a los aplicativos

La empresa cuenta con Políticas de seguridad que establecen los niveles de acceso de los usuarios y  procedimientos para la identificación y autenticación de usuarios. El usuario dado por la empresa para la realización de las pruebas es solo de consulta y con este  se corroboran que los permisos que tiene ese perfil son acordes al tipo de usuario.

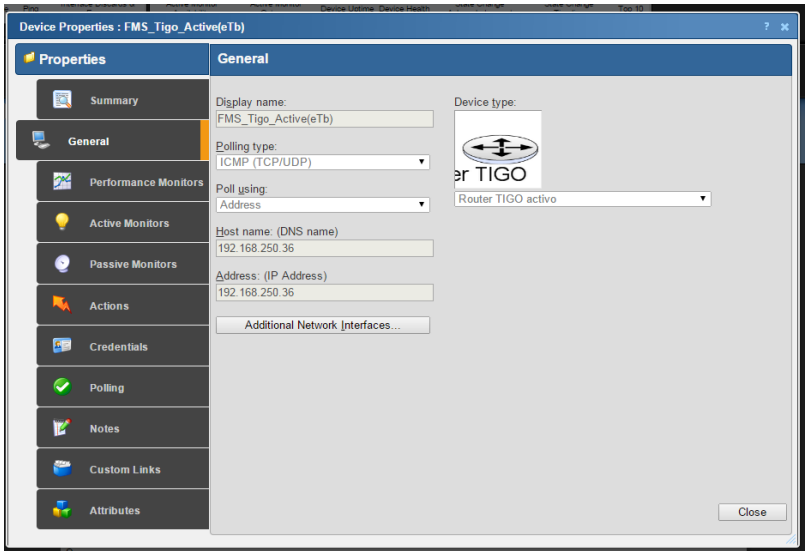
Con el usuario de consulta asignado por la empresa, de la herramienta *WhatsUp Gold*, donde aparecen los diferentes dispositivos de la red, se procedió a tomar aleatoriamente un dispositivo para realizar cambios en su configuración lo cual no fue posible debido a no tener ese permiso, Este usuario es creado con privilegios solo de consulta a los datos; por lo que no posee los permisos para realizar creación de objetos, procedimientos, tablas, etc., ni cuotas en los *tablespace*. Por tanto se validó que la empresa cuenta con procedimientos para la identificación y autenticación de usuarios como se muestra en las figuras.

Figura 12. Estado del dispositivo.




Fuente: El autor

Figura 13. Propiedades del dispositivo.

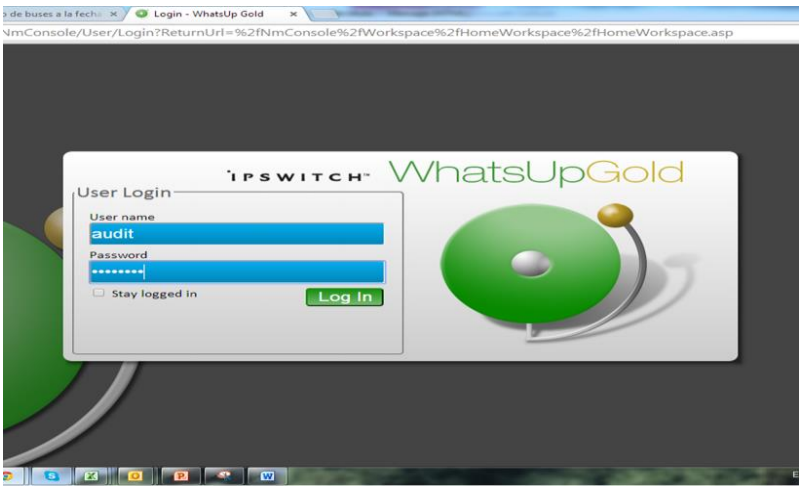



Fuente: El autor

**4.4.3.1 Pruebas con el aplicativo de gestión WhatsUp Gold.** Con el fin de garantizar el desempeño de los sistemas de comunicación de datos a través de la red, se realizaron pruebas de autenticación de usuarios y claves erróneas., a la herramienta de gestión proporcionada, WhatsUp Gold, la cual permite consultar los niveles de disponibilidad y latencia de la red, por periodos de tiempo específicos, para los centros de control. Utilizando la autenticación de usuario y clave correcta

se permite el acceso inmediato a la herramienta de gestión WhatsUp Gold, como se observa en la figura.

Figura 14. Herramienta de gestión WhatsUp Gold.

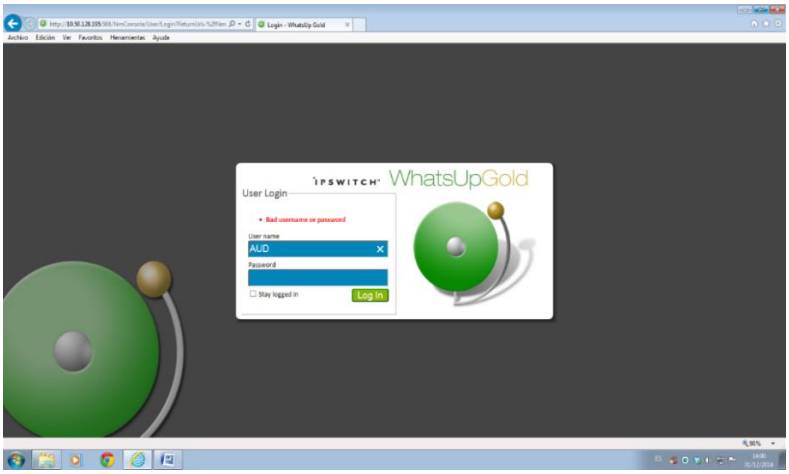



Fuente: El autor

**Ingreso a la herramienta de gestión WhatsUp Gold con usuarios y claves erróneas.**

Con base en las pruebas realizadas de autenticación de usuarios y claves erróneas a la herramienta Whats Up Gold, se observó el siguiente resultado. Bad usename or password, como se observa en la figura.

Figura 15. Ingreso usuarios y claves erróneas.



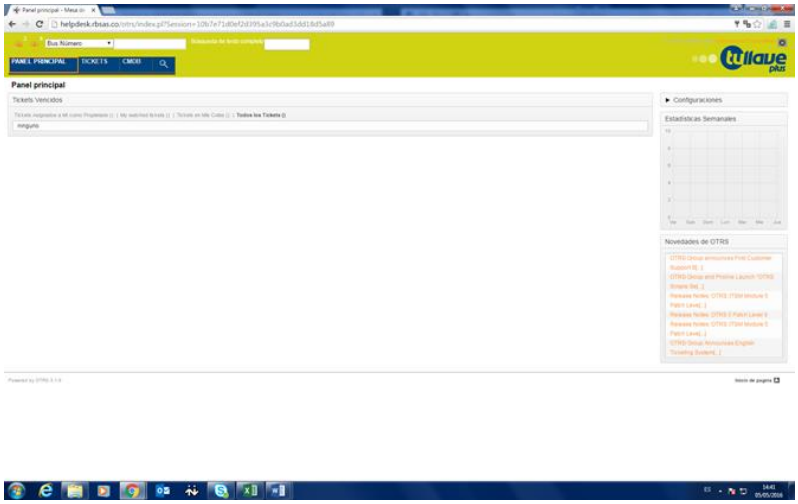

Fuente: El autor

Al realizar la prueba de ingreso a la herramienta de gestión WhatsUp con usuarios y claves erróneas durante diez (10) veces seguidas la herramienta arrojo el mismo resultado sin llegar a bloquearse la herramienta de gestión.

**4.4.3.2 Pruebas con el aplicativo de gestión OTRS.** La herramienta OTRS permite realizar una gestión integrada de las soluciones de servicio, información o cualquier requerimiento que realice un usuario a un área, dirección o cualquier entidad o agente que le solicite asistencia.

Utilizando la autenticación de usuario y clave correcta se permite el acceso de inmediato a la herramienta de gestión OTRS, como se observa en la figura.

Figura 16. Herramienta de gestión OTRS.



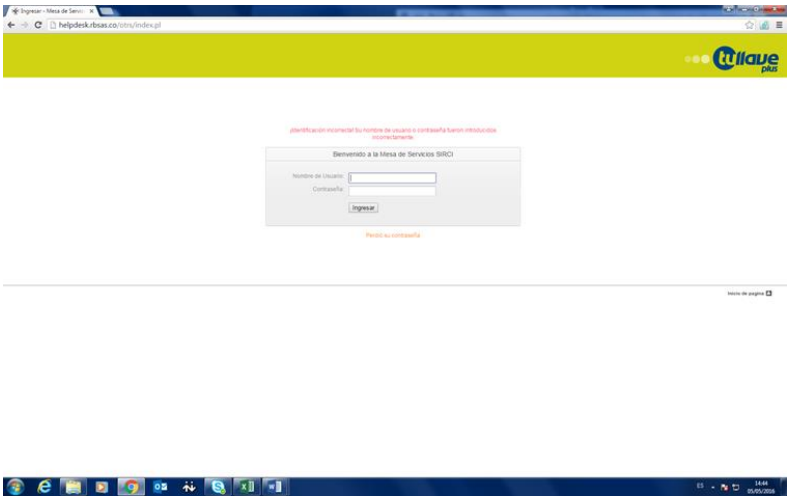

Fuente: El autor

- Se realizó pruebas de autenticación de usuarios y claves erróneas de vulnerabilidad a la herramienta OTRS., se observó el siguiente resultado, como se muestra en la figura.

  Ingreso a la herramienta de gestión OTRS con usuarios y claves erróneas.

  Si los datos ingresados por el usuario no son correctos el sistema visualiza un mensaje de error: ¡Identificación incorrecta! Su nombre de usuario o contraseña fueron introducidos incorrectamente, como se ve en figura.

Figura 17. Usuarios y claves erróneas.




Fuente: El autor

Al realizar la prueba de ingreso a la herramienta de gestión OTRS con usuarios y claves erróneas durante diez (10) veces seguidas la herramienta arrojo el mismo resultado sin llegar a bloquearse la herramienta de gestión.

## 4.5. PRUEBAS REALIZADAS CON LAS HERRAMIENTAS DE SOFTWARE WHATSUP GOLD Y OTRS

La arquitectura central se configura con una red redundante para asegurar la disponibilidad del sistema. Incluso en caso de que uno de los sistemas o de los enlaces falle, se activará de manera inmediata el sistema en espera al sistema continuo de respaldo del sistema.

En caso de conectividad WAN, el servicio de línea alquilado lo provee la compañía proveedora local de servicio y básicamente respalda más del 99.6% de disponibilidad por cada conexión WAN.

El diseño de fibra óptica proporciona una solución que asegura la interconexión, a través de enlaces de fibra óptica de nodos centrales y de acceso. La red de fibra óptica implementada es Metro Ethernet con giga bits tipo anillo cerrado para respaldar la conectividad redundante. El anillo de fibra óptica está compuesto por 5 sub-anillos.

La red de fibra óptica es redundante, y cuenta con 5 sub anillos que garantizan la comunicación, en caso de ruptura de alguno de los hilos, se cuenta con el protocolo de árbol de expansión el cual garantizará que se encuentra una nueva ruta para la transmisión de los datos.

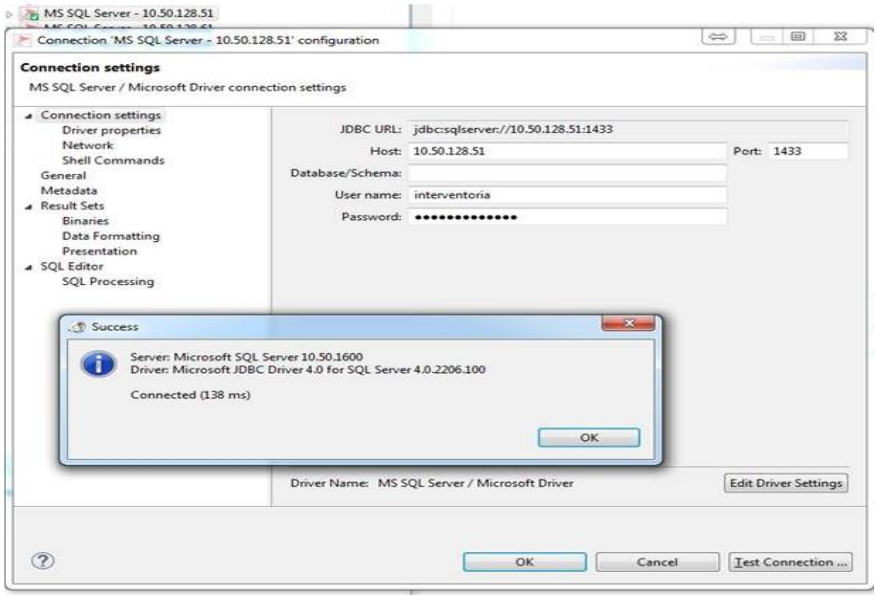
El documento de diseño de arquitectura de red y seguridad donde la empresa presenta la arquitectura de la red, se evidencia la redundancia en las redes de datos implementadas, con el fin de tener confiabilidad y seguridad de la información en cada terminal de la empresa.

Mediante la herramienta de gestión WhatsUp Gold, se pudo verificar la disponibilidad de todas las terminales de la red de comunicaciones, evidenciando la existencia de equipos en stand-by para soportar a los equipos principales en caso de falla.

La empresa cuenta con la herramienta de gestión OTRS, en donde se pueden evidenciar los tickets generados por problemas en la conexión de los terminales, ya sea por problemas de identificación de la persona, o porque se presente cualquier problema en la red, lo cual garantiza que todas las conexiones son programadas y controladas.

**4.5.1 Pruebas de seguridad realizadas a la base de datos.** En las siguientes figuras observamos que no es posible acceder a las aplicaciones y a la base de datos, ya que no contamos con los permisos de usuario. SQL Server 10.50.128.51.

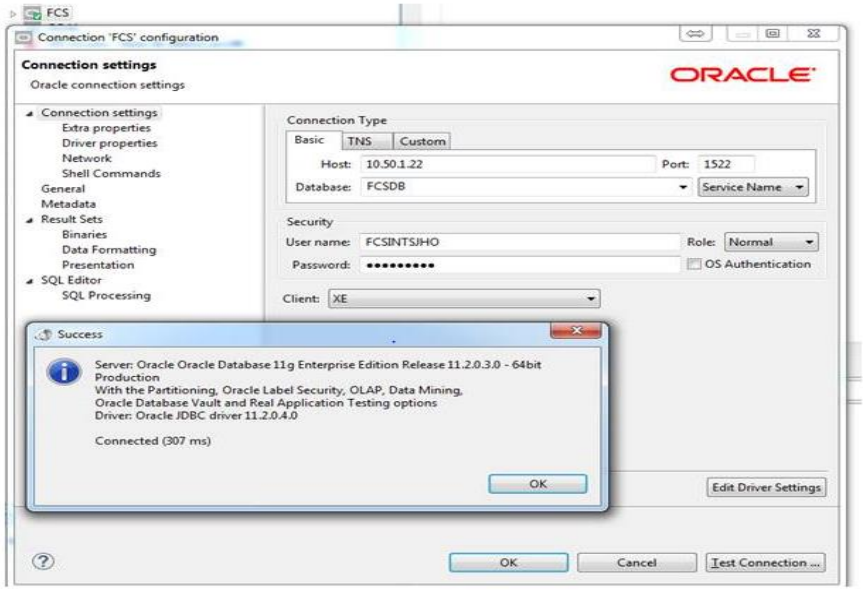
Figura 18. Base de datos SQL.




Fuente: El autor

## Oracle 10.50.1.22

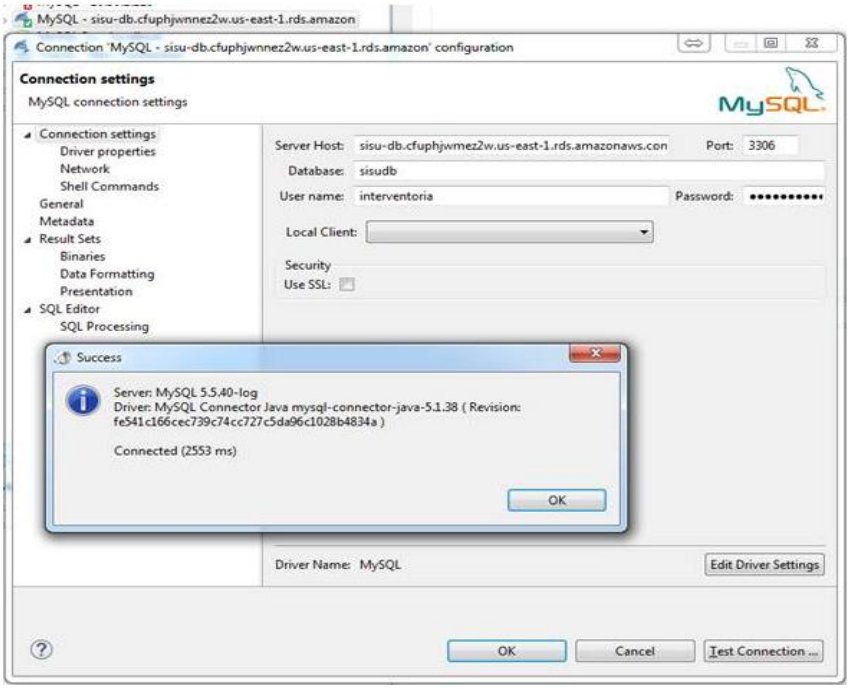
Figura 19. Oracle.




Fuente: El autor

MYSQL SISU

Figura 20. MYSQL SISU.



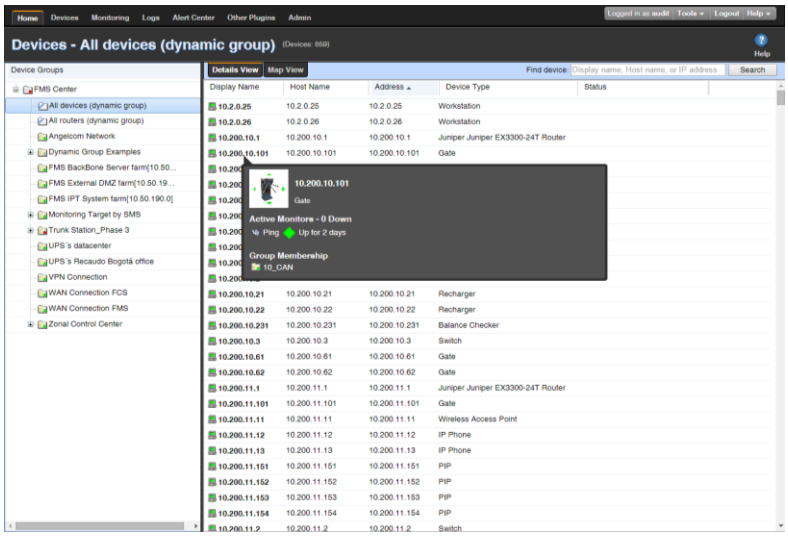

Fuente: El autor

El diseño de Arquitectura de Red y Seguridad se plantea el direccionamiento IP, con el fin de dividir las funciones de cada una de las partes y sus áreas dentro de la red y su configuración para permitir una gestión de aplicaciones y circulación fluida de datos al configurar una VLAN.

Cada red inalámbrica está configurada con su APN privada y realiza procesos de autenticación para prevenir conexiones no autorizadas que se intente hacer por la red, esta comunicación es mediante protocolos de comunicación 2G y 3G.

Con el usuario de consulta de la herramienta *WhatsUp Gold*, se procedió a verificar la información de los diferentes dispositivos de la red, como se observa en la figura, se validó que la empresa cuenta con la identificación y autenticación de las terminales. Lo cual garantiza que todas las conexiones son programadas y controladas.

Figura 21. Identificación de dispositivos en la red.




Fuente: El autor

La empresa cuenta con las herramientas de gestión, OTRS en donde se pueden evidenciar los tickets generados por problemas de conexión en las terminales y *WhatsUp Gold* en donde se evidencian registros de fallas de los equipos conectados a la red de fibra Óptica

La arquitectura central se configura con una red redundante para asegurar la disponibilidad del sistema. Incluso en caso de que uno de los sistemas o de los enlaces falle, se activará de manera inmediata el sistema en espera al sistema continuo de respaldo del sistema.

En caso de conectividad WAN, el servicio de línea alquilado lo provee la compañía proveedora local de servicio y básicamente respalda más del 99.6% de disponibilidad por cada conexión WAN.

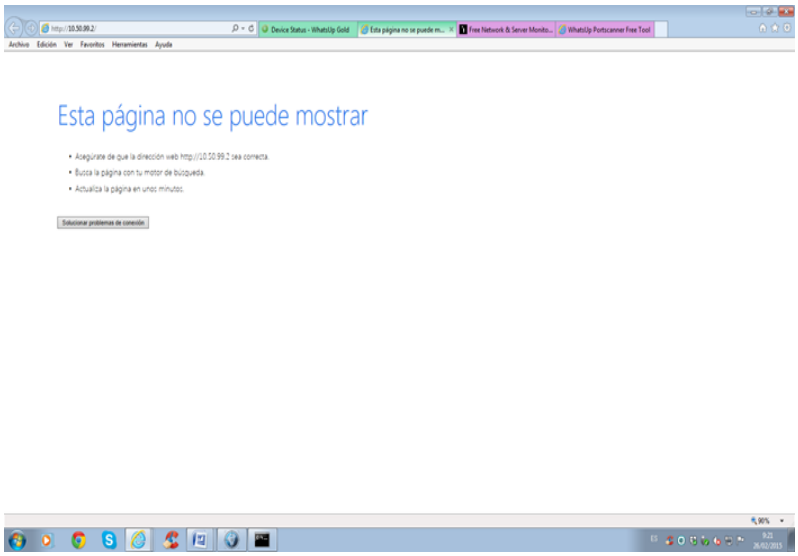
El diseño de fibra óptica proporciona una solución que asegura la interconexión, a través de enlaces de fibra óptica a toda la empresa. La red de fibra óptica implementada es Metro Ethernet con giga bits tipo anillo cerrado para respaldar la conectividad redundante.
Se realizaron pruebas para verificar que usuarios no autorizados no tengan acceso a las terminales de red y gestión para la comunicación de datos. Se verificó vía web y mediante consola vía Telnet, que el acceso a las terminales está restringido,

evidenciando las políticas de seguridad implementadas por la empresa a los equipos de red.

Los usuarios solo deben tener acceso a las terminales y servicios para cuyo uso están específicamente autorizados, en el cual se verifican los niveles de seguridad de los dispositivos y programas de seguridad para la operación y las políticas de seguridad implementadas por la empresa, las terminales deben responder automáticamente en caso de encontrar algún programa o intruso que quiera acceder a la red de comunicación de datos para borrar, sustraer o que haya perdida de datos en los paquetes que circulan por los sistemas centrales.

Se accedió a la dirección 10.50.99.2 por medio de internet la cual corresponde a WAN Connection, fmextsw1, obteniéndose el siguiente resultado de la figura, se puede observar que al intentar ingresar a la terminal fmextsw1 vía web, a través de la dirección http://10.50.99.2, no es posible la conexión.

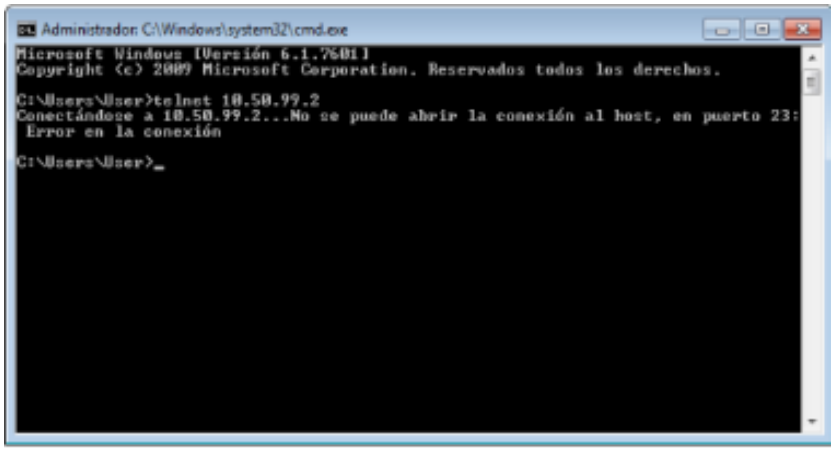
Figura 22. Acceso por medio de internet.




Fuente: El autor

Como lo evidencia la figura, se observa que hay un control y que las políticas de seguridad utilizadas por la empresa en caso de un acceso no deseado a los sistemas de datos de las terminales, el sistema de seguridad implementado niega el acceso a esta dirección no autorizada, por lo tanto si hay una sólida protección de seguridad del acceso a las terminales. En la figura, también se observa que no se puede acceder a la terminal fmextsw1 a través del comando Telnet.

Figura 23. Comando Telnet.



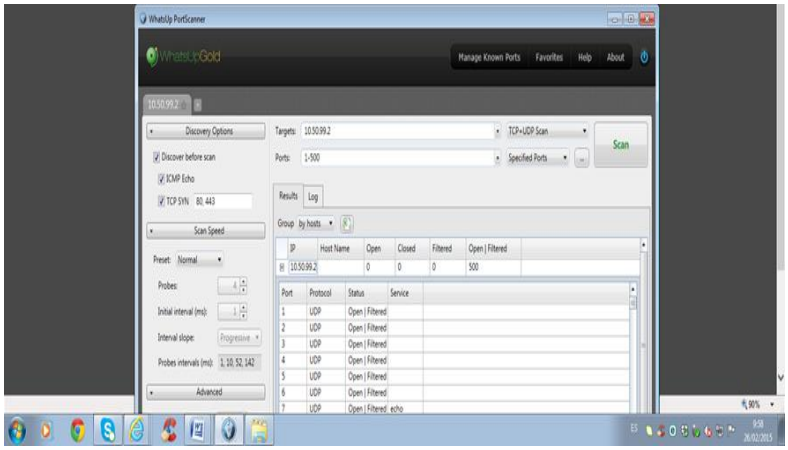

Fuente: El autor

Se utilizó la herramienta de escaneo de puertos WhatsUpGold PortScanner, para verificar la dirección: 10.50.99.2, WAN Connection, fmextsw1.

Displayname: fcextsw1
Device type: Juniper EX3200-24T Router
Host name: 10.50.99.2
Address: 10.50.99.2

En la figura se puede observar que la herramienta detecta la dirección, 10.50.99.2, fcextsw1, la cual verifica el puerto del Router, el protocolo UDP, el Status Open Filtered.

Figura 24. Acceso a las terminales.



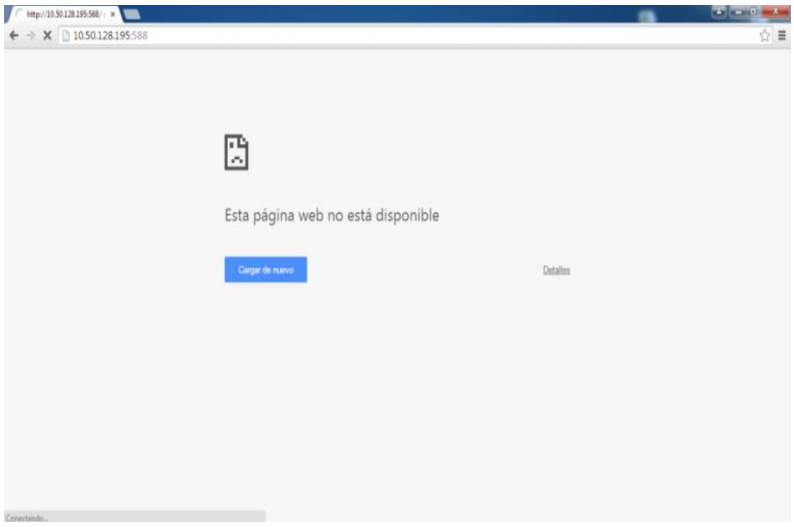

Fuente: El autor

En la figura, los controles para el acceso a los puertos y a las terminales está controlado por el uso de un bloqueo de llaves y procedimientos de soporte para controlar el acceso tanto del exterior como interior, ya que se trató de acceder a la dirección 10.50.99.2, WAN Connection , fmextsw1, por medio de la herramienta WhatsUpGold la cual detecto la dirección, más allá de poder ingresar por medio de esta herramienta, para poder borrar, extraer o modificar los datos no fue posible ya que los procedimientos de seguridad implementados por la empresa garantiza que solo sean accedidos mediante acuerdo entre el administrador del servicio del equipo activo y el personal de soporte de hardware que requiere el acceso.

## 4.6 PRUEBA DE INGRESO A LOS APLICATIVO DE GESTIÓN WHATSUP GOLD POR MEDIO DE INTERNET

Para Ingresar a la herramienta de gestión *WhatsUp Gold* se hace a través de la VPN/Firewall, por medio de la dirección http:// 10.50.128.195:588, al acceder con el perfil de consulta a la herramienta de gestión *WhatsUp Gold*, se realizó pruebas de ingreso a la herramienta por medio de un acceso público de internet para verificar si los usuarios no autorizados pueden acceder a los sistemas centrales, para poder manipular, modificar y extraer los datos allí contenidos por medio de esta herramienta. Como se observa en la figura.

Figura 25. Acceso denegado desde conexión pública.




Fuente: El autor

Como evidencia el tráfico de entrada y salida está controlado, así como accesos de tráfico alterno de conexiones públicas desde Internet a cualquier componente del sistema en el ambiente de datos. La seguridad de la red de datos garantiza la comunicación segura entre los sistemas centrales con los demás sistemas del ambiente, evitando el posible ingreso y modificación de los datos.

La arquitectura central se configura con una red redundante para asegurar la disponibilidad del sistema. Incluso en caso de que uno de los sistemas o de los enlaces falle, se activará de manera inmediata el sistema en espera al sistema continuo de respaldo del sistema.

En caso de conectividad WAN, el servicio de línea alquilado lo provee la compañía proveedora local de servicio y básicamente respalda más del 99.6% de disponibilidad por cada conexión WAN.

El diseño de fibra óptica proporciona una solución que asegura la interconexión, a través de enlaces de fibra óptica de nodos centrales y de acceso. La red de fibra óptica implementada es Metro Ethernet con giga bits tipo anillo cerrado para respaldar la conectividad redundante. El anillo de fibra está compuesto por 5 sub-anillos.

La red de fibra óptica es redundante, cuenta con 5 sub anillos que garantizan la comunicación, en caso de ruptura de alguno de los hilos, se cuenta con el protocolo de árbol de expansión el cual garantizará que se encuentra una nueva ruta para la transmisión de los datos. Esto asegura la disponibilidad del sistema.

Mediante la herramienta de gestión *WhatsUp Gold*, se pudo verificar la disponibilidad de todos los componentes de la red de comunicaciones, evidenciando la existencia de equipos en stand-by para soportar a los equipos principales en caso de falla.

Los indicadores de confiabilidad y disponibilidad del sistema de comunicaciones de la empresa son un buen indicativo de la seguridad en la transmisión de datos, garantizando que la información recibida es idéntica a la enviada.

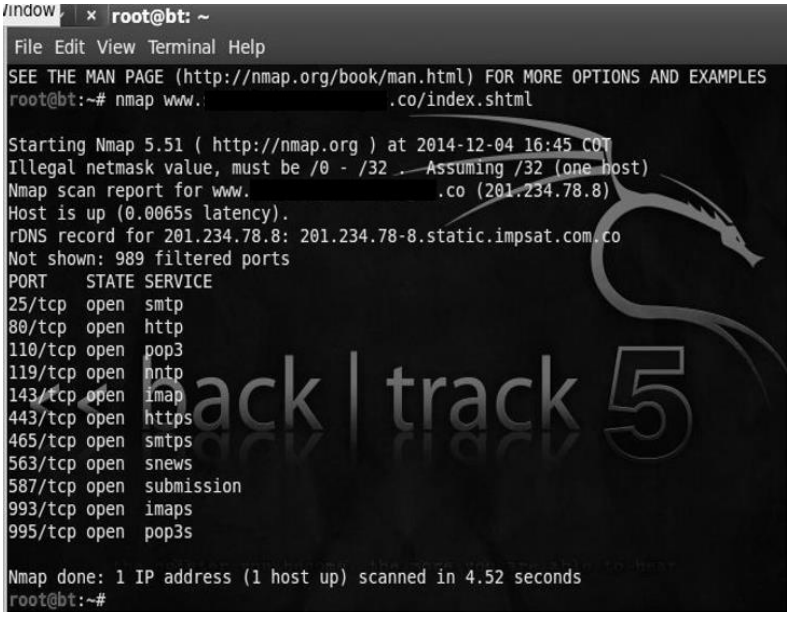
En el Anexo A. Se observa la Matriz de Evaluación de la red. Anexo B. Matriz de las Vulnerabilidades, Riesgos y Amenazas. Anexo C. La Matriz de Riesgos con Valoración.

## 4.7 PRUEBAS REALIZADAS CON LA HERRAMIENTAS DE SOFTWARE PENTESTING

Utilizando la herramienta de Pentesting o herramienta de penetración la cual sirve para detectar vulnerabilidades en los sistemas, en este caso se utiliza la Suite de Backtrack y algunos de sus componentes de Software para evaluar la red y determinar posibles vulnerabilidades.

Usando la herramienta Backtrack con el programa NMAP, para escanear los puertos que están abiertos, Como se observa en la figura.

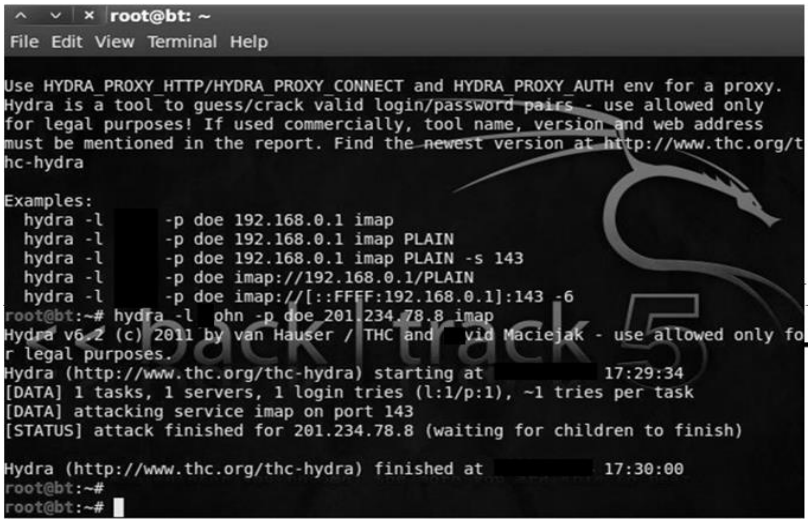
Figura 26. Herramienta Pentesting.




Fuente: El autor

Como se observa los puertos abiertos que tiene la empresa son vulnerables y cualquier potencial atacante los puede usar para atacar la red, utilizando la herramienta Hydra que está contenida en la suite de Backtrack,  ver figura.

Figura 27. Herramienta Hydra.

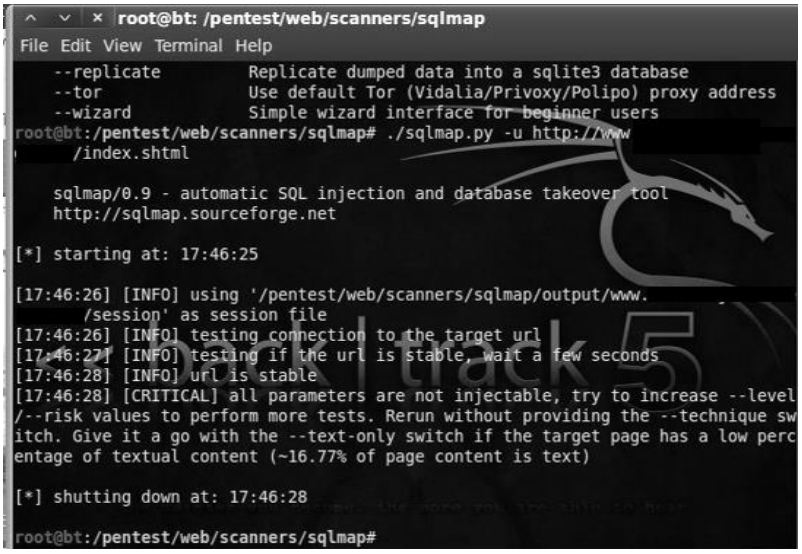



Fuente: El autor

Indica que el puerto 14, es vulnerable, que está  ejecutando 1 tarea y es un servidor.

Al evaluar con la herramienta SQLMAP vemos que es inmune a un ataque de inyección de Bases de datos, en la siguiente imagen se observa que la empresa está bien protegida a este tipo de ataques.

Figura 28. Herramienta SQLMAP.




Fuente: El autor

La figura  nos muestra que la red  es segura y no es posible extraer información de la base de datos SQL

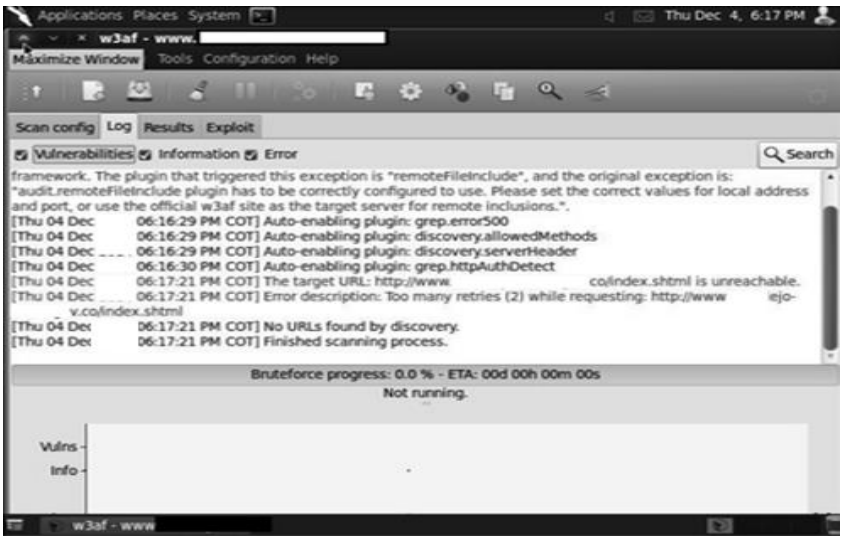
Se analizó la página web con la herramientaW3AF, para determinar vulnerabilidades en la direcciones IP que digitemos, como se observa en la figura siguiente.

Figura 29. Herramienta W3AF.


Fuente: El autor

En target se digita la dirección IP o página web a evaluar, en la parte izquierda le damos clic  en audit_high_risk y luego clic  en start al lado de donde dice target, la herramienta realizara el análisis correspondiente, ver figura.

Figura 30. Análisis de la  Herramienta W3AF.




Fuente: El autor

La herramienta indica que hay un error de código y una vulnerabilidad de acceso que puede ser utilizada por un atacante.

La herramienta realiza el análisis, como lo muestra la figura siguiente.

Figura 31. Resultado de la  Herramienta W3AF.


Fuente: El autor

El resultado de la herramienta indica que aparece un BUG que es  un error en las líneas de código de la página web, lo cual un atacante habilidoso podría aprovecharla para instalar algún tipo de malware, código malicioso o insertar backdoors,  para poder controlar los sistemas de la organización.

## 4.8 INFORME DE VULNERABILIDADES Y RECOMENDACIONES

La red corporativa de la compañía, presenta un grado de complejidad para la administración y control de seguridad informática, debido a que está diseñada en infraestructuras separadas de conectividad para la red operativa y administrativa. A continuación se presentaran las vulnerabilidades y recomendaciones que se le sugieren a la organización para mejorar su seguridad en sus sistemas de red de datos.

**Directivas y personal de la empresa**

- Concientizar a los empleados de la organización de la importancia que tiene la manipulación y confidencialidad de la información.

  **Recomendación**: Los funcionarios y empleados adquieren las responsabilidades y cuidados que se deben tener al manipular información confidencial de la empresa.

- Todas las claves y privilegios que tienen los empleados de la empresa deben ser bloqueados a la hora que se termine el contrato de forma definitiva.

  **Recomendación**: En caso que el contrato termine en malos términos se debe impedir que el afectado despedido manipule la información.

- Prohibir cualquier actividad de personal no autorizado en las áreas donde hay información y acceso a los equipos de cómputo.

  **Recomendación**: Se evitara daños en los equipos ya sea por derramamiento de líquidos o comida sobre ellos provocando la pérdida del equipo y de la información, además se evitara que personal no autorizado pueda acceder a la información de los usuarios.

- Los empleados de la organización que ejercen funciones en los sistemas de información deberán ser capacitados periódicamente en materia de seguridad.

  **Recomendación**: El departamento de seguridad informática deberá difundir las políticas de seguridad implementadas por la empresa a todos los empleados en general.

- Los usuarios de la empresa que tienen correo electrónico deberán conocer la importancia del uso del mismo, ya que si no le damos un buen uso, podemos ser víctima de virus por descargas de archivos adjuntos.

  **Recomendación**: Los empleados deberán tomar conciencia del uso del correo electrónico, del riesgo a que están expuestos por el mal uso del mismo, solo se deberá utilizar para intercambiar información exclusiva de la empresa.

- Es necesario que los empleados tengan claro los aspectos de integridad, disponibilidad y confiabilidad de los bienes y servicios de la entidad.

  **Recomendación**: Los empleados deberán adquirir el compromiso al momento de ser contratados de proteger y salvaguardar los activos informáticos, ya que es lo más valiosos que posee la organización y así se evitaran fugas de información.

**Base de datos**

Como resultados de las pruebas se identificaron las siguientes vulnerabilidades a la base de datos:

- Algunos usuarios cuenta con políticas de contraseñas débiles.

- Permite asignar contraseñas iguales al nombre de usuario fáciles de identificar.
- No cuenta con la longitud mínima de caracteres.
- Para la construcción de la contraseña no cuenta con criterios de asignación de caracteres especiales como condición obligatoria.

  **Recomendación**: Se recomienda establecer políticas más fuertes en la definición de contraseñas, contar con una longitud mínima, no asignar el mismo nombre de usuario a la clave y asignar un mínimo de caracteres especiales

- Usuarios en desuso.

  **Recomendación**: Se requerirá contar con tareas periódicas de monitoreo de la base de datos para identificar usuarios en desuso.

- La información contenida en las bases de datos deberá ser usada únicamente para asuntos relacionados con actividades de la empresa.

**Recomendación**: Los funcionarios y empleados deben dar buen uso a la información de las bases de datos y no utilizarla para su beneficio personal que no tiene nada que ver con la actividad de la empresa.

- Todos los datos de gran importancia deberán ser respaldados y almacenados en un lugar seguro.

  **Recomendación**: El departamento de sistemas deberá estar pendiente de realizar copias de respaldo de la información más importante de la empresa, ya que de esta forma se protegerá la información y en caso de desastre se pueda recuperar.

- La información contenida en las bases de datos solo la podrá utilizar y modificar el personal autorizado.

  **Recomendación**: Se deberá crear una política de control de acceso la cual debe ser gestionada por el administrador de base de datos.

- Incorporar a la base de datos un proceso que registre todos los accesos y las actividades realizadas.

  **Recomendación**: Actualizar las bases de datos, de esta forma la empresa contara con un historial de acceso a las bases de datos de los empleados en caso de un uso inadecuado de la información.

- Implementar una política que administre y controle la eliminación de información de la base de datos que ya no sea necesaria.

  **Recomendación**: La base de datos no se recargara con información innecesaria y serán más rápidas las consultas.

**Infraestructura y red**

- Socializar los procedimientos de prevención y mitigación de los riesgos informáticos.

  **Recomendación**: Difundir las políticas de riesgos tanto a las directivas como a los empleados de las diferentes áreas de la empresa, para prevenir futuros desastre en la red que puedan conllevar a la perdida en la información por culpa de ignorancia o desconocimiento de las políticas de seguridad informática implementada por la organización.

- Cumplir con todas las políticas de seguridad establecidas por la organización.

  **Recomendación**: El departamento de seguridad informática está encargado, de que todos los empleados cumplan con las políticas de seguridad implementadas, para evitar riesgos informáticos, que puedan ocasionar daño a la red y fuga de su información.

- Actualizar el cronograma de mantenimiento de equipos preventivo y correctivo.

  **Recomendación**: La empresa deberá realizar un cronograma de mantenimiento periódico a los equipos, así se evitara futuros daños en los computadores y la red será más eficiente.

- Se cuenta con un antivirus que no realiza una buena protección a los equipos, en ocasiones se pierde información por la existencia de código malicioso.

  **Recomendación:** La empresa deberá establecer un plan de protección de los registro, establecer procedimientos de detención, prevención y corrección de software malicioso (Virus, troyanos, spyware, etc.), actualizando el sistema operacional y el antivirus periódicamente.

- Mejorar la seguridad física, el ingreso de personal no autorizado.

  **Recomendación:** la empresa deberá hacer cumplir la política de control de acceso a las instalaciones, definir el perímetro de seguridad física, establecer mecanismos de protección contra amenazas externas y personal no autorizado en las diferentes áreas de la entidad.

- Los equipos que no estén en uso deberán ser almacenados en un lugar seguro donde se restrinja el acceso al personal no autorizado.

  **Recomendación:** Se deberán destruir los equipos almacenados y que ya no son útiles, para evitar la pérdida o sustracción de la información que pueda ocasionar daño a la entidad.

- Los equipos de cómputo serán asignados a un responsable para evitar el uso inadecuado del mismo.

  **Recomendación:** Así se mejorará la administración y mantenimiento de los recursos informáticos de la organización.

- El área de sistemas es la encargada de realizar los diferentes mantenimientos preventivo y correctivo de los quipos de cómputo.

  **Recomendación:** Para evitar deterioro de los equipos y una mala manipulación por personal no calificado**.**

- Se deberá establecer controles de acceso en áreas donde se ubican los servidores y equipos de comunicación de la empresa.

  **Recomendación:** De esta forma se llevara un control de quien y a qué hora ingresa el personal autorizado a estas áreas.

- Las contraseñas usadas para la configuración de servidores, equipos de red y telecomunicaciones deberán estar basadas en un estándar que defina aspectos como: estructura, tiempo de validez y reusabilidad.

  **Recomendación:** La utilización de contraseñas fuertes y difíciles de descifrar evitara el acceso no autorizado de personal a los equipos y a la información confidencial de la empresa.

- El personal que realiza trabajos de configuración de los dispositivos de red deberá poseer una certificación que avale sus capacidades.

  **Recomendación:** El personal que manipule, configure y repare los equipos deberán estar calificados debidamente para que no comprometan la seguridad de la red.

- Se deberá llevar un documento que registre todas las configuraciones que se realicen sobre los dispositivos de red, debidamente codificados e identificados.

  **Recomendación:** Facilitará y agilizará el proceso de reparación o mantenimiento de los dispositivos de Red.

- Los puertos que no estén en uso deberán ser bloqueados adecuadamente.

  **Recomendación:** De esta forma se evitaran accesos internos y externos de personal no autorizado a la red que puedan ocasionar daños y la manipulación de la información.

- El acceso a Internet será restringido, solo para realizar labores propias de la empresa.

**Recomendación:** Se deberán de bloquear algunas páginas de internet que no son necesarias para el desarrollo de la actividad de la empresa, para que los trabajadores no puedan acceder y empleen su tiempo más eficientemente en actividades propias de la empresa.

- Deberá cifrarse la información que circule a través de la red.

  **Recomendación:** Evitara que personal no autorizado puedan acceder a la información confidencial que circula a través de la red y la puedan manipular en contra de la organización.

**Utilización del software**

- La instalación de software en los equipo deberá ser instalado solo por el personal del área de sistemas autorizado.

  **Recomendación:** Los usuarios no podrán instalar programas que no sean de la organización para realizar su trabajo diario, ya que pueden poner en riesgo los equipos y la seguridad de la red de datos.

- Todos los equipos deberán tener configurado la opción de cierre de sesión después de un lapso de inactividad.

  **Recomendación:** Se preverá que usuarios no autorizados puedan acceder, modificar o borrar información confidencial, mientras el usuario no está en su sitio de trabajo,

- Crear una política de revisión periódica del funcionamiento del software.

  **Recomendación:** Se mejorara la vida útil, el rendimiento de los equipos, la seguridad en la red y se actualizara el software que ya no es eficiente.

- Se permitirá únicamente instalar software licenciado a los equipos.

  **Recomendación:** Se borrara el software inútil y se dará buen uso de los recurso informáticos utilizando únicamente el software licenciado, así se mejorara la seguridad de la red y se evitara la propagación de virus informáticos.

- Todo software nuevo antes de ser instalado en el equipo deberá ser probado y evaluado.

**Recomendación:** De esta forma se evitara un software defectuoso que pueda modificar la información o bloquee los equipos de la entidad y la red de datos será más eficiente y segura.

# 5 CONCLUSIONES

Se pudo identificar que el recurso humano tanto operativo como directivo de la empresa debe estar más involucrado en cumplir y divulgar el cumplimiento de las políticas de seguridad implementadas por la empresa, además debe definir de forma clara los roles y las responsabilidades del departamento de seguridad informática.

La empresa debe invertir en recurso económico periódicamente para que todo el personal de la empresa reciba una adecuada capacitación y actualización en materia de seguridad informática y de los riesgos a que está expuesta su red de datos.

Todo el personal de la empresa tanto interno como externo que manipule información confidencial y sensible de la empresa, debe comprometerse a protegerla, para evitar fugas de información, la cual pueda ser utilizada indebidamente.

## BIBLIOGRAFÍA


GUIA PROPUESTA DE PROYECTO DE INVESTIGACION, Universidad Popular del Cesar en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/capitulo_3__analisis_de_riesgos.html

CERTIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN con ISO/IEC 27001. Internet en: http://www.icontec.org/index.php/en/sectores50-colombia/certificacion-sistema/342-certificacion-iso-iec-27001

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

GUÍA A LA REDACCIÓN EN EL ESTILO APA, 6ta edición, recuperado el 5/03/2012. Disponible en: http://www.suagm.edu/umet/biblioteca/pdf/GuiaRevMarzo2012APA6taEd.pdf

GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA, Internet en: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. NTC-ISO/IEC 27001:2005. Bogotá D.C. El instituto 37p.

NORMA TECNICA COLOMBIANA, NTC 1486, en PDF. Presentación de tesis, trabajos de grado y otros trabajos de investigación, Modulo Icontec.

J. J. Cano, "La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes," ISACA Journal Online, vol. 5, 2011.

WWW.ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, Madrid, 2012.

Universidad Nacional de Luján, "seguridadinformatica," [Online]. Available: http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf. [Accessed Marzo 2016].

EL CONGRESO DE COLOMBIA, "Alcaldia Bogotá," 2009. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [Accessed 2016].

E. C. d. Colombia, "alcaldiabogot," 1999. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. [Accessed 2016].

EL CONGRESO DE COLOMBIA, "alcaldiabogotá," 2012. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Accessed 2016].

## *Anexo A. Matriz de Evaluación de la Red.*

| Dominio | Proceso | Evaluación | Actividades |
|---|---|---|---|
| Planificación y organización | Definición de la organización y de las relaciones de TI | La tecnología encontrada, satisface los requerimientos, a través de la infraestructura tecnológica utilizada. | - Adecuación y evolución de la infraestructura actual, en aspectos tales como arquitectura de sistemas y dirección tecnológica.<br>- El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento.<br>- Adquisición que se verá reflejada de acuerdo a las necesidades identificadas en el plan de infraestructura tecnológica. |
| | Administración de recursos humanos | Las cargas del personal a los procesos de TI, satisfacen los requerimientos de la empresa, a través de técnicas de administración de personal. | - Tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.<br>Los programas de capacitación, entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica |
| Adquisición e implementación | Identificación de Soluciones Automatizadas | Realización de análisis claro de las oportunidades comparadas contra los requerimientos de los usuarios. | Definir los requerimientos de información para poder aprobar un propósito de desarrollo.<br>Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios. |
| | Adquisición y mantenimiento de la infraestructura tecnológica | Proporcionan las plataformas apropiadas para soportar aplicaciones de la empresa | Realizar evaluación del desempeño de hardware y software.<br>Mantenimiento preventivo de hardware e instalación de seguridad y control de las aplicaciones utilizadas. |

***Anexo A. (Continuación)***

| Dominio | Proceso | Evaluación | Actividades |
|---|---|---|---|
| | Desarrollo y mantenimiento de procedimientos | El uso es apropiado de las aplicaciones y soluciones tecnológicas creadas. | Realizar enfoque organizado por desarrollo de manuales de procedimientos en operaciones para usuarios.<br>Requerir servicio y material de entrenamiento. |
| | Instalación y aceptación de los sistemas | La solución tecnológica utilizada es adecuada para el propósito deseado. | Efectuar un cambio de instalación, conversión y plan de permisos adecuadamente formalizados.<br>Revisar la ejecución posterior con el objeto de reportar si el sistema proporciona los beneficios esperados. |
| Entregar y dar soporte | Definir y administrar niveles de servicio | Hay comprensión común del nivel de servicio requerido | Se deben establecer ajustes de niveles de servicio que formalicen criterios de desempeño que midan cantidad y calidad del servicio. |
| | Administrar servicios de terceros | Las tareas y responsabilidades de terceras partes están definidas, cumplen con satisfacción de los requerimientos | Hay que establecer medidas de control dirigidas a la revisión y monitoreo de los procedimientos existentes, en efectividad y suficiencia, con respecto a las políticas de la empresa. |
| | Administración desempeño y capacidad | Los controles de manejo de capacidad de desempeño recopilan datos y reportes acerca del manejo de cargas de trabajo | Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.<br>Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas. |
| | Asegurar el Servicio Continuo | El servicio tecnológico disponible concuerde con los requerimientos y continua su provisión en caso de interrupciones. | Se requiere plan de continuidad probado y funcional, relacionado con los requerimientos de la empresa. |
| Monitorear y evaluar | Monitorear y evaluar el desempeño de TI | Se logran de los objetivos establecidos para los procesos de TI. | Definir indicadores claves de desempeño y/o factores críticos de éxito<br>Definir el grado de satisfacción de los clientes con respecto a los servicios de información proporcionados |
| | Monitorear y evaluar el control interno | Se obtienen los objetivos de control interno establecidos para los procesos de TI | Vigilar la efectividad de los controles internos a través de actividades administrativas y de supervisión.<br>Analizar la existencia de puntos vulnerables y problemas de seguridad. |

## *Anexo B. Matriz de Vulnerabilidades, Amenazas y Riesgo*

| CATEGORÍA DE ACTIVO | SERVICIO DE RED | VULNERABILIDAD | AMENAZA | RIESGO |
|---|---|---|---|---|
| 1. Comunicaciones | Desarrollo tecnológico informático | Deficiencias en los requerimientos presentados y en el mantenimiento de las herramientas desarrolladas. | Falta de personal que brinde soporte a los aplicativos. | Aplicación limitada de las herramientas informáticas desarrolladas |
| | Desarrollo tecnológico herramientas | Obsolescencia de herramientas tecnológicas | Ausencia de herramientas tecnológicas | Desarrollo y aplicación de herramientas tecnológicas no autorizadas |
| | Equipos de comunicaciones | Retraso en los enlaces de los equipos de comunicaciones | Daños presentados en los equipos de comunicaciones | Daños de los equipos de comunicaciones |
| | Red telefónica | Falta de comunicación entre empleados | Fallas en la red telefónica | Daños de la red telefónica |
| | Internet | Comunicación no permanente en la red | Conocimiento de información tardía | Cortes del servicio de internet |
| | Red Informática | La interceptación de información que es transmitida desde o hacia el sistema. | Penetración del sistema a través de la red | Intercepción de las comunicaciones |
| 2. Tecnología | Software | Presencia de software malicioso<br>Conflictos en los recursos compartidos | Instalación de programas innecesarios<br>Registro inadecuado de programas de Windows | Daños en software |
| | Hardware | Presenta software malicioso | Falla en la memoria, fuente, disipadores, board, disco duro, etc.<br>Consumo de alimentos en las áreas de trabajo | Daños en Hardware |
| | Red | Administración de la red | Daños en los dispositivos de comunicación (rack, servidores, routers) | Fallas en la red |
| | Sistemas de Información | Fallas en la administración de los aplicativos<br>Denegación del servicio a través de múltiples consultas concurrentes<br>Problemas en la oportunidad de la atención en los diferentes sistemas de información | Problemas en la configuración de los parámetros de seguridad del servidor del sistema de información<br>Falta de soporte y mantenimiento de fabrica<br>Fallas en los controles para el acceso físico a los servidores | Violación de los sistemas de Información |
| | Dispositivos de red | El constante cambio tecnológico genera que las herramientas adquiridas entren en inoperancia. | Referencia de repuestos descontinuados<br>Aceleración de nuevas tecnologías generando discontinuidad de las mismas en un corto periodo de tiempo | Obsolescencia Tecnológica |

***Anexo B. (Continuación)***

| CATEGORÍA DE ACTIVO | SERVICIO DE RED | VULNERABILIDAD | AMENAZA | RIESGO |
|---|---|---|---|---|
| 3. Seguridad Física | Hardware | Ausencia de Hardware | Falta de dispositivos para buen funcionamiento | Robos de hardware |
| | Infraestructura de red | Violación de autorización | Personas no autorizadas | Vandalismo |
| | Infraestructura de red | Perdida de hardware | Riesgos físicos | Incendios |
| | Infraestructura de red | Perdida de equipos en funcionamiento | Daños en hardware y software | Terremotos |
| | Punto de energía eléctrica | Funcionamiento irreparable de dispositivos | Perdida del funcionamiento correcto de equipos | Fallas eléctricas |
| | Hardware | Atrasos en el funcionamiento de los procesos | Perdida de la información almacenada | Fallas de hardware |
| 4. Manejo de Personal | Acceso | Manipulación de datos confidenciales | Extracción de datos no autorizados | Accesos no autorizados |
| | | Tenencia de información no autorizada. | Acciones sospechosas | Fraude |
| | Identidad | Autorizaciones no verificadas | Accesos no autorizados | Suplantación de identidad |
| | Autenticación | Intentos fallidos | Autenticación repetida | Fallas de autenticación |
| | Personal | Eficiencia afectada | Rendimiento desmejorado | Indisponibilidad del personal |
| | Información | Obtención de información | Perdida de información | Fugas de Información |
| 5. Protección de la Información | Información | Obtención de información | Perdida de información | Robo de información |
| | Información | Obtención de información | Perdida de información | Perdida de información |
| | Información | Información no veraz | Personal involucrado, Información errada | Manipulación de información |
| | Usuario | Entorpece funcionamiento | Demora en servicios ofrecidos | Errores de usuario |
| | Información | Falta de información completa | Ausencia de información real disponible | Eliminación de información |
| | Backup | Ante cualquier desastre la organización es perjudicada | Perdida de datos | No se encuentran definidas las políticas de copias de seguridad |
| 6. Seguridad de la red | Archivos y programas | El estado de programas y archivos se ve afectado | Programas y archivos eliminados o cambiados | Acceso a los programas y archivos por parte de personal no autorizado |
| | Destinatario | Extracción de información | Accesos de información por medio empleados | Información transmitida a un destinatario incorrecto |
| | Programas y archivos | Vulneración y funcionamiento errado de la información | Funcionamiento errado | Modificación de los programas y archivos por parte de los usuarios |
| | control de acceso | Información puesto es peligro | Vulneración de la privacidad de la información | Falta de software de control de acceso |
| | virus | Vulnerable todo el sistema de información | Mal funcionamiento de software o hardware | Entrada de virus y malware |

## *Anexo C. Matriz de Riesgos con Valoración*

| CATEGORÍA DE ACTIVO | SERVICIO DE RED | VULNERABILIDAD | AMENAZA | RIESGO | PROBABILIDAD | IMPACTO |
|---|---|---|---|---|---|---|
| 1.Comunicaciones | Desarrollo tecnológico informático | Deficiencias en los requerimientos presentados y en el mantenimiento de la herramienta desarrollada. | Falta de personal que brinde soporte a los aplicativos | Aplicación limitada de las herramientas informáticas desarrolladas | medio | moderado |
| | Desarrollo tecnológico herramientas | Obsolescencia de herramientas tecnológicas | Ausencia de herramientas tecnológicas | Desarrollo y aplicación de herramientas tecnológicas no autorizadas | medio | moderado |
| | Equipos de comunicaciones | Retraso en los enlaces de los equipos de comunicaciones | Daños presentados en los equipos de comunicaciones | Daños de los equipos de comunicaciones | alto | Catastrófico |
| | Red telefónica | Falta de comunicación entre empleados | Fallas en la red telefónica | Daños de la red telefónica | bajo | leve |
| | Internet | Comunicación no permanente la red | Conocimiento de información tardía | Cortes del servicio de internet | alto | Catastrófico |
| | Red Informática | La interceptación de información que es transmitida desde o hacia el sistema. | Penetración del sistema a través de la red | Intercepción de las comunicaciones | alto | Catastrófico |

***Anexo C. (Continuación)***

| CATEGORÍA DE ACTIVO | SERVICIO DE RED | VULNERABILIDAD | AMENAZA | RIESGO | PROBABILIDAD | IMPACTO |
|---|---|---|---|---|---|---|
| 2. Tecnología | Software | Presencia de software malicioso<br>Conflictos en los recursos compartidos | Instalación de programas innecesarios<br>Registro inadecuado de programas de Windows | Daños en software | medio | moderado |
| | Hardware | Presenta software malicioso | Falla en la memoria, fuente, disipadores, board, disco duro, etc.<br>Consumo de alimentos en las áreas de trabajo | Daños en Hardware | alto | Catastrófico |
| | Red | Administración de la red | Daños en los dispositivos de comunicación (rack, servidores, routers) | Fallas en la red | medio | moderado |
| | Sistemas de Información | Fallas en la administración de los aplicativos<br>Denegación del servicio a través de múltiples consultas concurrentes<br>Problemas en la oportunidad de la atención en los diferentes sistemas de información | Problemas en la configuración de los parámetros de seguridad del servidor del sistema de información<br>Falta de soporte y mantenimiento de fabrica<br>Fallas en los controles para el acceso físico a los servidores | Violación de los sistemas de Información | alto | Catastrófico |
| | Dispositivos de red | El constante cambio tecnológico genera que las herramientas adquiridas entren en inoperancia. | Referencia de repuestos descontinuados<br>Aceleración de nuevas tecnologías generando discontinuidad de las mismas en un corto periodo de tiempo | Obsolescencia Tecnológica | bajo | leve |

***Anexo C. (Continuación)***

| CATEGORÍA DE ACTIVO | SERVICIO DE RED | VULNERABILIDAD | AMENAZA | RIESGO | PROBABILIDAD | IMPACTO |
|---|---|---|---|---|---|---|
| 3. Seguridad Física | Hardware | Ausencia de Hardware | Falta de dispositivos para buen funcionamiento | Robos de hardware | bajo | moderado |
| | Infraestructura de red | Violación de autorización | Personas no autorizadas | Vandalismo | bajo | Moderado |
| | Infraestructura de red | Perdida de hardware | Riesgos físicos | Incendios | alto | Catastrófico |
| | Infraestructura de red | Perdida de equipos en funcionamiento | Daños en hardware y software | Terremotos | alto | Catastrófico |
| | Punto de energía eléctrica | Funcionamiento irreparable de dispositivos | Perdida del funcionamiento correcto de equipos | Fallas eléctricas | bajo | leve |
| | Hardware | Atrasos en el funcionamiento de los procesos | Perdida de la información almacenada | Fallas de hardware | alto | catastrófico |
| 4. Manejo de Personal | Acceso | Manipulación de datos confidenciales | Extracción de datos no autorizados | Accesos no autorizados | alto | catastrófico |
| | | Tenencia de información no autorizada. | Acciones sospechosas | Fraude | alto | catastrófico |
| | Identidad | Autorizaciones no verificadas | Accesos no autorizados | Suplantación de identidad | alto | catastrófico |
| | Autenticación | Intentos fallidos | Autenticación repetida | Fallas de autenticación | alto | catastrófico |
| | Personal | Eficiencia afectada | Rendimiento desmejorado | Indisponibilidad del personal | bajo | moderado |
| | Información | Obtención de información | Perdida de información | Fugas de Información | bajo | moderado |

***Anexo C. (Continuación)***

| CATEGORÍA DE ACTIVO | SERVICIO DE RED | VULNERABILIDAD | AMENAZA | RIESGO | PROBABILIDAD | IMPACTO |
|---|---|---|---|---|---|---|
| 5. Protección de la Información | Información | Obtención de información | Perdida de información | Robo de información | alto | catastrófico |
| | Información | Obtención de información | Perdida de información | Perdida de información | alto | catastrófico |
| | Información | Información no veraz | Personal involucrado, Información errada | Manipulación de información | alto | catastrófico |
| | Usuario | Entorpece funcionamiento | Demora en servicios ofrecidos | Errores de usuario | alto | catastrófico |
| | Información | Falta de información completa | Ausencia de información real disponible | Eliminación de información | alto | catastrófico |
| | Backup | Ante cualquier desastre la organización es perjudicada | Perdida de datos | No se encuentran definidas las políticas de copias de seguridad | alto | catastrófico |
| 6. Seguridad de la red | Archivos y programas | El estado de programas y archivos se ve afectado | Programas y archivos eliminados o cambiados | Acceso a los programas y archivos por parte de personal no autorizado | alto | catastrófico |
| | Destinatario | Extracción de información | Accesos de información por medio empleados | Información transmitida a un destinatario incorrecto | alto | catastrófico |
| | Programas y archivos | Vulneración y funcionamiento errado de la información | Funcionamiento errado | Modificación de los programas y archivos por parte de los usuarios | alto | catastrófico |
| | control de acceso | Información puesto es peligro | Vulneración de la privacidad de la información | Falta de software de control de acceso | alto | catastrófico |
| | virus | Vulnerable todo el sistema de información | Mal funcionamiento de software o hardware | Entrada de virus y malware | alto | catastrófico |

***Anexo D. RAE***

| **Resumen Analítico** | **RAE** |
|---|---|
| **Título de Documento.** | ANÁLISIS DE SEGURIDAD A LA RED DE DATOS DE LA EMPRESA ASISTIR COMPUTADORES DE LA CIUDAD DE BOGOTÁ |
| **Autor** | Raul Garcia Guacaneme |
| **Palabras Claves** | Seguridad informática, Seguridad Pasiva, Seguridad Activa, Riesgo, Usuario y Políticas de Seguridad. |
| **Descripción**<br><br>Se analizará la seguridad a la red de datos de la empresa ASISTIR COMPUTADORES de la ciudad de Bogotá, consultora e interventora de sistemas de información desarrollados bajo plataformas tecnológicas que incorporan el uso de hardware, software, módulos de integración, reportes y sistemas de consolidación y consulta, así como la definición de esquemas y políticas de seguridad informática a nivel de infraestructura empresarial.<br><br>En el presente proyecto se evaluaron los aspectos de seguridad y confiabilidad con que se llevan a cabo las operaciones de la transferencia de datos a través de la red, para determinar posibles vulnerabilidades. | |
| **Fuentes Bibliográficas** | GUIA PROPUESTA DE PROYECTO DE INVESTIGACION, Universidad Popular del Cesar en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/capitulo_3__analisis_de_riesgos.html |

CERTIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN con ISO/IEC 27001. Internet en: http://www.icontec.org/index.php/en/sectores50-colombia/certificacion-sistema/342-certificacion-iso-iec-27001

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

GUÍA A LA REDACCIÓN EN EL ESTILO APA, 6ta edición, recuperado el 5/03/2012. Disponible en: http://www.suagm.edu/umet/biblioteca/pdf/GuiaRevMarzo2012APA6taEd.pdf

GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA, Internet en: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. NTC-ISO/IEC 27001:2005. Bogotá D.C. El instituto 37p.

NORMA TECNICA COLOMBIANA, NTC 1486, en PDF. Presentación de tesis, trabajos de grado y otros trabajos de investigación, Modulo Icontec.

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Accessed 2016].

**Contenido:**

Seguridad Informática de la Empresa
Sistema de Gestión de la Seguridad de la información.
Seguridad informática en bases de datos.
Seguridad informática en redes.
Identificación de activos.
Plan de Contingencia.

Se desarrollaron los siguientes objetivos:

**OBJETIVO GENERAL**

Realizar un análisis de seguridad a la red de datos de la empresa ASISTIR COMPUTADORES de la ciudad de Bogotá, para conocer el estado actual de la red y realizar las recomendaciones de mejora pertinentes.

**OBJETIVOS ESPECÍFICOS**

- Levantar información pertinente que sirva de insumo para llevar a cabo la ejecución del presente proyecto.
- Identificar los activos de información que conforman la red de datos de ASISTIR COMPUTADORES.
- Instalar herramientas de gestión de seguridad y realizar las pruebas de detección de vulnerabilidades acordadas.
- Realizar el informe sobre las vulnerabilidades encontradas y las recomendaciones de mejora relacionadas con la seguridad de información de la red para la empresa ASISTIR COMPUTADORES.

**Metodología**

Se realizará una indagación de las políticas de seguridad implementadas por la organización para determinar si son suficientes e identificar las posibles vulnerabilidades a la red de datos y además se establecerá si hay la necesidad de implementar nuevas políticas de seguridad al interior de la entidad.

**Conclusiones**

La empresa debe invertir en recurso económico periódicamente para que todo el personal de la empresa reciba una adecuada capacitación y actualización periódica en materia de seguridad informática y de los riesgos a que está expuesta su red de comunicación de datos.

| |
|---|
| Todo el personal de la empresa tanto interno como externo que manipule información confidencial y sensible de la empresa, debe comprometerse a protegerla, para evitar fugas de información, la cual pueda ser utilizada indebidamente. |
| **Recomendaciones**<br>Los funcionarios y empleados adquieren las responsabilidades y cuidados que se deben tener al manipular información confidencial de la empresa.<br>Los empleados deberán tomar conciencia del uso del correo electrónico, del riesgo a que están expuestos por el mal uso del mismo.<br>Se requiere contar con tareas periódicas de monitoreo de la base de datos para identificar usuarios en desuso.<br>Difundir las políticas de riesgos tanto a las directivas como a los empleados de las diferentes áreas de la empresa.<br>El departamento de seguridad informática está encargado de que todos los empleados cumplan con las políticas de seguridad implementadas.<br>La empresa deberá hacer cumplir la política de control de acceso a las instalaciones, definir el perímetro de seguridad física, establecer mecanismos de protección contra amenazas externas.<br>Se borrara el software inútil y se dará buen uso de los recurso informáticos. |