ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE DEFENSA CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO EN LA RED PARA UNA EMPRESA DE SERVICIOS."

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

KAROL PAMELA BRIONES FUENTES
OMAR ANTONIO CÓRDOVA BALÓN

GUAYAQUIL – ECUADOR

2015

AGRADECIMIENTO

A Dios,

A nuestras familias.

DEDICATORIA

A nuestras familias.

TRIBUNAL DE SUSTENTACIÓN

MSIG. LENIN FREIRE COBO
DIRECTOR DEL MSIA

MSIG. ROKY BARBOSA
DIRECTOR DE TESIS

MSIG. ALBERT ESPINAL SANTANA
MIEMBRO PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y, el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

ING. KAROL BRIONES FUENTES

CI 0921279162

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y, el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

ING. OMAR CORDOVA

CI 0922892161

RESUMEN

Internet ha revolucionado la forma en que operan los negocios en la actualidad. Gran cantidad de datos son transmitidos a nivel mundial en tiempo real, como es el caso de las compañías en línea, las cuales dependen de la disponibilidad de sus servicios las veinticuatro horas del día, los trescientos sesenta y cinco días del año para que sus clientes se mantengan conectados de diversas maneras y sin interrupciones. Pero, este nuevo mundo de mayores velocidades, grandes volúmenes de datos y alta disponibilidad de los servicios, trae consigo oportunidades para los criminales cibernéticos, cuyo objetivo es aprovechar el mínimo fallo en los sistemas que operan dentro de la gran red mundial. Estos competidores maliciosos, crean dependencias entre la velocidad y disponibilidad de los servicios en internet en contra de sus propietarios, en otras palabras, crean mecanismos de ataque que impiden el acceso normal a los servicios de la empresa, a este tipo de mecanismos se les denomina Ataques de Denegación de Servicios.

La Denegación de Servicios (o DoS por sus siglas en inglés Denial of Services), es un ataque que pone en riesgo la disponibilidad de los servicios en la red y que ha existido por más de veinte años, modificando su forma de actuar de manera constante pero siempre cumpliendo su objetivo original.

En la actualidad, los ataques de Denegación de Servicios han evolucionado notablemente, agregando nuevos mecanismos de evasión que les permite atacar dispositivos de protección de red tanto perimetrales como locales de manera eficaz. Debido a esto, los fabricantes de los dispositivos de protección (Cortafuegos, Detectores de Intrusos, entre otros), incluyen en los equipos un cierto nivel de inteligencia que les permite detectar comportamientos que no se consideran normales dentro de la organización, obligando de esta manera a los criminales cibernéticos a necesitar diversos vectores de ataques simultáneos para llevar a cabo su fin.

A esta modalidad de ataques se les denomina Ataques de Denegación de Servicio Distribuido (o DDoS por sus siglas en inglés Distributed Denial of Services). Este tipo de ataques es relativamente nuevo, tiene sus orígenes

entre finales de junio e inicios de julio de 1999. Un Ataque de Denegación de Servicios Distribuidos es un ataque coordinado y a gran escala, que actúa sobre la disponibilidad de los servicios en un sistema o recursos de red de una organización considerada como víctima, enviados remota e indirectamente a través de muchos ordenadores comprometidos conectados a Internet. La inundación de mensajes entrantes al sistema comprometido afecta su disponibilidad causando una caída forzada, de esta manera deniega el servicio a los usuarios legítimos que realmente requieren hacer uso del sistema.

Por lo antes expuesto, las empresas se ven obligadas a reforzar las seguridades en su red, estableciendo mecanismos de defensa que ayuden a minimizar los riesgos de seguridad de información y garantizar la disponibilidad de los servicios publicados.

Es por este motivo que la implementación de un sistema de defensa contra ataques de Denegación de Servicio Distribuido debe ser la prioridad en toda empresa de misión crítica, siempre acompañado de un conjunto de Políticas de Seguridad claras y prácticas, que permitan la correcta interpretación y

utilización de los recursos de la empresa, para que, de esta forma, sean de ayuda y permitan mantener la disponibilidad de los servicios de manera efectiva.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

ACL	Access Control List
BSD	Berkeley Software Distribution
CERT	Coordination Center in response to the Morris worm incident
CPU	Central Processing Unit
DDoS	Distributed Denial of Services
DNS	Domain Name System
DoS	Denial of Services
FTP	File Transfer Protocol
GNU GPL	GNU General Public License
GRE	Generic Routing Encapsulation
HOIC	High Orbit Ion Cannon
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HULK	HTTP Unbearable Load King
ICMP	Internet Information Services
IDS	Intrusion Detection System
IIS	Internet Information Services
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System

IRC	Internet Relay Chat
IRC Bots	Robots de Canales IRC
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
LOIC	Low Orbit Ion Cannon
NMAP	Network Mapper
QoS	Quality of Service
RUDY	R-U-Dead-Yet
SLA	Service Level Agreement
SMTP	Simple Mail Tranfer Protocol
TCP	Transmission Control Protocol
TCP	Transmission Control Protocol
TI	Tecnologías de la Información
TICs	Tecnologías de la Información y Comunicaciones
TTL	Time-to-Live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoIP	Voice Over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WEB	World Wide Web (WWW) o Red

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo de Tesis mostrará el diseño y la implementación de un sistema de defensa contra ataques de Denegación de Servicio Distribuido, a una empresa de servicios, la cual se encuentra presuntamente afectada por este tipo de ataques. El sistema de defensa estará basado en herramientas propietarias y de distribución libre, que en su conjunto se complementan para cumplir los objetivos planteados.

Es importante mencionar que este tipo de sistemas de protección no estarían completos sin un conjunto de Políticas de Seguridad que permitan llevar a cabo una serie de procesos y procedimientos para validar continuamente la seguridad de la red.

Durante el desarrollo, en el capítulo dos, revisaremos los temas conceptuales que se encuentran relacionadas a la Denegación de Servicios Distribuidas, en

donde notaremos que su comportamiento es considerado una extensión de la Denegación de Servicios, agregando el concepto “Distribuido” por tratarse de peticiones provenientes de varias fuentes (equipos infectados) con agentes de ejecución de código remoto, que de manera coordinada actúan al unísono hacia un solo objetivo.

Luego tendremos en el capítulo tres, la clasificación de los ataques de Denegación de Servicio Distribuidos, diferenciándose cada uno por su forma de actuar. Brevemente observaremos que el término Interrupción se encuentra presente en estos ataques dado que puede afectar a su víctima en la disponibilidad, confidencialidad, integridad y autenticidad de los servicios.

Seguidamente en el capítulo cuatro, nos dedicaremos a la recolección de información de los equipos de comunicación, servidores y servicios de la empresa, relacionados a la afectación de la Denegación de Servicios Distribuida. Una vez realizada la recolección de información y con un mapa completo de la arquitectura de la red organizacional, se procederá a generar una solución acorde a las dimensiones tecnológicas de la empresa, estimando

riesgos, niveles de protección, análisis en línea para la detección de ataques y su plan de respuesta ante incidentes presentados.

Esta solución propuesta tendrá la oportunidad de ser implementada, y es por esto que, en el capítulo quinto, realizaremos tanto la implementación como las pruebas de funcionalidad que han sido diseñadas específicamente para la empresa de servicios.

Los resultados de la implementación y pruebas efectuadas serán posteriormente revisadas en el capítulo sexto, donde estudiaremos las mejoras obtenidas con este nuevo sistema de protección. Es posible que dentro de los resultados se detecte algún comportamiento considerado como falso positivo, por lo cual este capítulo involucra un análisis más exhaustivo.

Para finalizar, efectuaremos las debidas recomendaciones y señalaremos las conclusiones del estudio realizado en la empresa de servicios.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

La Empresa de Servicios, que por razones de confidencialidad de su seguridad lógica no se puede mencionar su nombre, está enfocada en proveer soluciones integrales en el área de Tecnologías de la Información y Comunicaciones (TICs), brindando servicios de consultoría, asesoría, implementación, soporte y mantenimiento. Cuentan con más de quince años de experiencia en el mercado y se identifican como una empresa en constante innovación y crecimiento, lo que le ha permitido obtener altos reconocimientos de marcas como DELL – EMC2.

La matriz de la Empresa de Servicios está ubicada en el centro de la ciudad de Quito y tiene dos sucursales, una al norte de la ciudad de Guayaquil y otra en la ciudad de Bogotá. Actualmente cuenta con clientes en todo el Ecuador y Latinoamérica, principalmente empresas de Banca, Gobierno, Telecomunicaciones y Educación.

Desde el segundo semestre del año 2014, la empresa ha estado experimentando lentitud en sus servicios tales como el Portal Web y Correo Electrónico, por lo que preocupados en conocer el motivo por el cual se presenta este tipo de problemas y en validar si las medidas de seguridad implementadas en su ambiente de producción son suficientes para proteger la infraestructura de la empresa, nos contactaron para realizar el análisis de la situación actual de la red, evaluar sus medidas de seguridad tanto físicas como lógicas y de manera específica verificar lo que sucede dentro de la red de su infraestructura empresarial.

La Empresa de Servicios posee su propia infraestructura de procesamiento la cual se encuentra ubicada en el edificio matriz. Este tipo de empresas, donde los servicios se procesan sobre equipos que se sitúan dentro de sus instalaciones, son el tipo de empresa ideal para este estudio, por lo que ofrecen una mayor apertura a las evaluaciones de seguridad informática.

Dentro de nuestro país, a nivel empresarial específicamente, existe una práctica muy común, la cual trata de darle poca prioridad a la seguridad de los sistemas y servicios que forman parte del desarrollo de la continuidad del negocio. Este no es el caso de la Empresa de Servicios objeto de este estudio.

1.2 Descripción del Problema

Debido a los inconvenientes en lentitud de respuesta de los servicios de la empresa, tales como el servicio de correo electrónico y portal web en los cuales se basa su procesamiento principal, la Empresa de Servicios nos ha solicitado una revisión de la red en su infraestructura empresarial.

De los problemas que están experimentando, indican que usualmente en días laborables específicamente durante la madrugada entre 01:00 am y 06:00 am y en el día en horarios de 10:00 am a 12:00 pm, el servicio de correo electrónico y el portal web se vuelven lentos y en algunos casos dejan de responder, causando una interrupción en la disponibilidad del servicio. A pesar de contar con una infraestructura protegida por un Cortafuegos (Firewall) y un Sistema de Prevención de Intrusos (o Intrusion

Prevention Systems por sus siglas en inglés IPS), estos no reportan ninguna anomalía en la red.

Realizando una revisión de los registros del tráfico de la red de datos empresarial, podemos observar un incremento de tráfico durante los horarios de lentitud de los servicios indicados anteriormente por el personal de la empresa. En el Servidor de Correo Electrónico se pueden ver registros de conexiones externas a la red de datos empresarial por el puerto TCP-25 o Protocolo de Control de Transmisión 25 para la transferencia de correos (Transmission Control Protocol por sus siglas en inglés TCP), de igual forma en el Servidor de Aplicaciones Web, se pueden ver conexiones hacia los puertos TCP-80 (Puerto usado para la transmisión de páginas web) y TCP-443 (Puerto usado para la transmisión segura de páginas web).

Estos aumentos de tráfico en la red también generan degradación del servicio de navegación hacia portales web de las marcas asociadas, impidiendo en algunos casos la ejecución normal de las herramientas utilizadas en áreas como Ventas y Soporte Técnico.

Entre otros problemas evidenciados, está el que no cuentan con una Política empresarial de Seguridad de la Información que le permita llevar un mejor control de su infraestructura e información crítica.

Ningún tipo de empresa está libre de ser víctima de los ataques informáticos y la mayoría tiende a ser vulnerable. Incluso aquellas empresas que realizan grandes inversiones en recursos y en expertos en el tema de la seguridad, pues ya han sido víctimas de ataques informáticos, tal es el caso de empresas como Sony, Amazon, Paypal, entre otras.

Actualmente los atacantes no solo buscan obtener información confidencial de las empresas, buscan poner en riesgo la operatividad de la misma y con ello paralizar sus operaciones. Para empresas que proveen servicios en línea o para aquellas de las cuales su negocio depende únicamente del comercio electrónico, ser víctima de un ataque informático se traduciría en pérdidas económicas enormes. En el caso de empresas de servicios, de las cuales su imagen depende de la operatividad de su sitio web y la recepción de los correos electrónicos, una afectación de este tipo resultaría en la pérdida de credibilidad y confianza de sus clientes.

En resumen, podemos indicar que la Empresa de Servicios presenta los siguientes problemas:

- Lentitud en sus servicios de correo electrónico y portal web en horarios ya identificados.
- No cuenta con Políticas de Seguridad de la Información.
- Su red empresarial está expuesta a ataques informáticos.

De acuerdo a las revisiones realizadas y al patrón de comportamiento de la red, es posible que estemos frente a un ataque de Denegación de Servicios Distribuido (o DDOS, Distributed Denial of Services por sus siglas en inglés).

1.3 Solución Propuesta

La Empresa de Servicios, preocupada por la seguridad de su información, tiene dispositivos de protección que le ayudan a rechazar el tráfico considerado como malicioso, sin embargo, estos equipos no poseen mecanismos de inteligencia para analizar el tráfico normal invasivo. Los dispositivos de protección actual comprenden Cortafuegos, Sistema de Prevención de Intrusos, equipos de comunicación, servidores y estaciones.

La solución propuesta se basa en la implementación de un Sistema de Defensa contra Ataques de Denegación de Servicio Distribuido, en conjunto con la definición de políticas de seguridad. Este sistema de defensa está compuesto por un Sistema de Detección (Anti DDOS), un Mecanismo de Redirección y un Sistema de Mitigación, tal como se muestra en la Figura 1.1.

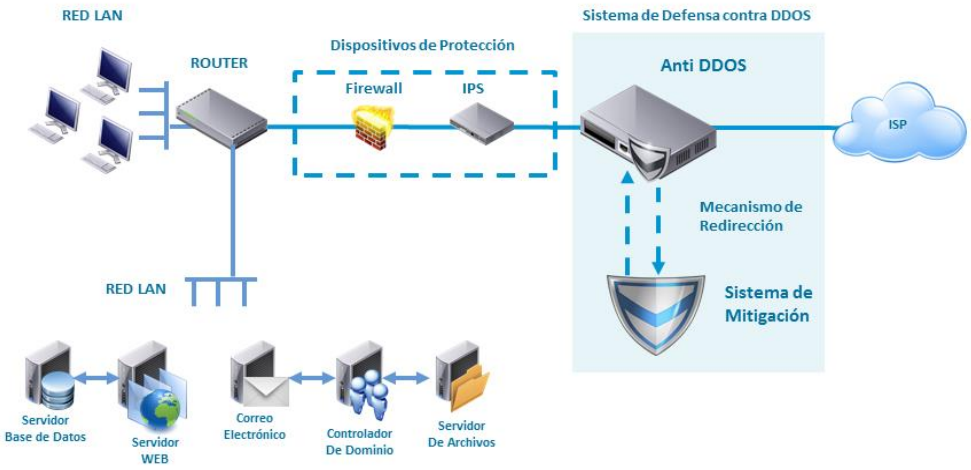


Figura 1.1 Esquema de red de la solución Anti DDoS propuesta para la Empresa de Servicios.
Fuente: Autoría propia

El Sistema de Defensa, será el encargado de detectar y analizar las anomalías en el tráfico que ingresa a la red. Este sistema está situado en el perímetro de la red recibiendo todo el tráfico enviado por los Proveedores de Internet (o Internet Service Provider por sus siglas en

inglés ISP). Cuando se detecta tráfico anómalo o intentos de inundación en la red, el tráfico será gestionado por el Mecanismo de Redirección.

El Mecanismo de Redirección se inicia cuando existe tráfico no legítimo. Consiste en enviar el tráfico recibido hacia una nueva ruta o dirección, de tal forma que el tráfico dirigido a las direcciones de internet del servidor de correos y del servidor web, se dirija al Sistema de Mitigación con la finalidad de evitar la saturación en los servicios de correo y web.

El Sistema de Mitigación está compuesto por dispositivos de red que reciben todo el tráfico dirigido por el Mecanismo de Redirección. Es el encargado de separar el tráfico legítimo del no legítimo, lo cual se realizará mediante análisis estadístico. Luego se encargará de retornar un tráfico “limpio” o legítimo mediante túneles GRE (Generic Routing Encapsulation) cifrado. Los Sistemas de Mitigación tienen la característica de poder gestionar grandes cantidades de tráfico, y son generalmente provistos por servicios externos especializados, de tal forma que son difíciles de saturar mediante ataques típicos.

Mediante esta solución se puede brindar una capa adicional de protección a los sistemas contra ataques de Denegación de Servicio Distribuido, ya

que evitamos que la red sea saturada mediante la separación de tráfico malicioso del tráfico legítimo.

La solución planteada se basa en implementar el Sistema de Defensa contra ataques de Denegación de Servicio. Los dispositivos de protección actuales, tales como Cortafuegos (Firewall) y el Sistema de Prevención de Intrusos (IPS), se convierten en capas adicionales de protección, no pueden ser descartados de una Infraestructura de Seguridad, sino que a su vez la complementan.

El beneficio de la implementación de este sistema de defensa es mantener los servicios de la empresa siempre protegidos contra ataques de Denegación de Servicios, garantizando una operatividad estable y confiable para así mantener la imagen empresarial. El sistema será capaz de analizar el tráfico hacia los servicios actuales y los servicios que se presenten a futuro durante el crecimiento de la empresa. Se podrán obtener los datos estadísticos acerca de los eventos de ataques de tal manera que se pueda llevar un control de acuerdo a las políticas implementadas.

1.4 Objetivo General

Diseño e Implementación de una solución que integre un conjunto de elementos de seguridad para la Prevención, Detección y Mitigación de ataques de Denegación de Servicio Distribuido en la Red para una empresa de servicios.

1.5 Objetivos Específicos

- Identificar el problema presentado en la Empresa de Servicios y proponer una solución.

- Establecer la base teórica que servirá de guía para el diseño de la solución propuesta.

- Analizar la situación actual de la Empresa de Servicios.

- Diseñar una solución que integre elementos de seguridad que actúen como mecanismo de defensa contra ataques de Denegación de Servicio Distribuido.

- Implementar la solución propuesta como prueba del diseño de seguridad planteado.

- Presentar el análisis de los resultados de las pruebas realizadas en base a la solución implementada.

1.6 Metodología

La metodología a seguir durante el presente trabajo de Tesis, se basa en dos tipos de investigación: Exploratoria y Explicativa, las cuales serán aplicadas para analizar la situación actual de la Empresa de Servicios en lo que respecta a su seguridad lógica, luego podremos determinar los problemas de seguridad que existan, y finalmente mostraremos los resultados de la investigación en conjunto con las soluciones implementadas y las propuestas de mejoras que complementarán el trabajo realizado.

Durante la investigación, se mantendrá el contacto directo con la Empresa de Servicios, específicamente con el área de Tecnologías, la cual es la más afectada y la que está a cargo de toda la infraestructura tecnológica. Se obtendrá información a partir de los registros de datos de todos los dispositivos de seguridad, servidores y estaciones de trabajo de la

empresa, es decir, se realizará un trabajo de campo minucioso para la recolección de información que servirá de base para todo el proceso investigativo.

Se tomarán como referencias las recomendaciones brindadas por la División de Preparación para Emergencias Informáticas del Instituto de Ingeniería de Software (CERT Division, Software Engineering Institute) [1], así como normas de seguridad físicas y lógicas proporcionadas por la norma ISO 27002:2013, con la finalidad de obtener una guía que permita presentar la información de manera clara, correcta y precisa.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Ataques Informáticos

Los ataques informáticos son una agresión contra la seguridad de la información de una empresa, y que dependiendo de su éxito o fracaso podría traer consigo grandes problemas.

Los servicios en línea sufren ataques informáticos por diferentes técnicas cuyo objetivo es dejar las redes y sistemas empresariales improductivos.

Un ataque informático trata de aprovechar alguna falla o las debilidades existentes dentro de un software, un hardware o inclusive de una persona,

todo esto con el fin de obtener beneficios, en la mayoría de los casos del tipo económico, causando un efecto negativo en la seguridad de un servicio o sistema generando así un riesgo para la organización.

Existen varios tipos de ataques informáticos que han sido reportados, por ejemplo:

- Extracción, duplicación o filtrado de datos sin autorización
- Manipulación de datos (cambios no autorizados en los datos)
- Destrucción y eliminación de información crítica
- Descarga desde fuentes no autorizadas o uso de software inapropiado que contiene código malicioso
- Escuchando el tráfico de la red (Sniffing)
- Suplantación de identidad (Spoofing)
- Ingeniería social
- El mal uso de los recursos para actividades no relacionados con el negocio o no autorizados
- Instalación de software malicioso a propósito

Cada una de estas acciones pueden considerarse maliciosas, pero no todas dejan un rastro (referenciado en los sistemas y servicios como registro log) que sirvan para ser rastreadas, muchas de las veces se

encuentran registros de acciones no relacionadas al ataque sucedido, con el fin de crear una distracción sobre lo que realmente se está efectuando.

Para disminuir el impacto generado por ataques informáticos, varias instituciones han definido procedimientos y mejores prácticas que facilitan al personal de IT a combatir, en una constante lucha, las actividades delictivas hasta reducir notablemente el campo de acción.

Los ataques informáticos pueden ser minimizados mediante la educación del personal de IT, es muy importante conocer las debilidades más comunes y básicas que podrían aprovechar los atacantes y cuáles son los riesgos presentes, para luego desplegar una solución inteligente mediante estrategias de seguridad efectivas y equipamiento informático.

2.2 Ataques de Denegación de Servicios

Los ataques de Denegación de Servicios funcionan en diferentes formas, pero de manera común, el atacante DoS selecciona un sistema de destino previsto y pone en marcha un ataque especializado contra el sistema destino, buscando llevar al sistema y la red a un estado inutilizable o inaccesible, esto lo puede realizar generando una saturación de recursos o inclusive causar errores catastróficos que detengan en su totalidad la

ejecución de procesos o sistemas completos. Mientras se efectúa el ataque, el servicio o sistema afectado pasa a un estado “no disponible” y temporalmente pierde su conectividad a través de la red, dejando a los usuarios clientes sin acceso. Los ataques DoS pueden llegar a incapacitar a una red completa, especialmente donde la comunicación de servicios y sistemas están basados en una comunicación mediante el protocolo TCP / IP (Transmission Control Protocol / Internet Protocol).

Los ataques de Denegación de Servicios en las redes corporativas han generado daños a la productividad y los ingresos, puesto que tienen la habilidad de llegar a corromper el software de un servidor. Los ataques pueden ser lanzados hacia cualquier tipo de plataforma de hardware o sistemas operativos, ya que generalmente tienen como base la comunicación mediante el Protocolo de Internet (IP). El sistema operativo favorito usado para ejecutar las herramientas de ataques suele ser Linux, y desde este sistema operativo se apunta a varios sistemas operativos víctimas. Una vez realizado un ataque, los desarrolladores del mismo evolucionan la forma de acción del ataque en periodos cortos de tiempos, referenciando un máximo de dos semanas, con el fin de que no sean identificados.

Las ejecuciones de los ataques de Denegación de servicios son cada vez más fáciles de efectuar, inclusive para las personas que no tienen conocimientos profundos de informática, ya que los programas o software de ataque, actualmente poseen de una interfaz gráfica en la que solo se siguen una serie de instrucciones para poner en marcha un ataque.

Debido al impacto crítico que los ataques de Denegación de Servicios pueden representar para una organización, no pueden tomarse a la ligera. Estos ataques han existido desde la década de 1980, intensificando por el continuo crecimiento del uso de las redes internas empresariales y de internet.

Una prevención exitosa y defensiva hacia estos ataques se puede obtener cuando se presente una cooperación por parte los proveedores de servicios de internet (ISP - Internet Service Provider), sistemas conectados en todo el mundo, software antimalware inteligente capaz de detectar anomalías en la red y desde luego una cultura de los usuarios al mantener sus sistemas actualizados.

Se podría pensar en los efectos de un ataque de DoS en términos de la productividad o del costo financiero que representa para una empresa, sin embargo definirlo por un valor acertado no es posible de forma general, ya

que para el caso de una interrupción en un solo proceso crítico de una empresa puede representar alto costo, mientras que para una empresa donde su red organizacional se vuelve inaccesible para los usuarios internos y no puede operar de manera normal, pues representa un bajo costo. Además, el tema se torna delicado al momento de definir pérdidas que sufre una empresa por un ataque de DoS ya que esto representa una publicidad negativa la cual podría disminuir su cuota de mercado.

2.3 Ataques de Denegación de Servicios Distribuidos

El ataque de Denegación de Servicios se basa en solicitar un recurso en grandes cantidades hasta que el servidor no pueda atender más solicitudes. Sin embargo, esta técnica ya no es efectiva debido al desarrollo de cortafuegos (Firewalls) y equipos de detección y prevención de intrusos (IDS - IPS) que controlan puertos y cantidad de ancho de banda empleada para satisfacer a un cliente. En el momento que se detecta que hay excesivas peticiones se procede a bloquear las solicitudes provenientes de dicho cliente. Además, estos equipos actualmente pueden detectar la procedencia del ataque y verificarlo en su base de firmas con la cual identifican rápidamente y registran el ataque que es bloqueado al instante. Es por esto que la denegación de servicios puede ser útil solo para los sistemas que se desarrollen ya que puede servir para realizar pruebas.

Para mantener una alta solicitud de recursos a un servicio, el atacante ya no puede realizarlo desde una sola fuente, porque será bloqueada instantáneamente, para esto se ha perfeccionado esta técnica involucrando muchas fuentes, con el fin de que cada una de las fuentes efectúe solicitudes que los equipos consideren un comportamiento normal hacia un solo destino. Es decir, el ataque será realizado por dos o más

equipos utilizando direcciones IP’s diferentes. Así, la posibilidad de efectuar este comportamiento es teniendo el control de varios equipos de diferentes puntos alrededor del mundo, mientras mayor es la cantidad de equipos involucrados en el ataque, es más difícil identificarlo y es más eficiente el ataque. En la mayoría de los casos, los atacantes buscan equipos inseguros, toman control de ellos y los administran para enviar un ataque de DDoS.

Las herramientas para realizar DDoS se encuentran disponibles para descarga gratuita realizando la búsqueda en el internet, sin embargo, un ataque de DDoS requiere un mayor grado de preparación y compromiso para un atacante. Generalmente un ataque de DDoS se puede dividir en tres etapas. La primera etapa consiste en identificar y reclutar a los equipos que participaran en el ataque, luego, en la segunda fase, el atacante debe crear canales de comunicación hacia estos equipos, y finalmente la última fase es poner en marcha el ataque.

Durante la fase de reclutamiento de computadores, se incluyen todos aquellos equipos que han sido previamente infectados previamente por malware (del inglés Malicious Software), estos equipos serán conocidos como zombis. El número de zombis, o cantidad de computadores infectados que pueden ser administrados por los atacantes para enviar un

ataque de Denegación de Servicios, varía en función al tipo de ataque, la resistencia o protección del servicio atacado y de la voluntad del atacante. Por lo general los atacantes forman los zombis infectando o comprometiendo computadores que tienen un nivel alto de recursos, esto significa que son equipos que tienen: alto nivel computacional, conexión a internet de alta velocidad y de bajo nivel de seguridad.

La primera etapa del reclutamiento de equipos zombis es escanear los ordenadores vulnerables conectados a internet. En los primeros días la exploración se realizaba manualmente por los atacantes, pero hoy en día se han desarrollado métodos de escaneo y software que permita realizar este trabajo de forma automatizada. En primer lugar, se puede usar algunas herramientas de escaneo como nmap, otorgando resultados con información de ordenadores conectados y sus direcciones. Por otro lado, el atacante puede usar robots de canales IRC (IRC Bots) es decir, programas que se ejecutan en segundo plano y que examinan las comunicaciones de IRC para realizar escaneos así mismo. Otra opción es el uso de los gusanos de internet (del inglés Internet Worms), programas que son hechos con el objetivo de replicarse ellos mismo y expandirse a través de la internet, con el fin de buscar vulnerabilidades en equipos de cómputos y luego informar al atacante.

Después de haber explorado el internet en busca de computadoras vulnerables, el atacante tiene que tomar el control de ellos a fin de coordinarlos y lanzar el ataque. Pero antes, el atacante tiene que explotar la vulnerabilidad específica y obtener el control total del sistema operativo. En la mayoría de las vulnerabilidades descubiertas, se debe obtener el mayor permiso posible, es decir, permisos de administrador. Es conocido que los proveedores de software están continuamente emitiendo parches de seguridad con gran rapidez ante los agujeros de seguridad que se descubran en sus sistemas, por esto el atacante debe actuar con rapidez antes que el proveedor de software descubra su vulnerabilidad, tema que actualmente lo conocemos como ataque de día cero. Luego de que la vulnerabilidad ha sido explotada por el atacante, se envía el detalle a la comunidad de atacantes (del inglés Hacker), y se convierte en un computador infectado disponible para cualquier atacante que lo necesite, hasta que el proveedor de software libere una actualización del sistema, cerrando la brecha de seguridad que ha sido ganada por el atacante. Los atacantes llaman a esos equipos como ya lo hemos previamente mencionado, zombis o agentes.

En la segunda fase del ataque de Denegación de Servicio Distribuido, es el establecimiento de canales de comunicación entre los zombis y el atacante. Esta comunicación tiene dos objetivos específicos. La primera

razón es para coordinar los demás zombis y organizar el ataque, y la segunda razón es para recoger datos sobre el sistema objetivo. La comunicación puede realizarse a través de redes controlador/zombi o canales de comunicación IRC.

Las primeras herramientas DDoS estaban usando el método Controlador/Agente, para proporcionar canales de comunicación entre atacante y los ordenadores zombis. El atacante, también llamado Cliente, selecciona de entre los ordenadores zombis cuáles serán los agentes y cuáles los controladores. Luego, a cada controlador se le asignan varios agentes. El atacante envía los comandos a los controladores y estos luego los transfieren a los agentes. Esta comunicación se realiza mediante los mecanismos comunes de internet, a través de protocolos TCP / IP, UDP o paquetes ICMP. Cada herramienta utiliza puertos específicos para la comunicación, por ejemplo, la herramienta Stacheldraht, utiliza el puerto 16660 para la comunicación entre el atacante y los controladores. Esta explicación se puede ilustrar en la Figura 2.2.

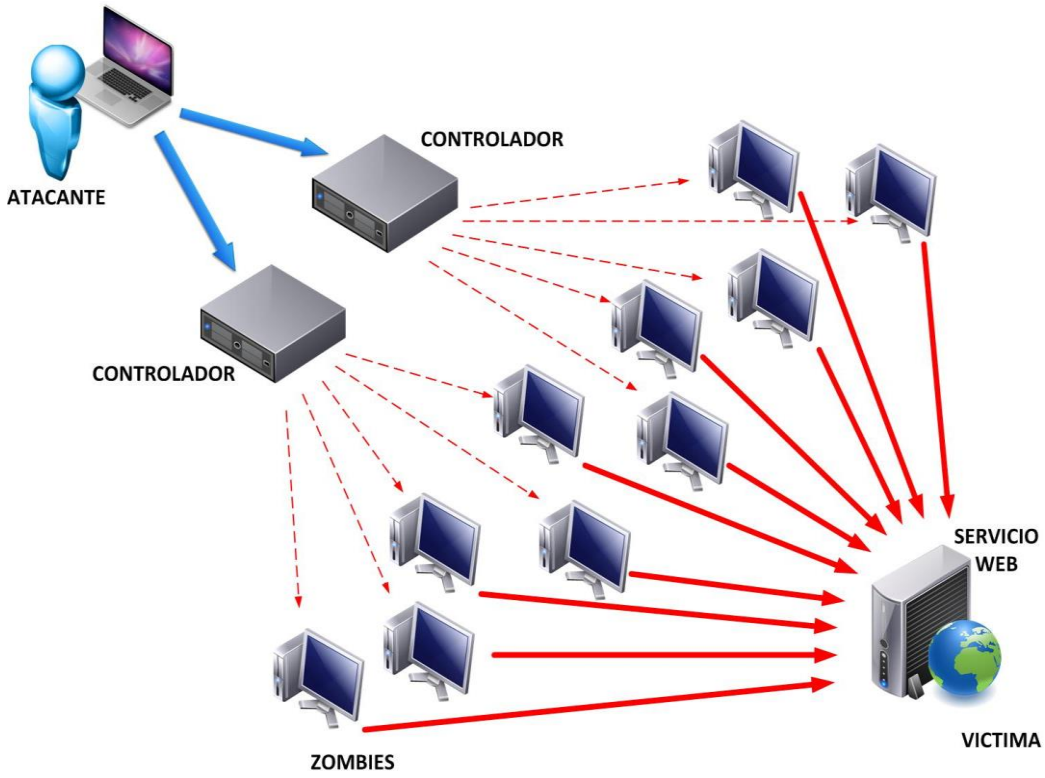


Figura 2.2 Estructura de un ataque de Denegación de Servicios Distribuidos.
Fuente: Autoría propia

La segunda técnica de comunicación entre atacante y zombi es el uso de canales IRC (del inglés Internet Relay Chat). La herramienta Trinity, fue la primera en ser descubierta en usar este tipo de comunicación. Su funcionamiento radica en que el atacante y los zombis se encuentran dentro de un mismo canal IRC y se comunican a través de este mismo. Este esquema mantiene algunas ventajas, las cuales, en primer lugar, el atacante no necesita tener un servidor definido como sucede en el modo Controlador/Agente, ya que esta función la realizará el servidor de IRC.

Esto también ofrece anonimato y hace que los análisis forenses sean un proceso difícil de seguir. Además, todos los ordenadores zombis participan en el ataque utilizando el mismo canal, lo que se traduce como rapidez y facilidad de administrar los agentes.

La tercera fase de la Denegación de Servicios Distribuida es el lanzamiento real del ataque. Hay varias decisiones que deben ser consideradas en esta fase. El atacante tiene que determinar el objetivo o los objetivos del ataque y su duración. El momento de esta decisión se basa en la herramienta a utilizar. Algunas herramientas permiten al controlador enviar el ataque definiendo el inicio inmediato o programando la fecha y el destino. Por otra parte, queda a decisión del atacante mantenerse conectado a los zombis o desconectarse de ellos para mantenerse en anonimato o correr el riesgo de ser detectado.

Una forma común de efectuar un ataque consistiría en saturar al servicio “víctima” con peticiones de comunicaciones externas, de tal forma que no pueda responder al tráfico legítimo de los usuarios, o que responda tan lentamente que lo lleva a un estado de “no disponible”. Estos ataques llevan a una sobrecarga de servidor. Hay países como Reino Unido donde estos ataques son penalizados con 10 años de prisión en registro de ley (Police and Justice Act 2006) [2] y en Estados Unidos de igual manera es

considerado un crimen federal bajo el concepto de Fraude Computacional (Computer Fraud and Abuse Act) [3] que igualmente incluye años de prisión.

2.4 Origen del ataque de Denegación de Servicio Distribuidos

Los ataques de DoS han existido por décadas bajo una serie de nombres. Pero los ataques de DDoS son mucho más actuales. A finales de junio e inicio de julio de 1999, un grupo de hackers estaban instalando y realizando pruebas de una herramienta de DDoS llamada Trinoo, para lanzar medianos y grandes ataques de DDoS. Las pruebas involucraron la participación de más de 2000 sistemas computacionales involucrados con objetivos definidos en todo el mundo.

La mayor cantidad de documentos que hacen referencia a los inicios de DDoS a larga escala concuerdan que este se produjo en agosto de 1999, cuando Trinoo se desplegó por lo menos en 227 sistemas (de los cuales 114 estaban en Internet2), para inundar un solo sistema de la Universidad de Minnesota, el cual estuvo fuera de servicio por más de dos días.

El 28 de diciembre de 1999, el CERT/CC emitió un comunicado con recomendaciones sobre DDoS, CA-1999-17 [4].

El 7 de febrero del 2000, la empresa Yahoo! fue víctima de un ataque de DDoS durante el cual su portal de internet estuvo inaccesible durante tres horas. El 8 de febrero, otras empresas como Amazon, Buy.com, CNN y eBay, fueron atacados con DDoS causando la paralización de sus servicios o en algunos casos, la ralentización. Y el 9 de febrero en el mismo año 2000, E*Trade y ZDNet, ambas sufrieron ataques de DDoS. Los analistas estiman que durante las tres horas que estuvo sin servicio Yahoo!, este tuvo pérdidas de comercio electrónico y de ingresos por publicidad que ascendieron a los $500.000. De acuerdo con el anuncio de Amazon, el ataque que sufrió resultó en una pérdida de $600.000 durante las 10 horas que estuvo sin servicio.

Durante los ataques de DDoS, Buy.com, una empresa con 100% de disponibilidad, bajó a 9,4% de disponibilidad, mientras que los usuarios de CNN descendieron por debajo del 5% del volumen normal, y ZDNet junto a E*Trade estuvieron prácticamente fuera de línea. Schwab.com, empresa dedicada al negocio de corredores de bolsa, también fueron atacados, pero se negaron a dar cifras exactas de sus pérdidas. Uno puede solamente suponer que una empresa que hace $2000 millones por semana en comercios en línea, tendría pérdidas enormes por inactividad.

Otro tipo de daño causado indirectamente por los ataques de DDoS fue la disminución de valor de las acciones en los 10 días posteriores a los ataques, en los cuales eBay sufrió un descenso del 24%, Yahoo! cayó un 1% y Buy.com un 44%.

Estos ataques fueron manejados por Michael Calce, un joven de 15 años de edad que vive en el extremo oeste de la isla de Montreal, en Quebec, cuyo seudónimo era Mafiaboy. Con el tiempo se declaró culpable de 56 cargos de delitos informáticos y sirvió 8 meses de detención juvenil.

Estos tipos de ataques DDoS han continuado desde el verano de 1999. Uno de los incidentes más conocidos fue una serie de ataques dirigidos contra Steve Gibson's en su sitio web GRC.com en mayo de 2001. El atacante era un niño de 13 años de edad, utilizando un pequeño programa a través de un canal de chat IRC (Internet Relay Chat), en que manejaba y propagaba programas que explotaban los sistemas usando clientes de IRC y los convertía en zombis DDoS.

El ataque DDoS que tuvo mayor impacto potencialmente devastador ocurrió el 21 de octubre del 2002, cuando todos los servidores raíz del servicio DNS fueron objeto de un ataque sostenido por miles de zombis. Nueve de los 13 servidores raíz DNS estuvieron fuera de servicio, los

cuatro restantes fueron capaces de mantenerse operativos durante el ataque.

Todos los principales proveedores de internet y muchas redes privadas mantienen sus propios servicios DNS, aunque muchos de estos servidores privados dependen de los servidores raíz para encontrar aquellos destinos que no se encuentran en sus registros. El ataque estaba programado para actuar entre una y dos horas, sin embargo, este continuo por mucho más tiempo, los servidores posiblemente se habían sobrecargado generando así un bloqueo de respuestas DNS de todas las direcciones solicitadas.

Una tendencia preocupante y que se encuentra en crecimiento es el uso de DDoS como una herramienta de extorsión. Un incremento en el número de criminales que están usando las herramientas de DDoS como una forma de amenazar con un ataque, en lugar de realizar realmente el ataque para interrumpir la red de una organización. Aunque varios proveedores de red, seguridad y servicios, afirman que ellos y varios de sus clientes han recibido este tipo de extorsión, pocos son públicos sobre el nombramiento de los objetivos, muchos de estos extorsionadores realizan las amenazas con el objetivo de obtener dinero por el chantaje. Los expertos están de acuerdo en que no se deben satisfacer las demandas de extorsión, ya que hacerlo solo alienta el comportamiento criminal. Si se

recibe una amenaza, se debe solicitar la presencia de las respectivas autoridades, tanto del proveedor como la participación de organismo de control ante la ley local.

2.5 Objetivos de los atacantes

Los ataques cibernéticos son más frecuentes cada día y su aumento es considerable en los últimos años, así como también el número de individuos u organizaciones que deciden realizar este tipo de ataques en contra de organizaciones o enemigos ha aumentado, igualmente ha aumentado el uso de computadoras y redes comprometidas.

La motivación de estos ataques tiene un sin número de orígenes, pero nombraremos tres de ellos los cuales parecen tener un fin más fuerte.

2.5.1 Ganancias Financieras

Las organizaciones utilizan ataques DDoS para obtener ganancias de las caídas financieras de dos maneras: quienes quieran obtener ventajas sobre sus competidores y los que realizan extorsión criminal.

En estos casos alguna organización legítima paga a sueldo los servicios de DDoS para atacar a sus competidores poniéndolos en una desventaja significativa, ya que las pérdidas son desproporcionadamente grandes en comparación con el costo de los servicios DDoS.

Las entidades que ofrecen estos servicios de pago por alquiler DDoS suelen recurrir a extorsión criminal. Para dar a conocer sus intereses lanzan un pequeño ataque de DDoS a su objetivo como muestra. Luego envían un mensaje a su objetivo sugiriendo que tienen el poder de evitar un ataque más grande mediante el pago de cierta cantidad de dinero. Si el objetivo realiza el pago del dinero puede evitar el ataque anunciado, sin embargo, es tildado de “pagador” y es usado como objetivo para futuros intentos de extorsión.

En estos casos es necesario implementar soluciones de mitigación de DDoS para prevenir futuros ataques.

2.5.2 Motivación Política

Aparte de las ganancias financieras mediante el ataque a los competidores o la extorsión criminal, muchas organizaciones tienen motivaciones políticas o de ocio, comúnmente una combinación de ambas.

Estas motivaciones son relativamente nuevas y marcan una evolución en el mundo de los ataques cibernéticos, lo cual nos conduce a acuñar el término “Hacktivismo”, es decir, el uso de ataques cibernéticos promovidos por una agenda política.

Estos atacantes cibernéticos se encuentran agrupados como Anonymous y el ya desaparecido LulzSec.

Entre sus operaciones se encuentran Operación PayBack, Operación AntiSec, Operación Blackout y Operación Defensa.

2.5.3 Amenazas Persistentes Avanzadas (APT) y Ciberguerra

Cualquier persona u organización que cuente con un motivo persistente y los medios avanzados para ejecutar un ataque

cibernético sigiloso sin discriminación es conocido como una amenaza persistente avanzada (APT).

Como muestra de lo que un individuo u organización es capaz de crear con los recursos suficientes y adecuados, tenemos a Duqu, Stuxnet y Flame, los cuales fueron piezas altamente complejas de malware y herramientas de ciberguerra desplegadas fácilmente sin ser detectadas.

Este tipo de amenazas desempeñan un papel muy importante en el futuro de la seguridad, dado su capacidad de robar inteligencia o paralizar las actividades de sus objetivos con ataques DDoS más devastadores que los propios ataques físicos.

2.6 Tipos de Ataques

Los ataques de Denegación de Servicios, cualquiera sea su origen inclusive si son accidentales, manifiestan sus resultados en la indisponibilidad de los servicios, sean estos servidores o equipos personales se vuelven inoperables o la red se vuelve inaccesible.

Los ataques de Denegación de Servicios se lanzan deliberadamente por un atacante, y los sistemas y redes que están en peligro se refieren como las víctimas. Estos ataques pueden ser lanzados desde los sistemas del atacante, que a menudo son lanzados por un proceso automatizado que permite al atacante iniciar el ataque a distancia con sólo pulsar unas teclas. Estos programas se conocen como demonios, y se colocan a menudo en otro sistema que el pirata informático ya ha comprometido.

Hay cuatro tipos básicos o categorías de ataque de Denegación de Servicios:

- Por Consumo de Recursos
- Por Destrucción o alteración de configuración de información
- Por Destrucción física o alteraciones de componentes de la red
- Por Interrupción de las comunicaciones

2.6.1 Por Consumo de Recursos

Las redes y las computadoras en general necesitan de ciertos aspectos importantes para operar correctamente. El tipo de ataque de DoS por Consumo de Recursos, pretende privar a computadoras, servidores y redes de los recursos escasos, limitados o no renovables que puedan poseer, y que son esenciales para que el ordenador o red pueda operar. Recursos de este tipo incluyen el tiempo de CPU, el espacio en disco, la memoria, estructuras de datos, ancho de banda de red, acceso a otras redes y computadoras y los recursos ambientales como el aire fresco y la energía.

Para este tipo de ataque de DoS, existen cuatro subcategorías de ataques por consumo de recursos:

- Conectividad en la Red
- Uso de sus propios recursos en contra de usted
- Consumo de Ancho de Banda
- Consumo de otros recursos

2.6.1.1 Conectividad en la Red

El objetivo de los ataques de Denegación de Servicio es evitar que las redes y los dispositivos de red se mantengan comunicados. Es por este motivo que la mayoría de ataques de DoS son ejecutados comúnmente en contra de la conectividad de la red.

El mecanismo utilizado para este tipo de ataques es que el atacante inicia el proceso de establecimiento de conexión hacia un dispositivo de red víctima, pero lo hace de tal manera que impide que la comunicación final se establezca. Por otro lado, el dispositivo de red víctima ya ha reservado uno de los números limitados de estructuras de datos necesarios para completar la conexión pendiente. Como resultado de esta pseudo comunicación, las conexiones legítimas serán rechazadas mientras el dispositivo de red víctima espera por completar las conexiones falsas o ¨medias abiertas¨.

Debemos considerar que este tipo de ataques no son dependientes de que el atacante pueda consumir todo el

ancho de banda de red o no. En este caso, el intruso consume estructuras de datos del núcleo del sistema operativo (Kernel) que participan en el establecimiento de una conexión de red en general. Adicionalmente, es posible realizar tipos de ataques asimétricos, ya que este tipo de ataque se puede ejecutar normalmente desde una conexión dial-up contra un dispositivo que se encuentre en una red muy rápida.

Un ejemplo de este tipo de ataque es el ataque "SYN flood" o también conocido como inundaciones del bit de sincronización de una conexión de tres fases.

2.6.1.2 Uso de sus propios recursos en contra de usted

Un intruso puede hacer uso de nuestros recursos en contra nuestra de diversas formas. Un ejemplo de este tipo de ataques es el de Denegación de Servicio de puertos UDP.

En este tipo de ataque, el intruso usa paquetes UDP falsificados para conectar el servicio ECHO de una máquina al servicio Chargen (nombre conocido del inglés Character

Generator Protocol) en otra máquina. El resultado es que ambos servicios, ECHO y Chargen, consumen todo el ancho de banda disponible de la red entre ellos y por tanto la conectividad de todos los dispositivos de la red puede verse afectada.

2.6.1.3 Consumo de Ancho de Banda

En este tipo de ataque, un intruso es capaz de consumir todo el ancho de banda de red disponible mediante la generación de un número elevado de paquetes que son dirigidos hacia la red. Estos paquetes dirigidos generalmente son paquetes de tipo ICMP ECHO, pero también pueden ser cualquier tipo de paquetes. Hay que considerar que el atacante no necesariamente estará operativo desde una sola máquina, ya que puede ser capaz de coordinar o cooptar a varias máquinas en diferentes redes para lograr el mismo efecto.

2.6.1.4 Consumo de otros recursos

Además del consumo del recurso ancho de banda de la red, los atacantes son capaces de consumir otros recursos que

nuestros sistemas necesitan para operar. Tal es el caso que, en muchos sistemas, las estructuras de datos tienen un número limitado de entradas disponibles para almacenar la información de los procesos, como por ejemplo identificadores de proceso, entradas de la tabla de procesos, ranuras o slots de proceso, entre otros. Un atacante es capaz de consumir estas estructuras de datos escribiendo un simple programa o script que no hace más que crear copias repetitivas de sí mismo. Muchos sistemas operativos modernos tienen nuevos mecanismos para protegerse contra estos problemas, pero no todos lo hacen. Además, incluso si la tabla de procesos estuviese vacía, el CPU podría ser consumido por un gran número de procesos y por el tiempo gastado asociado a la conmutación entre estos procesos.

Un atacante también puede intentar consumir espacio de disco en otras formas, tales como:

- Generando un número excesivo de mensajes de correo, mediante ataques de Email Bombing y Spamming.

- Generando intencionalmente errores que deben ser registrados o guardados en archivos de log.
- Colocando archivos en áreas ftp anónimas o recursos compartidos de red.

En resumen, mientras los sistemas no tengan configuraciones que limiten la cantidad de datos o conexiones que realmente deberían tener, fácilmente se podrá ejecutar un ataque de denegación de servicio. Un atacante podría ser capaz de hacer que los sistemas se bloqueen o se vuelvan inestables mediante el envío de datos inesperados en la red. Un ejemplo de este tipo de ataque es el ataque de denegación de servicio vía ping.

2.6.2 Por Destrucción o alteración de configuración de información

Este tipo de ataque destruye o altera información de configuración en los sistemas host, servidores o routers. Este tipo de ataque puede ser muy grave debido a que los ordenadores que estén pobremente configurados o no estén correctamente configurados podrían no funcionar u operar de manera adecuada.

Por ejemplo, si un atacante es capaz de cambiar la información de rutas de los routers, toda la red podría ser deshabilitada, o en otro ejemplo si los registros de un servidor Windows son modificados por un atacante, probablemente ciertas funciones del servidor quedarían fuera de servicio.

2.6.3 Por Destrucción física o alteraciones de componentes de la red

Este tipo de ataque resulta en componentes de la red que son físicamente destruidos o alterados. Para protegerse contra este tipo de ataque, es necesario tener una buena seguridad física para proteger los ordenadores y otros componentes de la red, se deben evitar los accesos no autorizados a las computadoras, routers, armarios de red de cableado, segmentos troncales de red, estaciones de energía y refrigeración, y cualquier otro tipo de componente crítico de la red.

Es importante destacar que la seguridad física es un componente primordial en la defensa, no solo contra los ataques de Denegación de Servicio, sino también contra muchos otros tipos de ataques.

2.6.4 Por Interrupción de las comunicaciones

Este ataque impide la comunicación entre dos dispositivos de red mediante la alteración del estado de la información, como por ejemplo el estado de una conexión virtual TCP, tal que la transferencia efectiva de datos es imposible.

2.6.5 Ataques más comunes identificados

A continuación, se detallarán algunos ataques de denegación de servicios, que pueden ser considerados como ejemplos de los métodos generales empleados en un ataque de DoS o DDoS.

2.6.5.1 Destructive Devices

Destructive Devices son programas que realizan, ya sea el hostigamiento o la destrucción de datos. Si estos dispositivos son capaces de destruir o colapsar una red de tal manera que la vuelve ineficiente, dichas herramientas pueden ser consideradas instrumentos de ataque de Denegación de Servicio.

Los virus, email bombs y herramientas DoS son considerados dispositivos destructivos, debido a que algunos de ellos pueden atacar sistemas a nivel de hardware, tal como sucede con los ataques que emplean Stuxnet y Flame.

2.6.5.2 Email y Email Subscription Bombing

Email y Email Subscription Bombings (Bombardeo de Correo electrónico y de subscripción de correo electrónico) fueron unos de los primeros ataques de denegación de servicio documentados.

El ataque de email bomb consiste en el envío de gran número de mensajes de correo electrónico que saturaran el buzón de correo electrónico de la víctima. Este envío masivo de mensajes puede obstruir una conexión en línea, disminuir la velocidad de entrega de correo, e incluso sobrecargar el sistema del servidor de correo electrónico hasta que colapse. Se cree que la mayoría de ataques de correo electrónico son ejecutados por personas

disgustadas, cuyos objetivos son personas a las cuales les tienen un rencor en particular, así como también podrían ser accidentales como los ejecutados por el Christmas Tree worm (Gusano del árbol de Navidad) y el Internet Worm (Gusano de Internet).

Estos ataques también pueden ser automatizados mediante el envío de paquetes a la red. Existen algunos conocidos como Up Yours, Kaboom, Avalanche, Gatemail, y el Unabomber, estos paquetes se pueden colocar en un servidor de red durante un ataque DoS y pueden ser utilizados para atacar a otros sistemas. Como sugerencia los administradores de red deben escanear regularmente sus unidades y eliminar este tipo de archivos. Se pueden utilizar mecanismos de seguridad para protegerse de este tipo de ataques, como por ejemplo el uso de filtros de correos, los cuales mediante ciertas configuraciones pueden rechazar correos enviados utilizando paquetes de email bomb.

Con el email subscription bombing, también conocido como la lista de enlace, el usuario está suscrito por el atacante a

docenas de listas de correo sin el conocimiento del usuario. Si un usuario está suscrito apenas de 50 a 100 listas, podría comenzar a recibir diariamente cientos de miles de mensajes, y solamente podrá darse de baja a cada lista de manera manual. Para prevenir este tipo de ataques, es recomendable siempre tener la confirmación del supuesto suscriptor e incorporar los mecanismos CAPTCHA (Por sus siglas en inglés: Completely Automated Public Turing test to tell Computers and Human Apart) para interferir con los robots que intentan suscribir a víctimas a sus envíos. Otra forma de ataque inadvertido es cuando un usuario configura su cliente de correo electrónico para que se envíen mensajes de auto respuesta por vacaciones y acuses de recibo de todos los mensajes enviados. Los recibos devueltos, a su vez, generan más mensajes de vacaciones de respuesta automática.

Otra variante de este bucle de retroalimentación se produce cuando un empleado se va de vacaciones y reenvía todo el correo electrónico a un ISP externo. Si el empleado decide no revisar el correo durante el viaje, por diversas razones, el buzón de correo del ISP se llena de mensajes re-

enviados. Si el buzón se llena, el ISP enviará un rebote mensaje de vuelta al servidor corporativo, el cual reenvía el mensaje de devolución de nuevo a la ISP, que genera otro mensaje de devolución. Con el tiempo, incluso el servidor de correo corporativo se llenará con los mensajes de un solo individuo, causando un ataque DoS de correo electrónico.

2.6.5.3 Buffer Overflow

Los ataques de Buffer Overflow pueden ser maliciosos y dañinos. Es posible enviar una cadena de entrada a un programa de destino que contiene código real y es lo suficientemente largo para desbordar el espacio de memoria o memoria intermedia de entrada. A Veces este código clandestino se coloca en la pila de proceso (el área en la memoria de un ordenador en el que el sistema operativo mantiene un registro de entrada del programa y código relacionado utilizado para el procesamiento de las entradas), y el código seguidamente se procesa.

Un desbordamiento se puede producir cuando los datos de entrada desbordan su espacio de búfer y desemboca en la pila, donde se sobrescribe los datos anteriores y la dirección de retorno. Si el programa está escrito para que los puntos de dirección de pila en el código malicioso se encuentren en el búfer de retorno, el código se ejecuta con los privilegios iniciales del programa. Buffer Overflow es el resultado de una mala programación, donde el programador no comprueba el tamaño de la entrada en comparación a la memoria intermedia de entrada. Aunque la base de mala programación de los Buffer Overflow se ha erradicado por ahora, los nuevos ataques de desbordamiento de búfer surgen mensualmente.

A partir de enero de 2013, la National Vulnerability Database [5] incluyó 6.273 Buffer Overflows fuera de un total de 64.398 vulnerabilidades - alrededor del 10 por ciento. Este porcentaje ha ido disminuyendo en los últimos años; en el período comprendido entre enero de 2010 hasta diciembre de 2012, 1.281 de los 14.510 registros fueron por desbordamientos de búfer - sólo el 9 por ciento; por el contrario, de los 39.822 registros de vulnerabilidades

introducidas antes de 2010, 5047 (13 por ciento) involucraron Buffer Overflow. [6]

No todos los desbordamientos de búfer permiten al usuario insertar código ejecutable. Ataques de denegación de servicio tales como el ping de la muerte simplemente adjuntan un bloque de datos que es más grande de lo permitido por el protocolo IP (es decir, mayor que 65.536 bytes). Debido a que los paquetes se rompen en fragmentos para la transmisión, se las arreglan para conseguir a través de la red y, probablemente, el router y firewall. Una vez vuelto a montar en el objetivo, sin embargo, los paquetes causan el búfer del núcleo IP se desborde y, si no se maneja adecuadamente, el sistema se bloquea.

Otro ejemplo es un viejo error en Internet Information Services 2 de Microsoft (IIS) que podría ser explotado para permitir detener el servicio web. Para ello, un atacante pediría un documento con una muy larga URL de un sitio web basado en IIS (y cómo se puede identificar un sitio de IIS) Si una página de usar sitio web con las extensiones

.htm o .asp, es una buena suposición de que el sitio se está ejecutando IIS). Tras la recepción de la solicitud, se produjo una violación de acceso y el servidor detendría. Aunque Microsoft publicó un parche para esta vulnerabilidad, los ataques exitosos continuaron tomando lugar durante años.

2.6.5.4 Bandwidth Consumption o ataques de Amplificación

En los ataques de Bandwidth Consumption (o ataques de Consumo de Ancho de Banda) está implícito el envío de un gran número de paquetes dirigidos a la red atacada, el cual puede ser ejecutado de manera local o remota. Esto puede ocurrir debido a que el atacante intentará inundar el mayor ancho de banda disponible de la víctima, sin importar la velocidad de conexión de la red. Este tipo de ataques puede ser perpetrado con el uso de cualquier tipo de paquete, pero el más común es el ICMP (Internet Control Message Protocol) de mensajes echo, los cuales son generados haciendo ping, y que al ser ejecutado por varios sitios a la vez amplifican un ataque DDoS. Algunos ejemplos de ataques muy comunes incluyen ataques Smurf

(amplificación ICMP) y ataques Fraggle (amplificación UDP).

El ataque Smurf utiliza herramientas nativas de los sistemas IP y emplea sitios de terceros sin necesidad de tomar el control de cualquier sistema en cualquier lugar. En los ataques Smurf, el atacante envía cadenas continuas de grandes mensajes ping a una dirección IP broadcast de un tercero, falsificando la dirección IP origen del mensaje ping para que parezca que estos mensajes provienen de un router de la red destino. Si el intruso envía grandes paquetes a la IP broadcast del sitio intermedio, las respuestas consumirán grandes megabits (Mb) de la red. Aunque la víctima tenga un ancho de banda considerable, el atacante puede inundar la red simplemente mediante el envío de un único gran ping por segundo. Este sitio intermedio se llama, por razones obvias, la red de amplificación, y la proporción de los paquetes transmitidos originalmente para el número de sistemas que responden se conoce como la relación de amplificación (amplification ratio).

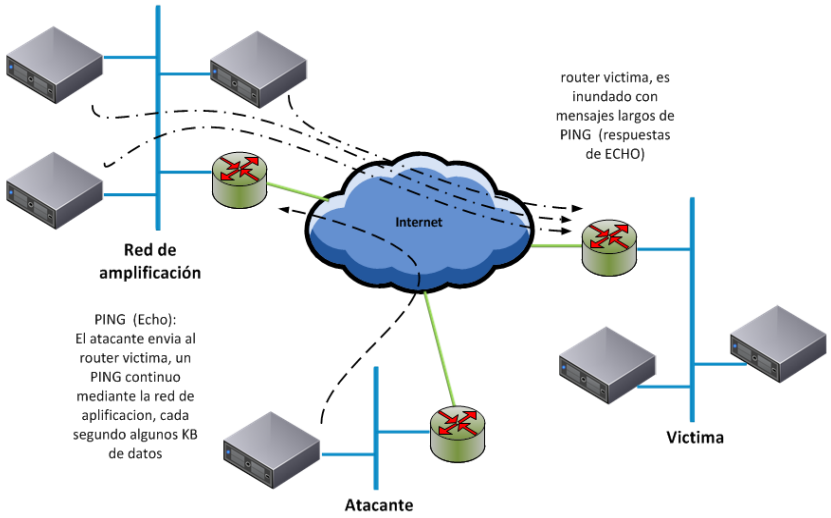


Figura 2.3 Estructura de un ataque Smurf de Denegación de Servicios Distribuidos.
Fuente: Autoría propia

Los ataques Fraggle, una variante del ataque Smurf, basan su funcionamiento en la suplantación de paquetes UDP (User Datagram Protocol) en lugar de mensajes ECHO a la dirección broadcast de la red de amplificación.

Otro ejemplo de un tipo de ataque de amplificación es la amplificación de DNS, en el que un atacante, habiendo comprometido previamente un servidor de nombres DNS recursivo para almacenar en caché un archivo de gran tamaño, envía una consulta directamente o a través de una red de bots a este servidor DNS recursivo, que a su vez

abre una solicitud pidiendo el archivo de caché de gran tamaño. El mensaje de respuesta (significativamente amplificado en tamaño de la solicitud original) se envía a la dirección IP (falsa) de la víctima, causando una condición de denegación de servicio.

Rastrear al intruso que perpetra un ataque al consumo de ancho de banda puede ser difícil, ya que los atacantes pueden falsificar sus direcciones de origen.

2.6.5.5 Ataques de Enrutamiento y del Sistema de Nombres de Dominio

Ataques de enrutamiento y del sistema de nombres de dominio (DNS) son ataques inteligentes que son logrados de manera repetitiva. Por manipulación del DNS, el nombre de dominio de un sitio se resuelve a la dirección IP de cualquier otro sitio que el atacante desea.

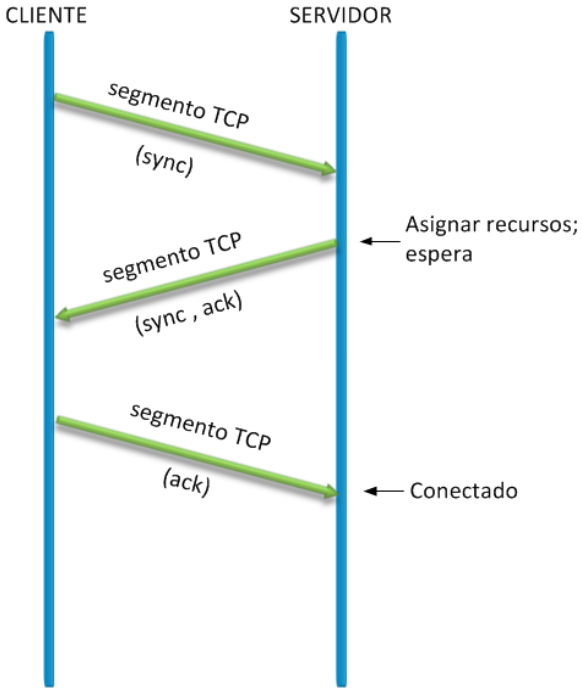


Figura 2.4 Estructura negociación de tres pasos (3-way handshake).

Fuente: Autoría propia

Aunque estos ataques DNS son poco tradicionales, todavía son ampliamente vistos actualmente.

El Phishing es una forma de ataque de Ingeniería Social por el que los usuarios se dirigen a sitios web fraudulentos, pero de aspecto auténtico, de empresas bancarias o de tarjetas de crédito y son tentados a introducir información personal utilizada para el robo de identidad, en donde al observar detenidamente la URL del sitio es una URL sospechosa.

El Pharming es una variante del Phishing que se basa en algún tipo de envenenamiento de DNS para que un usuario vaya a la URL real de un banco o compañía de tarjeta de crédito, y luego será redirigido al sitio falso. También han surgido otras variantes de Phishing, como Spearphishing (dirigir un ataque de Phishing a una persona específica, función de trabajo, o grupo), Vishing (un ataque de Phishing a través de la red de telecomunicaciones, tales como Voz sobre IP - VoIP), y Smishing (Phishing a través de servicio de mensajes cortos SMS, o mensajes de texto).

2.6.5.6 SYN Flooding

Este ataque DoS explota la negociación en tres pasos utilizada por los host TCP para sincronizar la conexión lógica antes del intercambio de datos.

En una conexión TCP normal host a host, los dos anfitriones intercambian tres segmentos TCP antes de intercambiar datos, como se muestra a continuación:

1. El cliente envía un segmento al servidor con su número de secuencia inicial (ISN). La bandera SYN (sincronización) se establece en este segmento.
2. El servidor responde enviando un segmento que contiene su ISN y reconoce el ISN del cliente. Este segmento tendrá establecido tanto la bandera del SYN y del ACK (acknowledgment). En este punto, el servidor asigna recursos para la conexión a ser establecida pronto y espera por el tercer segmento.
3. El cliente envía un segmento reconociendo el ISN del servidor. Esto y todos los segmentos posteriores hasta el final de la sesión tendrán sólo el conjunto de la bandera ACK.

Una inundación SYN, se aprovecha de la negociación en tres pasos y el hecho de que un servidor puede tener sólo un número finito de conexiones TCP abiertas. El ataque se origina cuando un atacante inicia conexiones para las que nunca habrá un tercer segmento. Después de que el servidor envía el segmento en el paso 2, se espera una respuesta.

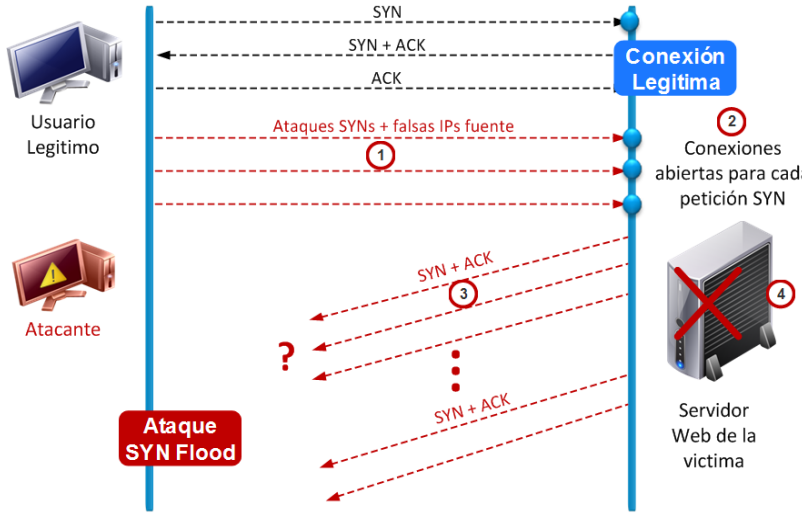


Figura 2.5 Estructura de ataque SYN DoS.
Fuente: Autoría propia

En circunstancias normales, el cliente responderá a los pocos segundos. El servidor podría esperar, por ejemplo, 10 segundos antes de tiempo de espera y la liberación de los recursos. Pero supongamos que el atacante envía cientos de mensajes de conexión por segundo de forma sostenida. El servidor se ve obligado a mantener las conexiones abiertas para cada una de las solicitudes de conexión originales, tratando de enviar paquetes SYN-ACK varias veces antes de recurrir a una solicitud de tiempo de espera. Debido a que los recursos del servidor son limitados, el servidor es incapaz de mantener las

conexiones abiertas lo que causa una condición de denegación de servicio.

2.6.5.7 Inanición de recursos

Este ataque es una categoría general para muchos otros tipos de ataques de denegación de servicio que son el resultado de algún recurso escaso ya sea el ancho de banda, potencia de procesamiento, espacio siendo disco consumido y agotado. Puede ser realizado de manera remota o local.

Otra variante de este tipo de ataque se llama Slowloris, que se enfoca en los servidores web y utiliza una cantidad relativamente baja de ancho de banda por el atacante. Utilizando el esquema Slowloris, un atacante envía un gran número de solicitudes de conexión a un servidor Web de destino y las mantiene abiertas el mayor tiempo posible. En algunas circunstancias, el servidor Web afectado agotará su fuente de recursos de conexión en las peticiones incumplidas, negando así las peticiones legítimas. Existen

muchos tipos de servidores Web susceptibles a Slowloris, incluyendo varias versiones de Apache.

Una variante de Slowloris se llama R-U-Dead-Yet (RUDY). RUDY absorbe recursos de conexiones desde un servidor Web mediante el envío de un gran número de mensajes POST y aleatoriamente grandes valores de Content-Length en el encabezado del mensaje HTTP.

2.6.5.8 Ataques de Router

Han sido desarrollados para una amplia variedad de routers. Debido a que los routers son la columna vertebral de la Internet y la puerta de enlace a través del cual las organizaciones se conectan a Internet, matando a un router se niega el servicio de red de cientos de máquinas. Objetivos populares para este tipo de ataques son los routers de Ascend, Cisco, Juniper, Lucent, y 3Com. Por desgracia, muchos administradores de red hacen que los ataques sean fácilmente ejecutados mediante el empleo de Telnet o HTTP para el acceso remoto, y no aseguran

adecuadamente la red contra el acceso remoto por cualquier persona a través de Internet.

2.6.6 Herramientas de ataques más comunes

Las herramientas de DDoS se han vuelto cada vez más sencillas de usar y disponibles en distintas plataformas, lo que hace fácil su ejecución y las vuelve peligrosas para sus objetivos.

Algunas de estas herramientas nacieron como herramientas de prueba de red, pero posteriormente fueron modificadas para usarlas con fines maliciosos. Otras herramientas han sido desarrolladas específicamente para realizar ataques DDoS y liberadas para su uso libre, evolucionando constantemente, volviéndose cada vez más livianas, efectivas y peligrosas.

2.6.6.1 Trinoo (Trin00)

Fue la primera herramienta conocida para realizar ataques de Denegación de Servicios. Es una herramienta que envía paquetes UDP (por sus siglas en inglés User Datagram Protocol) para crear un ataque DDoS. Trinoo administrador o Trinoo Master, es un sistema usado para la administración

y así enviar ataques de DDoS en contra de uno o más sistemas objetivos. Este sistema administrador tiene la característica de enviar instrucciones a los diferentes agentes (llamados demonios) que han sido previamente instalados en sistemas víctimas para atacar a una dirección IP definida. Este ataque ocurre por un periodo de tiempo definido, en el cual aprovechan la vulnerabilidad de sobrecarga del buffer de sus víctimas.

Los programas de detección de intrusos o los sistemas de análisis de rutina pueden buscar un listado de eventos que podrían indicar la presencia de Trinoo en la red:

- Un sistema escuchando en el puerto UDP 27444 podría ser un demonio Trinoo
    - La comunicación de un demonio Trinoo contendrá la cadena l44
    - El mecanismo de inundaciones SYN selecciona el puerto de destino utilizando una función de generador de números aleatorios.
    - Un demonio Trinoo enviará la cadena PONG si este recibe un comando ping.

- Un sistema escuchando en el puerto TCP 27665 podría ser un Trinoo Master
- Un sistema escuchando en el puerto UDP 27444 podría ser un Trinoo Master
    - Los paquetes UDP contendrán la cadena l44adsl

Existe una herramienta llamada WinTrinoo que se ejecuta desde el sistema operativo Windows y realiza las mismas funciones.

2.6.6.2 Tribe Flood Network (TFN)

Esta herramienta hizo su aparición después de Trinoo. Puede ejecutarse fácilmente en sistemas UNIX comprometidos, usando errores de buffer overrun en los servicios de llamadas a procedimientos remotos (RCP). TFN es muy diferente a Trinoo ya que todas las comunicaciones entre el cliente (atacante), controladores y agentes utilizan paquetes ICMP ECHO y de respuestas echo. Esto lo hace difícil de detectar ya que muchas

herramientas de monitoreo no están configuradas para capturar y visualizar tráfico ICMP.

En el campo identificador del paquete ICMP se envían comandos generados por los demonios; luego comienzan los ataques de inundación SYN, UDP e ICMP mediante valores de 345, 890 y 901 respectivamente. El campo de número de secuencia en el mensaje de respuesta de echo siempre se establece en 0x0000, que hacen que parezca que la respuesta al paquete de echo inicial es enviado por el comando ping.

El programa cliente TFN normalmente se llama tribe.c y el demonio es td.c.

2.6.6.3 Stacheldraht (German for barbed wire)

Esta herramienta apareció como una combinación de las características de Trinoo y TFN, y otras características como cifrado de comunicaciones de atacantes master y actualizaciones de agentes automatizados.

Stacheldraht usa una arquitectura similar de cliente servidor Trinoo. El manejador (en inglés handler) escucha en el puerto TCP 16660 esperando los comandos del intruso, y los agentes escuchan el puerto TCP 65000 de comandos del controlador. Las respuestas del agente al manejador emplean mensajes de respuesta ICMP ECHO. Se emplean los mismos ataques de TFN como ICMP Flood, SYN Flood, UDP Flood y adicionalmente ataques Smurf. Trinoo, basado en TCP, también está sujeto a ataques TCP comunes como secuestro de sesión (session hijacking). Stacheldraht aborda estas deficiencias mediante el empleo de un cliente de cifrado telnet por igual (Telnet por igual o Telnet alike es un término de Stacheldraht). El cliente usa criptografía de clave secreta a diferencia de Trinoo y TFN que intercambian comandos en texto plano.

La red Stacheldraht comprende un número de programas:

- El atacante utiliza un cliente de cifrado llamado telnetc/client.c para controlar a uno o más manejadores.
- El manejador se llama mserv.c, y cada manejador puede controlar hasta 1000 agentes.

- El software de agente se llama leaf/td.c y coordina el ataque contra una o más víctimas al comando del manejador.

2.6.6.4 TFN2 K (Tribe Flood Network 2 K)

TFN2 K es una variante compleja de TFN, cuyos objetivos son sistemas basados en UNIX y Servidores Windows NT.

Tal como lo hace TFN, puede consumir todo el ancho de banda mediante inundación de datos a la máquina de la víctima. Pero a diferencia de TFN, también puede incluir ataques diseñados para dañar o introducir inestabilidades en el sistema mediante el envío de paquetes malformados o inválidos, tales como los encontrados en ataques Teardrop y Land.

TFN2 K utiliza una arquitectura cliente servidor, donde el único cliente emite comandos simultáneos a un conjunto de agentes de TFN2 K, los cuales ya han sido instalados en la

o las máquinas comprometidas. Estos agentes luego realizan el ataque DoS contra la víctima.

2.6.6.5 LOIC, HOIC y HULK

Luego de la aparición de Trinoo, TFN, TFN2 K y Stacheldraht, muchas otras herramientas aparecieron, tal es el caso de Shaft, Ataques HTTP Apache, Trinity, SubSeven, Mydoom, HPing, Slowloris, RUDY entre otros.

Otras variantes de este tipo de ataques son el Low Orbit Ion Cannon (LOIC), diseñado para realizar pruebas de estrés de la red, pero también usado como herramienta para realizar ataques de DoS y DDoS. Básicamente realiza inundaciones de paquetes TCP y UDP con el fin de saber si los routers pueden manejar la carga y como ellos responderán. Es ampliamente usado por el colectivo Hacktivista Anonymous.

El High Orbit Ion Cannon (HOIC) es una variante de LOIC. Posee una interfaz gráfica muy fácil que permite realizar ataques mediante scripts.

El HTTP Unbearable Load King (HULK) es una variante de otras herramientas que realizan ataques a un servidor con un abrumador número de paquetes. A diferencia de otras herramientas que hacen predecible su ataque, HULK genera un conjunto de solicitudes únicas, no predecibles, destinadas a frustrar las defensas basadas en el reconocimiento de filtrado de patrones de paquetes.

2.6.6.6 Software Explotable

Las herramientas vistas anteriormente tienen un mismo fin, el cual es aprovechar una vulnerabilidad de la víctima potencial y utilizar mecanismos para lanzar ataques a la víctima.

Sin embargo, nuevos ataques de DDoS utiliza código que es comúnmente conocido con vulnerabilidades conocidas. Tal es el caso de los ya conocidos parches de Microsoft, los cuales son lanzados para corregir vulnerabilidades que ha dado a conocer y que son inmediatamente explotables por los atacantes.

Esto es comúnmente ignorado por los Administradores de Sistemas, quienes de haber implementado oportunamente los parches anunciados por los fabricantes hubiesen evitado ser blanco de ataques.

Algunos ataques de este tipo son Code Red (julio de 2001) y NIMDA (septiembre 2001).

CAPÍTULO 3

SITUACIÓN ACTUAL

3.1 Equipos que conforman la red de datos

La red empresarial está conformada por equipos de seguridad, equipos de comunicaciones (red LAN), Servidores de procesamiento y terminales de usuario.

El servicio de internet es provisto por el ISP Level3, cuyo enlace de internet es de 4 Mb simétrico.

Entre los equipos de seguridad, o dispositivo de protección, encontramos un Cortafuegos y un Sistema de Prevención de Intrusos, los cuales se

detallan a continuación de acuerdo a la función que cumplen dentro de la red empresarial en conjunto con todos los equipos involucrados:

3.1.1 Cortafuegos

El Cortafuegos cumple la función de proteger y limitar las redes LAN de la organización, de esta manera se limita el acceso entre equipos críticos de la empresa y los usuarios finales.

Adicionalmente controla limitando el acceso desde las terminales de usuario y servidores hacia redes externas de la empresa, asegurando que solo el tráfico autorizado mediante reglas implementadas en el cortafuego, permite que ingresen o salgan hacia y desde la red.

Tabla 1 Detalle de las características del servidor firewall.

Característica	Detalle
Software	Servicio IPTables
Plataforma	Linux
CPU	Intel® Celeron® G1820 2.7GHz, 2M Cache, 2 Core
RAM	4 GB
Puertos de red	2 puertos Gigabit Ethernet
Sistema Operativo	CentOS 5 x64
Espacio en disco	140 GB
Protocolos soportados	TCP, UDP, IPv4, IPv6, AX.25, X.25, IPX, DDP, Netrom
Características	Soporte de JumboFrames Soporte de lectura con baja latencia Manejo de 8 colas por puerto de red para protección de Buffer Over Flow

3.1.2 Sistema de Prevención de Intrusos

El Sistema de Prevención de Intrusos cumple la función de detener el tráfico malicioso que ingresa y sale de la red empresarial. Esta función la realiza gracias al aprovisionamiento del fabricante al otorgar una base muy nutrida con las últimas firmas de IPS recopilada por los demás equipos implementados en otras empresas, y así poder considerar un tráfico como malicioso.

Tabla 2 Detalle de las características del servidor de prevención de intrusos.

Característica	Detalle
Software	IPS Snort 2.9v
Plataforma	Linux
CPU	Intel® Celeron® G1820 2.7GHz, 2M Cache, 2 Core
RAM	4 GB
Puertos de red	2 puertos Gigabit Ethernet
Sistema Operativo	CentOS 5 x64
Espacio en disco	140 GB
Protocolos soportados	TCP, UDP, IPv4, IPv6, AX.25, X.25, IPX, DDP, Netrom
Características	Soporte de JumboFrames

	Soporte de lectura con baja latencia Manejo de 8 colas por puerto de red para Protección de Buffer Over Flow

3.1.3 Equipo de Comunicación

El equipo de comunicación es un router encargado de separar la red de usuarios de la red de servidores.

Tabla 3 Detalle de las características del router.

Característica	**Detalle**
Hardware	Router
Marca	Cisco
Modelo	Small Busines RV082
Puertos WAN	2
Puertos LAN	8
Velocidad de conexión	10/100/1000 Mbps
Características	VPN, Filtrado de contenido, Voz por IP

3.1.4 Red LAN de Usuarios

La red de usuarios está compuesta por los distintos departamentos de la empresa, cuyas estaciones de trabajo son del tipo portable ya que es la herramienta de trabajo principal para el personal vendedor y de soporte, por lo que debe ser trasladada a todas partes. Solo el personal administrativo, a pesar de poseer las computadoras portátiles, no tienen permitido la salida de los equipos fuera de oficina.

Tabla 4 Detalle de las características de los computadores de los usuarios.

Característica	**Detalle**
Hardware	Computador Portable
Marca	Dell
Modelo	Inspiron
Sistema operativo	Windows 7 y 8
Memoria RAM	4GB
Procesador	Core i3
Almacenamiento	300GB

3.1.5 Red LAN de Servidores

La red de Servidores está compuesta por servicios de Correo Electrónico, Servidor Web, Base de Datos, Controlador de Dominio y Servidor de Archivos. Estos servicios se encuentran ejecutando en una infraestructura de virtualización de la marca VMware, con su producto vSphere 6.0.

El servidor de Correo Electrónico tiene implementado Zimbra sobre el sistema operativo CentOS 5.

El servidor web tiene implementado Apache 2.0 sobre el sistema operativo CentOS 5.

El servidor de base de datos tiene implementado MySql 5.0.

El controlador de dominio cumple la función de autenticación de usuarios en las estaciones Windows. Se trata de un servidor Windows 2008 Server Standard de 64 bits.

El servidor de archivos tiene implementado Samba versión 4, sobre el sistema operativo CentOS 5.

3.2 Estructura de la red de datos

La infraestructura de seguridad está basada en una arquitectura básica de red, que comprende un Cortafuegos en el perímetro de la red y un Sistema de Prevención de Intrusos.

La red está sub dividida en dos redes LAN, una red LAN de usuarios finales en donde se encuentran todos los departamentos de la empresa tales como el departamento de Sistemas, Contabilidad, Ventas, entre otras, y otra red LAN de servidores tales como Servidor de Correo Electrónico, Navegación, Controladores de Dominio, Servidores Web, etc.

El acceso entre redes LAN está regulado por el Firewall de perímetro, que a su vez regula el acceso de redes externas a las redes internas.

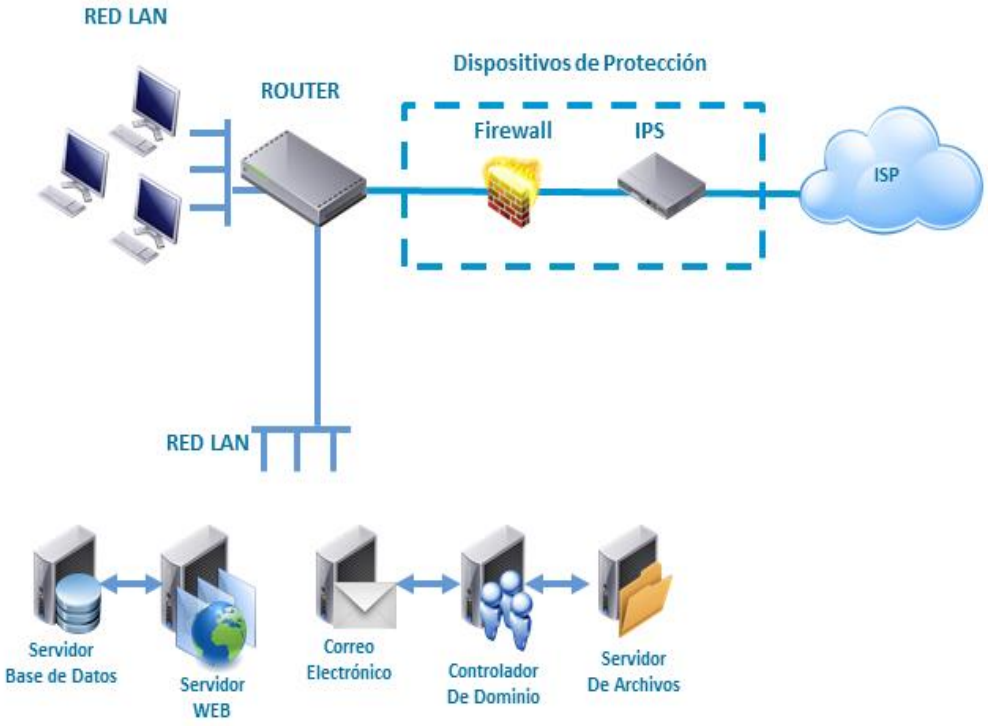


Figura 3.6 Esquema de red actual de la Empresa de Servicios.
Fuente: Autoría propia

3.3 Políticas actuales del Cortafuegos

Las Políticas del Cortafuegos permiten definir qué tipo de tráfico dirigido a la red empresarial está permitido o denegado, en conjunto con las políticas de excepciones debidamente planteadas.

Estas políticas deben estar diseñadas de acuerdo a las capacidades de la empresa, pero también deben considerar las amenazas y vulnerabilidades presentes en redes externas.

Las Políticas de seguridad en general, deben ser planteadas en base a todos los elementos de la red interna que se desean proteger, en el caso de la Empresa de Servicios, se detallaran las Políticas de Cortafuegos consideradas por los administradores de sistemas, que, si bien no se encuentran plasmadas en un documento oficial, han sido consideradas en las configuraciones de Cortafuego existentes en base a la experiencia diaria.

El paradigma de seguridad planteado por los administradores de sistemas en la Empresa de Servicios, se basa en prohibir cualquier servicio excepto aquellos expresamente permitidos.

Entre los servicios que se encuentran permitidos dentro de las políticas del cortafuego se encontraron los siguientes:

Tabla 5 Políticas actuales del Cortafuegos de la Empresa de Servicios.

Nombre de la Política	Origen	Destino	Excepciones	Comentarios
Acceso Total	Any	Any	Ninguna	Acceso a la red sin restricciones
Antivirus Trend Micro Control Manager	Red Corporativa	Any	Permite todo el tráfico TCP y UDP saliente a los puertos 80 y 10319	Acceso a actualizaciones de firmas en las estaciones de usuario
Correo Electrónico y Servidores Web	Any	Red Corporativa	Permite todo el tráfico TCP entrante a los puertos SMTP, 80 y 443	Recepción de correo electrónico y servidores web
Correo Electrónico	Red Corporativa	Any	Permite todo el tráfico TCP saliente al puerto SMTP	Envío de correo electrónico
Soporte Técnico	Red Corporativa	Any	Permite todo el tráfico TCP saliente a los puertos 80 y 443	Soporte técnico remoto a los clientes
Denegar Todo	Any	Any	Denegar	Denegar todo el tráfico

Podríamos deducir que la Estrategia de Seguridad aplicada en la Empresa de Servicios es prudente, en donde se controla y se conoce todo el tráfico que sale y llega a la red empresarial.

Sin embargo, en los próximos capítulos se realizarán algunas recomendaciones en la implementación de Políticas de Cortafuegos enfocadas a la prevención de ataques de Denegación de Servicio Distribuido.

3.4 Políticas actuales del Sistema de Prevención de Intrusos

Un sistema de Prevención de Intrusos comparte la misma funcionalidad de un Sistema de Detección de Intrusos, el cual es mediante activación de módulos de seguridad. La única diferencia es que los IPS cumplen una función proactiva ya que establecen políticas de seguridad para proteger los equipos de la red ante un ataque.

Existen diversos métodos en los que un IPS puede actuar:

- Detección basada en firmas, similar a un antivirus.
- Detección basada en políticas, políticas de seguridad establecidas.
- Detección basada en anomalías, comportamiento en la red.
- Detección Honey Pot, configurado para atraer a los hackers, conocer su accionar y en base a esto implementar políticas de seguridad.

En el caso de la Empresa de Servicios el IPS tiene establecida su funcionalidad mediante Detección basada en Firmas.

Estas firmas tienen la capacidad de reconocer ciertos patrones en la cadena de bytes transmitido, cuando coincide dentro de algún patrón se lanza una alerta y se bloquea el tráfico.

Sin embargo, este tipo de detección es muy similar al de un antivirus, en donde el administrador debe tener especial cuidado para que constantemente estén actualizadas las bases de firmas.

Existen dos tipos de políticas de respuesta aplicados, una pasiva y una activa.

Una política de respuesta pasiva es limitante, ya que solo se registran los datos de la intrusión, pero no ejerce ninguna acción para detenerlo.

Una política de respuesta activa a diferencia de la activa, si ejerce acciones para detener el ataque.

Entre las políticas de respuesta pasiva y activa encontramos descritas en la tabla 6.

Tabla 6 Políticas actuales del Sistema de Prevención de Intrusos de la Empresa de Servicios.

Políticas de respuesta pasiva	**Políticas de respuesta activa**
Cuando se detecta una intrusión se envía un correo electrónico al administrador de sistemas.	Se analiza el ataque y se bloquea la IP de origen mediante listas negras.
Se registra la IP atacante.	Si el ataque es recurrente se reinicia el equipo.

Estas políticas no se encuentran registradas en un documento formal en la Empresa de Servicios, sin embargo, se encuentran configuradas en el IPS y han surgido a partir de la experiencia diaria de los administradores.

3.5 Captura de muestras del tráfico de la red de datos organizacional

Mediante la implementación de un analizador de paquetes IP (sniffer) en la red, con la debida autorización de los administradores de sistemas, logramos capturar el tráfico que circula en la red en varias horas del día incluyendo las horas de mayor demanda.

Con los datos obtenidos de la captura, se obtuvieron datos estadísticos del tipo de tráfico de la red.

En primera instancia obtuvimos una muestra de dos días del comportamiento del tráfico de la red hacia y desde el internet, en donde se observa que existe un tráfico usual durante el día y otro poco usual en las madrugadas, este detalle se visualiza en la Figura 3.7. Adicionalmente podemos observar como los tiempos en que mayor uso de red existe.

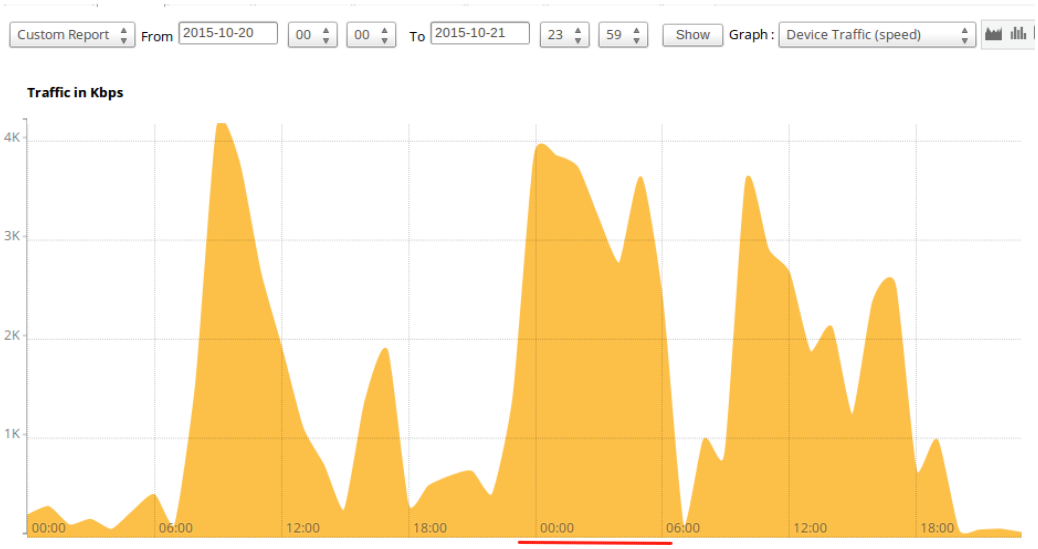


Figura 3.7 Tráfico de datos en el canal de internet durante los días 20 y 21 de octubre de 2015. La línea roja indica presencia de tráfico no común. **Fuente: Autoría propia**

Los aplicativos que de mayor tráfico en la red se mostraban durante los días 20 y 21 de octubre del 2015, se detallan en la Figura 3.8.

	Application	Traffic	Total Traffic
1	https	88.38 MB	6 %
2	ipsec-nat-t	44.24 MB	3 %
3	http	23.07 MB	2 %
4	domain	9.57 MB	1 %
5	smtp	7.98 MB	1 %
6	atmp	1.23 MB	0 %
7	imaps	1.14 MB	0 %
8	Unknown_App	598.41 KB	0 %
9	icmp	562.71 KB	0 %
10	sip	160.59 KB	0 %

Figura 3.8 Detalle de la cantidad de tráfico por aplicativos en la red durante un día laborable
Fuente: Autoría propia

Y lo que nos llama la atención es la ubicación de las IPs que acceden a los servicios de la página web y correo electrónico de la empresa, como se muestra en la Figura 3.9, estos provienen de países fuera del Ecuador, lo cual es algo inusual al contar la empresa con sus usuarios localmente.

	Target Location	Events
1	Ecuador(EC)	297
2	United States(US)	216
3	Not Available(NA)	81
4	Germany(DE)	12
5	France(FR)	11
6	Argentina(AR)	9
7	Canada(CA)	3
8	Brazil(BR)	3
9	Netherlands(NL)	2
10	Colombia(CO)	2

Figura 3.9 Detalle de los países que accedieron a los servicios de la empresa durante el día 21 de octubre.
Fuente: Autoría propia

Podemos luego divisar el comportamiento de los servicios de forma individual, en la cual podremos observar el comportamiento y la demanda que tiene a ciertas horas del día.

El detalle para la página web lo veremos en la Figura 3.10 y Figura 3.11, en donde la Figura 3.10 mostrara todas las consultas realizadas por medio del protocolo HTTP, mientras que la Figura 3.11 mostrara el comportamiento del protocolo HTTPS.

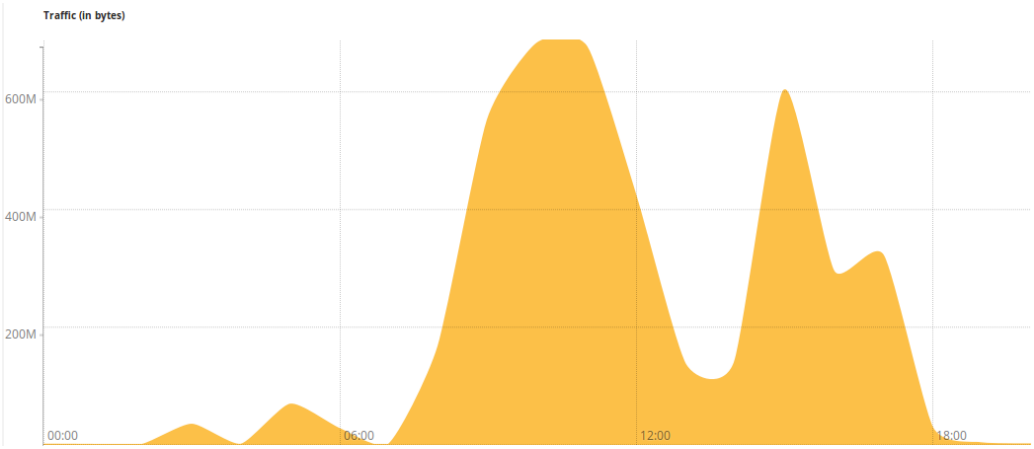


Figura 3.10 Muestra del tráfico de red hacia la página web de la empresa a través del protocolo HTTP durante un día laborable.
Fuente: Autoría propia

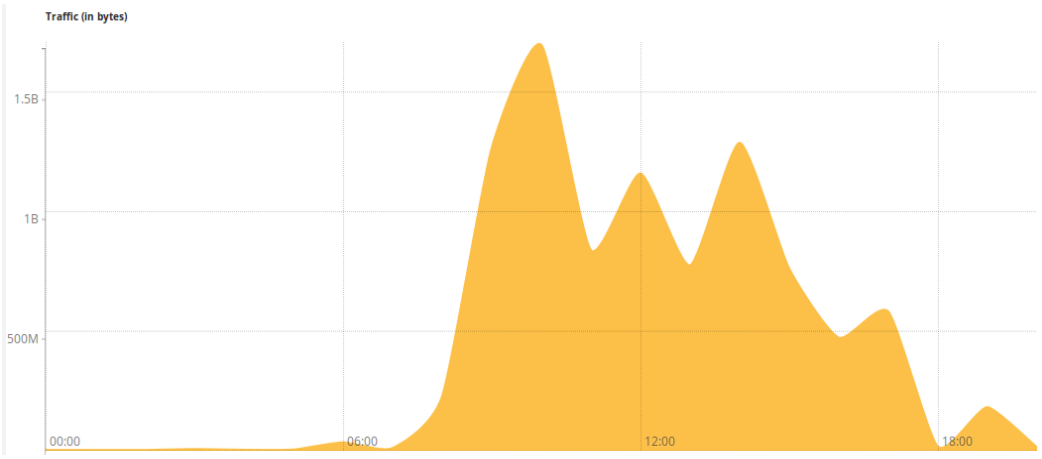


Figura 3.11 Muestra del tráfico de red hacia la página web de la empresa a través del protocolo HTTPS durante un día laborable.
Fuente: Autoría propia

El comportamiento del correo electrónico también podrá ser visible a través de la Figura 3.12, en la cual se detalla el uso del protocolo SMTP. Posteriormente se mostrará la demanda del correo por medio del protocolo IMAP (Figura 3.13) como también en el protocolo IMAPS (Figura 3.14).

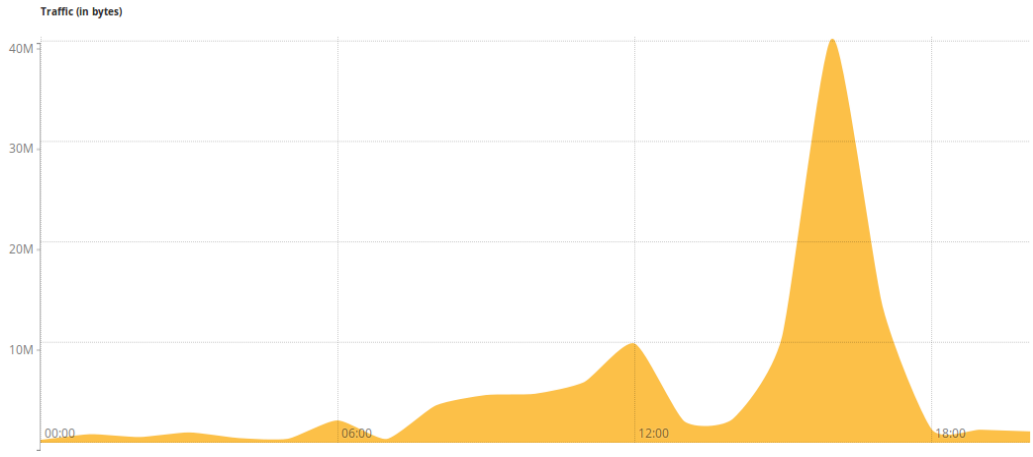


Figura 3.12 Muestra del tráfico de red hacia el correo electrónico de la empresa a través del protocolo SMTP durante un día laborable.
Fuente: Autoría propia

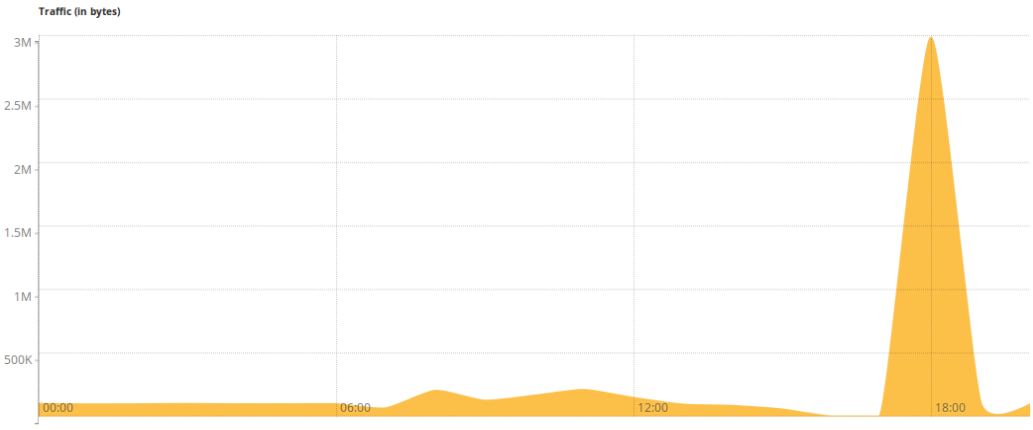


Figura 3.13 Muestra del tráfico de red hacia el correo electrónico de la empresa a través del protocolo IMAP durante un día laborable.
Fuente: Autoría propia

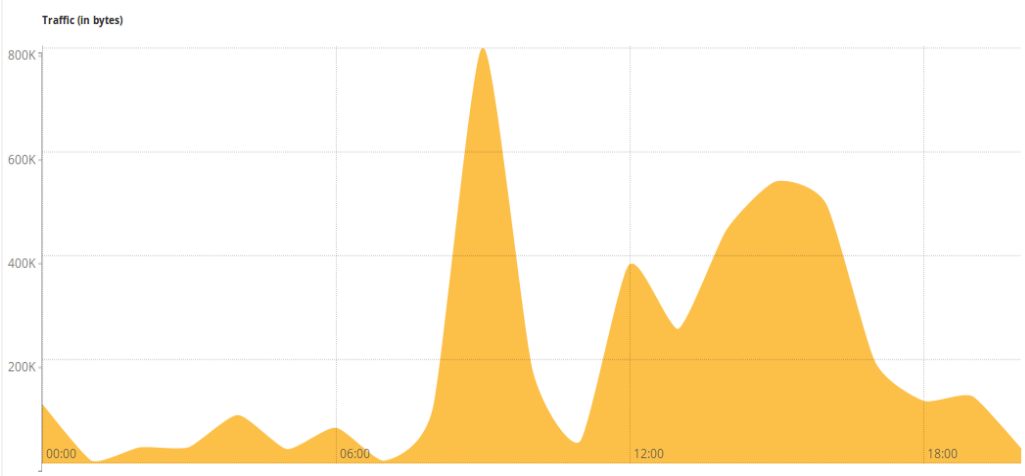


Figura 3.14 Muestra del tráfico de red hacia el correo electrónico de la empresa a través del protocolo IMAPS durante un día laborable.
Fuente: Autoría propia

CAPÍTULO 4

DISEÑO DE LA SOLUCIÓN PROPUESTA

4.1 Arquitectura de la Solución

La arquitectura de la solución propuesta para la Empresa de Servicios, se basa en la integración de un nuevo componente entre la red empresarial y la nube (internet provisto por el ISP), el cual funcionará como Sistema de Defensa contra Ataques de Denegación de Servicio Distribuido. El sistema estará en constante funcionamiento una vez que aprenda del comportamiento de las peticiones y consultas que se realicen a los servicios de correo electrónico y de la página web de la empresa. Este sistema de defensa está compuesto por un Sistema de Detección (Anti DDOS), un Mecanismo de Redirección y un Sistema de Mitigación.

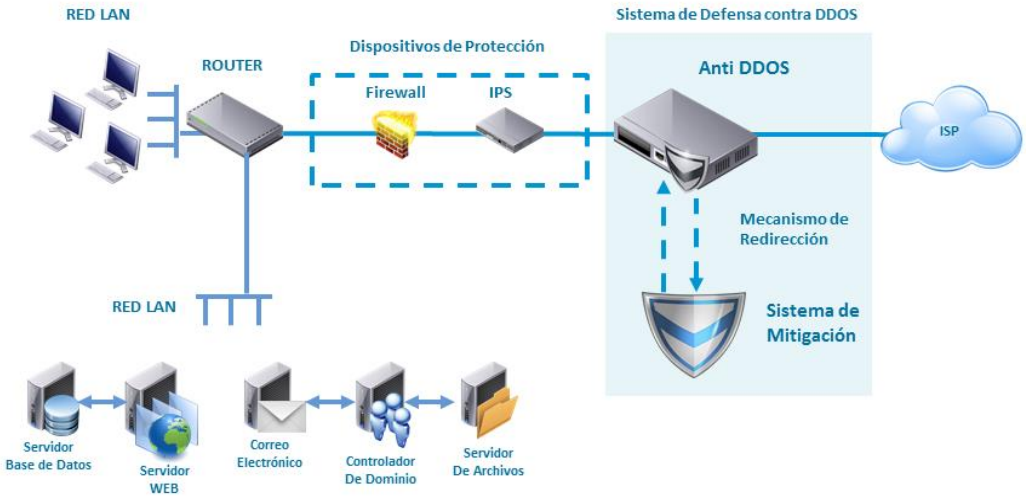


Figura 4.15 Solución propuesta para la Empresa de Servicios.
Fuente: Autoría propia

Este sistema de defensa contra DDoS tiene incorporado internamente tres componentes que están siendo implementados bajo la marca AndriSoft, con su producto anti-DDoS llamado WANGUARD. Este software ha sido de elección de nuestro cliente al tratarse de una solución de código abierto anti-DDoS, escalable y sobretodo que el costo de su implementación se encuentra dentro del presupuesto de la empresa.

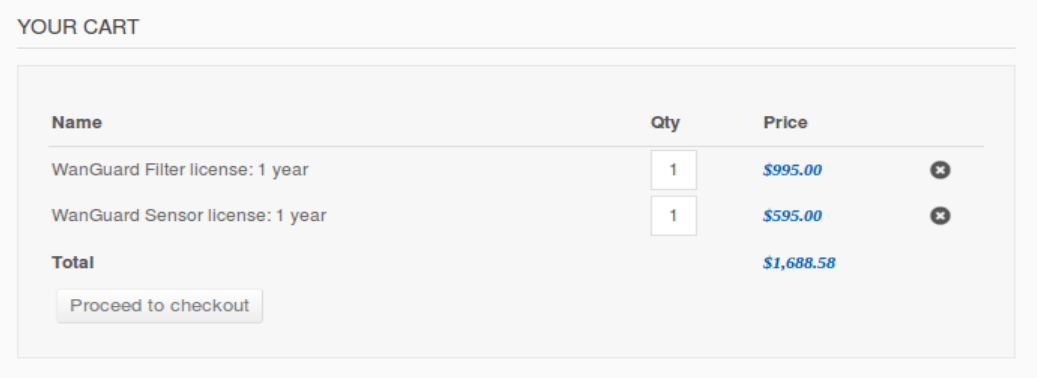


Figura 4.16 Costo de la solución Anti-DDOS Andrisoft por un año.
Fuente: Autoría propia

El funcionamiento de este sistema de defensa proporcionado por Andrisoft nos proporciona funcionalidades de visibilidad del tráfico de la red, así como también la protección a través de un solo paquete integrado de componentes. Las amenazas se pueden presentar como el propio ataque DDoS, el sobredimensionamiento de los recursos o servicios, y por crecimiento temporal de tráfico que afecte la disponibilidad de red.

Los componentes internos del sistema de defensa WANGuard constan de los siguientes:

- El mecanismo de redirección.
- El sistema de detección.
- El sistema de mitigación.
- Consola de Administración.

4.1.1 Mecanismo de redirección

La solución se está implementando bajo un esquema ALL-IN-ONE, el cual nos indica que todos los módulos involucrados en la mitigación de un ataque, se están ejecutando dentro de un solo equipo. Este equipo se encontrará conectado en forma IN-LINE, es decir que se encuentre en medio del tráfico de datos. El modo out-of-line no aplica en este caso ya que su objetivo es copiar todos los paquetes para solo ser monitoreados, y en nuestro caso necesitamos monitoreo y remediación en línea.

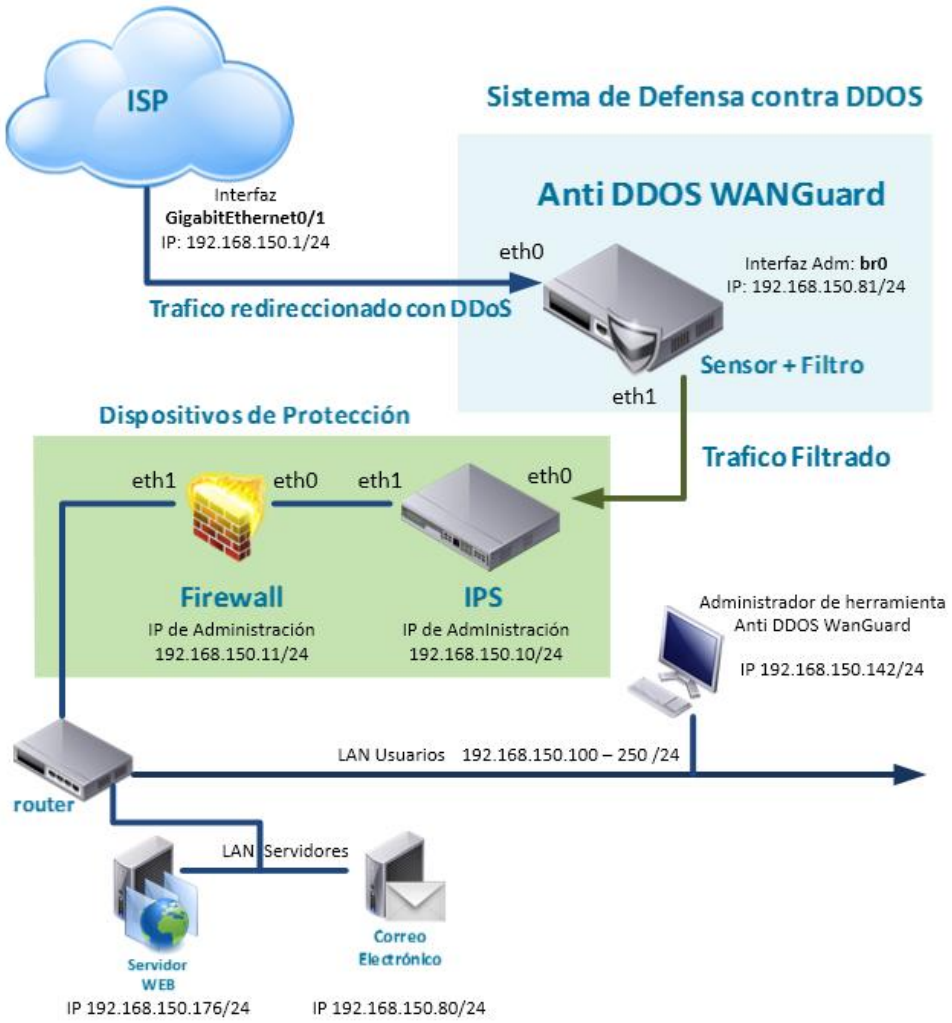


Figura 4.17 Arquitectura del Anti-DDOS Andrisoft.
Fuente: Autoría propia

Todo el tráfico que se recibe del ISP es direccionado hacia el equipo WANGUARD, de esta forma todo el tráfico de datos pasa a través de un análisis en tiempo real y a su vez en caso de detectar alguna anomalía, ésta sea mitigada a través del módulo de filtrado. Una vez

que el tráfico ha pasado el proceso de revisión y limpieza entonces es dirigido hacia el equipo IPS para posteriormente pasar a los servidores destino.

4.1.2 El sistema de detección

Este sistema se encuentra proporcionado por el módulo WANGUARD SENSOR. Este módulo se encargará de realizar el monitoreo del tráfico IP, analizarlos y proporcionar gráficas estadísticas mediante la revisión de los paquetes que se encuentren en circulación, detectando así cualquier anomalía del tipo DoS, DDoS y otros tipos de ataques volumétricos. La información que el sensor recopila permitirá posteriormente generar informes para poder visualizar el preciso momento en que se inicia un ataque, comprender el patrón de afectación al rendimiento de los servicios de la empresa y así ayudarnos a tomar decisiones correctas sobre las acciones a seguir para mitigarlo. En cuanto a la escalabilidad del sensor, inicialmente se formará parte de un equipo en el cual se consideran solo los servicios de página web y de correo electrónico de la empresa, sin embargo, conforme la empresa vaya creciendo, es posible que requieran incrementar el número de sensores, aprovechando que la herramienta es modular, se pueden

incrementar varios sensores, y estos funcionan al unísono siendo administrados desde una sola consola, su escalabilidad depende del crecimiento del tráfico que maneje la empresa a futuro. A medida que se van incrementando el número de sensores, se puede construir una imagen más precisa y detallada en tiempo real del comportamiento del tráfico que fluye a través de la red.

4.1.3 El Sistema de Mitigación

Este sistema se encuentra proporcionado por el módulo WANGUARD FILTER, el cual tiene la función de detectar patrones de ataque y genera reglas de filtrado de contenido, en donde puede separar el tráfico anómalo de forma granular, para de esta manera no afectar la experiencia del usuario, o que pueda resultar en una caída de servicios.

Es importante mencionar que el sistema que realiza la mitigación a través del módulo filtro lleva internamente integrado un Cortafuegos (Firewall), un sistema de Detección de Intrusos (IDS) y un sistema de Protección de Intrusos (IPS), sin embargo, estas funcionalidades no serán activadas ya que para esto la empresa consta de equipos dedicados.

4.1.4 Consola de Administración.

La consola es una herramienta basada en aplicación web, que permite realizar la administración de los módulos que se integren dentro del sistema de defensa, para nuestro caso están considerados el Módulo Sensor y el Módulo Filtro. De esta forma se puede tener un solo punto para efectuar configuraciones en el sistema y además obtener los reportes consolidados de ambos módulos provisionados en el sistema de defensa.

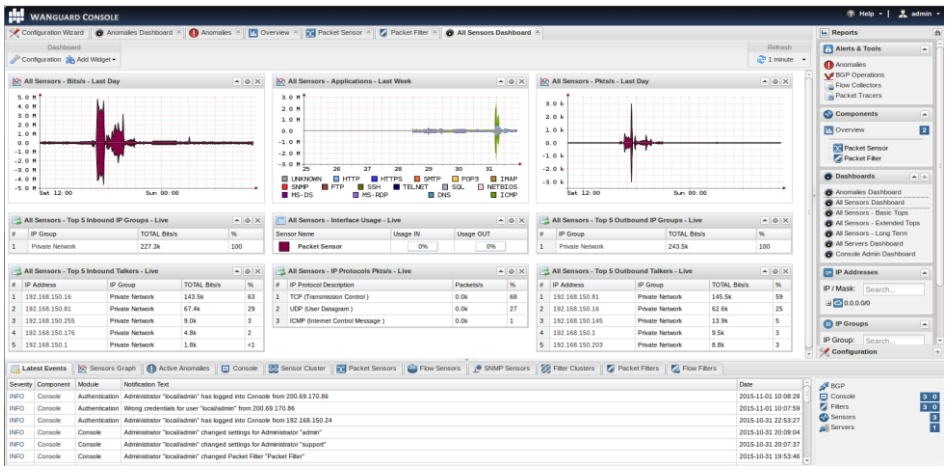


Figura 4.18 Consola de administración del sistema de defensa WanGuard.
Fuente: Autoría propia

Los requerimientos del equipo en donde se tiene instalado del sistema de defensa se encuentran basadas en los requerimientos mínimos para los componentes.

Tabla 7 Requerimientos mínimos para componentes de WanGuard.

Característica	**Instalado**
Tipo de implementación	En línea
CPU	Intel® Celeron® G1820 2.7GHz, 2M Cache, 2 Core
RAM	26 GB
Puertos de red	2 puertos Gigabit Ethernet
Sistema Operativo	CentOS 7
Espacio en disco	140 GB

Entre las características que presenta la solución podremos resaltar las siguientes:

- Soporta las últimas tecnologías de monitoreo tales como detección de paquetes a 10Gbps, Netflow, sFlow. IPPIX, NetStream, cflowd y SNMP.
- La generación de reportes incluyendo detalles por host, grupo de IPs, interfaces, aplicaciones, protocolos, ubicación o geo locación de las consultas.
- Los flujos de datos que son colectados a través de NetFlow, sFlow e IPPIX, pueden ser exportados, filtrados y se pueden realizar búsquedas.
- El analizador de paquetes puede realizar la presentación en detalle de cualquier parte de la red para poder luego descargarlo o verlo in line.
- Se pueden generar reportes en tiempo real desde 5 segundos a los últimos 10 años, pre configurando intervalos por tiempo, por hora, diarios, semanales o mensuales.
- Los componentes o módulos pueden ser distribuidos en mayor número de servidores, esta funcionalidad se comportará como un servicio en clúster.

- En caso de requerir soporte del fabricante, dentro de la licencia ya viene incluido el soporte con tiempo de respuesta de una hora durante todo el año.

4.2 Estimación de Riesgos: Políticas

En este punto se decidió realizar una evaluación rápida de los riesgos de seguridad, con la finalidad de conocer las amenazas que pueden materializarse y definir los bienes que se desean proteger, con ello definiremos las Políticas de Seguridad que deben regir.

La evaluación de riesgos se realizará de manera cualitativa, mediante una matriz de riesgo en la Seguridad Informática distribuida por Markus Erb, protegida con la licenciada Creative Commons Atribución-No Comercial-Compartir Obras Derivadas Igual 3.0 España License, que considera la fórmula **Riesgo = Probabilidad de Amenaza X Probabilidad de Impacto.**

Los factores antes mencionados toman los valores 1 (Insignificante o ninguna), 2 (Baja), 3 (Mediana) y 4(Alta).

El resultado de este producto se resume en la Figura 4.19.

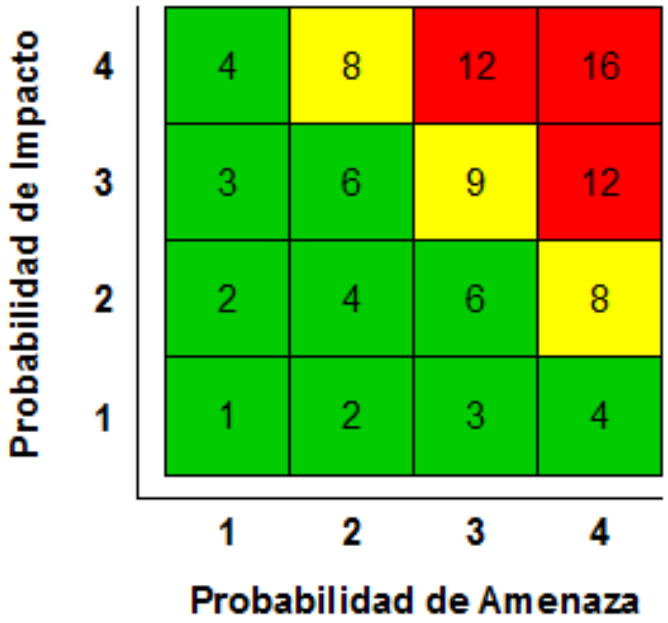


Figura 4.19 Matriz de valores del Análisis de Riesgo Promedio.
Fuente: Autoría propia

El riesgo por lo tanto estaría agrupado en tres rangos, los cuales son:

- Riesgo Bajo = entre 1 y 6 (**Color verde**)
- Riesgo Medio = entre 8 y 9 (**Color amarillo**)
- Riesgo Alto = entre 12 y 16 (**Color rojo**)

Se consideraron dos categorías a evaluar, Datos e Información y Sistemas e infraestructura, cada uno con sus respectivos elementos.

Entre los elementos considerados en la categoría Datos e Información tenemos los siguientes:

- Correo electrónico
- Bases de datos internos
- Página Web externa

Entre los elementos considerados en la categoría Sistemas e infraestructura tenemos:

- Equipos de la red cableada (router, switch, etc.)
- Equipos de la red inalámbrica (router, punto de acceso, etc.)
- Cortafuego
- IPS
- Servidores
- Computadoras

Entre los elementos considerados en la categoría Personal tenemos posibles ataques internos provocados por el personal de la empresa.

Entre las amenazas consideradas tenemos actos de criminalidad, sucesos de origen físico o natural y negligencia de los usuarios.

Como resultado del uso de esta matriz, se obtuvieron siete formularios de diferentes personas de la Empresa de Servicios con diversos cargos, las cuales pueden ser consultadas en el Anexo 1 Formularios Matriz Análisis de Riesgo. Con ello se obtuvieron los siguientes resultados:

Tabla 8 Análisis de Riesgo Promedio de Seguridad de la Empresa de Servicios.

Matriz de Riesgo		**Probabilidad de Amenaza**		
		Actos de Criminalidad (Criminalidad común, motivación política, Hackers)	**Sucesos de origen físico o natural**	**Negligencia de Usuarios**
Probabilidad de Impacto	**Datos e Información**	**5.7**	**4.8**	**6.3**
	Sistemas e Infraestructura	**6.1**	**5.2**	**6.8**
	Personal	**5.2**	**4.4**	**5.7**

La matriz de Análisis de Riesgo Promedio muestra el promedio aritmético de los diferentes riesgos, en relación con los diferentes grupos de amenazas y daños. Su objetivo es determinar en qué grupo de Probabilidad de Amenaza contra Probabilidad de Impacto hay mayor o menor peligro.

De acuerdo a los datos obtenidos, podemos deducir que el riesgo promedio de seguridad es bajo, tendiendo a un riesgo medio debido a amenazas como Actos de Criminalidad como ataques informáticos y robo de información, como por negligencia de los usuarios en el manejo de los activos y la información confidencial.

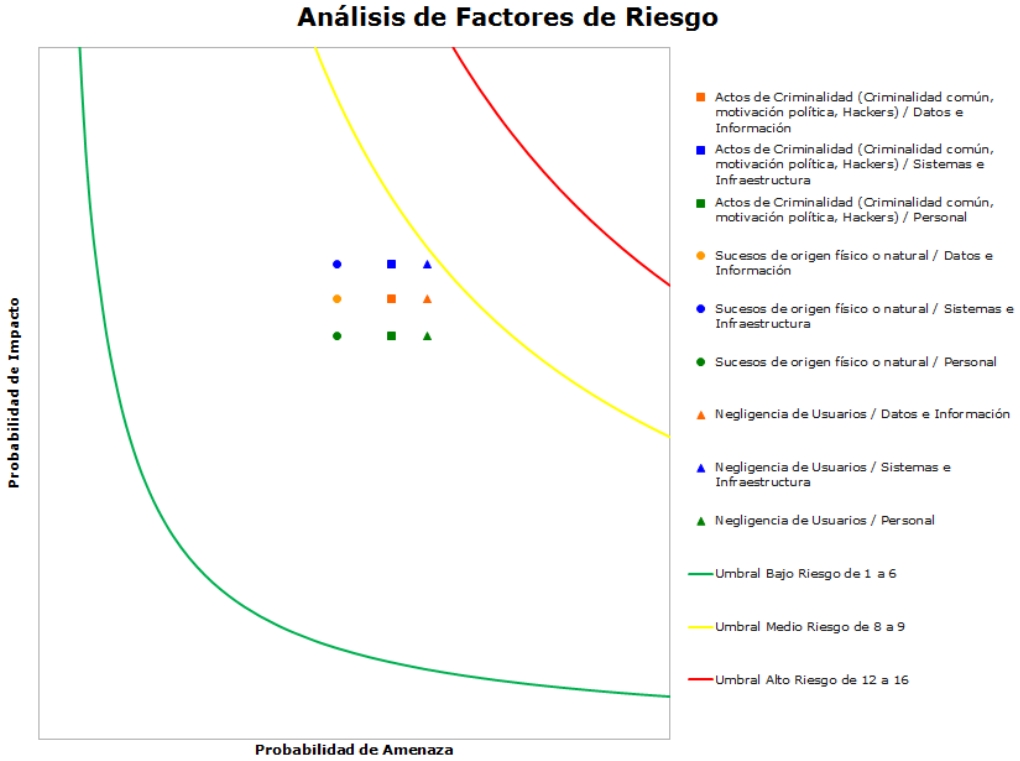


Figura 4.20 Gráfico de Análisis de Factores de Riesgo de Seguridad.
Fuente: Autoría propia

El gráfico de análisis de factores de riesgo tiene el mismo propósito que la matriz, pero de manera gráfica, ilustra la cercanía del riesgo bajo, medio y alto de los diversos factores que intervienen en el análisis.

Como podemos observar existe una cercanía pequeña en el umbral de Riesgo Medio, por lo que se deben tomar acciones para evitar caer en riesgos más altos.

Un recurso que se utiliza para mitigar los riesgos, es la aplicación de Políticas de Seguridad, las cuales apalancan una correcta administración de los recursos mediante su aplicación y actualización continua.

4.2.1 Políticas en el equipos anti-DDoS

1. Mantener documentación actualizada de todos los cambios realizados en la red.
2. Actualizar las configuraciones del sistema anti Denegación de Servicios Distribuido con los nuevos servicios que son expuestos hacia internet.
3. Realizar una auditoría a las configuraciones de seguridad implementadas al menos una vez al año.

4. Realizar pruebas controladas de Denegación de Servicio al menos una vez por año.
5. Probar el Plan de Respuesta a Incidentes al menos una vez por año.
6. Realizar al menos una revisión por año del Plan de Respuesta a Incidentes y mantenerlo actualizado conforme a las necesidades del negocio.
7. Mantener actualizado el software de la solución anti Denegación de Servicios Distribuidos a su última versión estable con los parches de seguridad adecuados.
8. Trabajar en conjunto con el área de Recursos Humanos en un programa de capacitación continua sobre el manejo de incidentes de Denegación de Servicios Distribuido.

4.2.2 Políticas recomendadas en los demás equipos de la red.

Las siguientes políticas que se indican tienen el objetivo de minimizar un ataque potencial limitando la distribución de herramientas no autorizadas y la propagación de los paquetes de ataque ofensivo a un sistema local o que pueda ser usado como un zombi para atacar a otros.

Estas políticas fueron consideradas como apoyo a la solución implementada y enfocadas a mitigar ataques de Denegación de Servicios Distribuidos desde las demás herramientas de seguridad de la Empresa de Servicios.

4.2.2.1 Usuarios Administradores de Sistemas

Dentro de las Políticas de Seguridad sugeridas para los usuarios Administradores de Sistemas tenemos las siguientes:

1. Trabajar en conjunto con el área de Recursos Humanos en un programa de capacitación continua sobre la Seguridad de la Información.
2. Definir el software permitido para estaciones de usuarios y servidores que pueden ser utilizados e instalados en la empresa.
3. Mantener actualizado el software de las estaciones de usuarios y servidores con los últimos parches estables.

4. Cada computador en la red debe tener instalado un software firewall que sea administrado centralizadamente.
5. Realizar análisis de vulnerabilidades en la red al menos una vez por año.
6. Realizar una auditoría a las configuraciones y funcionalidades habilitadas en las estaciones de usuarios al menos una vez al año.
7. Establecer controles que establezcan el monitoreo regular de los registros del sistema de actividades sospechosas para estaciones de usuarios y servidores.
8. Todas las estaciones de usuario y servidores tendrán instalado un software antivirus y software antimalware actualizados.
9. Los Administradores de Sistemas deben aplicar directivas de protección al software antivirus y software antimalware a fin de evitar la instalación de software malicioso.
10. El software antivirus debe realizar análisis de software malicioso permanentemente en estaciones de usuarios y servidores.

11. Trabajar en conjunto con el área de Recursos Humanos en un programa de capacitación continua sobre concienciación en la seguridad de la información.

4.2.2.2 Acciones en la red

Las Políticas aplicadas a las acciones que se deben tomar en la red son:

1. Todas las redes que tengan acceso a Internet debe pasar por un filtro de navegación.
2. Todas las redes deben bloquear los paquetes entrantes dirigidos a la dirección de difusión o broadcast.
3. Enrutamiento (Router). Dentro de los equipos de enrutamiento existen características que pueden prevenir los ataques, como lo son:

    - Desactivar la fragmentación IP de los equipos de enrutamiento.

- Limitar el número de conexiones principalmente por usuario, direcciones IP de origen y nuevas conexiones por segundo.
- Limitar los tiempos para establecer una sesión y las sesiones ya establecidas.
- Restringir la utilización de ancho de banda por tipo de servicio mediante definición de calidad de servicio o QoS.
- Realizar una auditoría a las configuraciones y funcionalidades habilitadas en los equipos de enrutamiento al menos una vez al año.
- Establecer políticas Anti Spoofing en los routers mediante configuración uRPF.
- Restringir los accesos a las IPs de los usuarios/clientes.
- Habilitar la opción de registros (logs) para controlar las conexiones que existen con los equipos de enrutamiento.
- Deshabilitar el enrutamiento de direcciones privadas a través de internet. Consultar Anexo 2 Direcciones IPv4 reservadas para redes privadas.

- No redirigir (enrutar) hacia internet las direcciones IP reservadas que no están asignados a las redes o hosts públicos. Consultar Anexo 3 Direcciones IPv4 que no se encuentran asignadas.

4. Cortafuegos (Firewalls). Se consideran las siguientes Políticas a ser aplicadas en los Cortafuegos:

    - Bloquear todos los paquetes que contengan cualquier dirección IP privada o reservada en el Origen de la dirección o el campo Dirección de destino.
    - Bloquear todos los puertos de aplicación no utilizados en el firewall, principalmente puertos como IRC (6665-6669 / TCP) y los asociados con el software de DDoS.
    - Filtrar la entrada de paquetes con direcciones no enrutables y salida de paquetes con direcciones que no pertenezcan a la organización.

- Establecer políticas de protección contra ataques de inundación SYN (SYN flood) en los cortafuegos.
- Mantener actualizado el software del Cortafuegos a su última versión estable con los parches de seguridad adecuados.
- Bloquear la IP de listas de distribución o broadcasts.
- Denegar todos los accesos a servicios no autorizados por la política de seguridad.
- Utilizar cortafuegos que puedan examinar paquetes dentro del contexto de todo el intercambio de paquetes.
- Utilizar cortafuegos de aplicaciones web.
- Realizar una auditoría a las configuraciones y funcionalidades habilitadas en los cortafuegos al menos una vez al año
- Establecer las políticas de seguridad descritas anteriormente tanto para IPv4 e IPv6 para comunicaciones de entrada y salida.

5. Detector de Intrusos (IPS). Independientemente del tipo de detección que aplique el IPS de la empresa, se detallan algunas consideraciones que debe tener:

    - Implementar un sistema de detección y prevención de intrusiones para proteger la red.
    - Implementar controles que permitan monitorear la actividad de red para detectar aberraciones en el flujo de tráfico.
    - Mantener las bases de firmas del IDS/IPS (intrusion-detection/prevention system) constantemente actualizadas y en su última versión disponible.
    - Mantener actualizado el software de los Sistemas de Detección de Intrusos a su última versión estable con los parches de seguridad adecuados.
    - Realizar una auditoría a las configuraciones y funcionalidades habilitadas en los Sistemas de Detección de Intrusos al menos una vez al año.

Posiblemente este tipo de ataques seguirán ocurriendo a lo largo del tiempo. Es por esto que es necesario adoptar medidas preventivas para intentar evitarlos, así como también contar con los recursos necesarios a la hora de responder en caso de que el ataque fuera exitoso.

6. El DNS, es un sistema de nombres distribuido que permite el acceso a Internet mediante el uso de denominaciones reconocibles y fáciles de recordar en lugar de direcciones IP numéricas, en las cuales la infraestructura de red re direcciona los mensajes de un ordenador a otro. Desde que DNS es distribuido, muchas organizaciones utilizan y mantienen sus propios servidores DNS para que sus sistemas sean visibles en Internet. Sin embargo, estos servidores son a menudo blanco de ataques DDoS, y si el atacante consigue alterar las operaciones del DNS, todos los servicios de las víctimas pueden desaparecer de Internet, causando el deseado efecto de Denegación de Servicio. Es

imprescindible disponer de mecanismos de protección bidireccionales permitiendo realizar un tracking de las peticiones y respuestas, tanto a aplicaciones Web, como a DNS.

7. Medidas que deben ser consideradas con los proveedores de internet (ISP):

    - Filtrado de IP, en ISPs a paquetes provenientes de IPs autorizadas
    - Limitación de número de paquetes/s TCP SYN
    - Búsqueda reversa de IP para evitar el spoofing, utiliza DNS.
    - Monitorización del tráfico de red, análisis del tráfico para detección de ataques.
    - Arquitectura de seguridad basada en Políticas de seguridad relativas a cortafuegos, routers de filtrado, IDSs, planes de contingencia y recuperación de desastres

8. Recuperación de Desastres. Desarrollar con el ISP un plan de recuperación de ataque DoS que cubra:

    - Procedimientos de apagado de servicios afectados, y en caso de ser servicios web proporcionar una página que muestre un mensaje que se encuentran trabajando.
    - Filtrado de ciertos paquetes como ICMP en un momento dado
    - Utilización de logs

4.3 Protección: Configuración de equipos en la red

El equipo con la herramienta WanGuard deberá estar configurado bajo el esquema “en línea”, es decir se encuentra en medio del tráfico entre el internet y la red LAN de la empresa a modo de puente.

Previo a la puesta en producción del equipo anti DDOS en la red, se realizó una revisión de todas las configuraciones que serán implementadas por cada componente, de acuerdo a las necesidades de la empresa y al análisis del comportamiento normal de la red.

4.3.1 Consola

Dentro de la consola iniciamos definiendo los parámetros principales:

1. En la opción Retención de Datos, definir la Política de no borrar registros o logs de comandos, eventos, respuestas, tráfico de anomalías, IPs, y cualquier información capturada en la red a través de los sensores.
2. Configurar un servidor SMTP desde el cual la herramienta pueda enviar emails de alertas antes eventualidades detectadas.
3. Definición de directorios de almacenamientos bajo la ruta /opt/andrisoft/.
4. Habilitar monitoreo de todos los protocolos permitidos por la herramienta, tales como, TCP, TCP+SYNC, UDP, ICMP, BAD, FLOWS, FLOW+SYNC, FRAGMENT, TCP-NULL, TCP+RST, TCP+ACK, TCP+SYNACK, HTTP, MAIL, DNS, SIP, SSL, y Otros.
5. Definir la red que se analizara, en este caso 192.168.150.0/24.
6. Definir los valores que limitan un comportamiento anómalo.

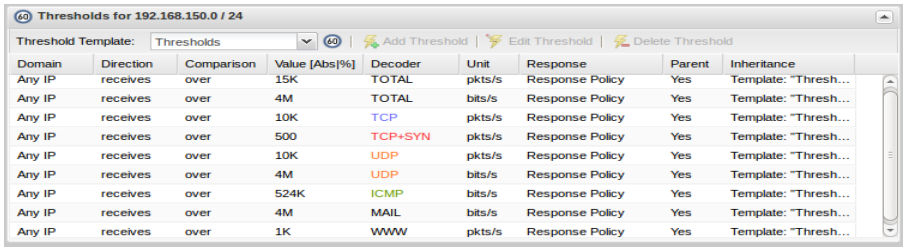


Figura 4.21 Definición de umbrales de detección de ataques de DDOS para los servicios de red en la herramienta anti DDOS.
Fuente: Autoría propia

7. Configurar políticas de respuestas ante eventualidades.

   En respuesta ante evento DDoS se activará el filtro y tomará una muestra de tráfico anómalo. Posteriormente el tráfico será limpiado a partir de la muestra obtenida. La muestra es obtenida de los paquetes que superan los 10K.

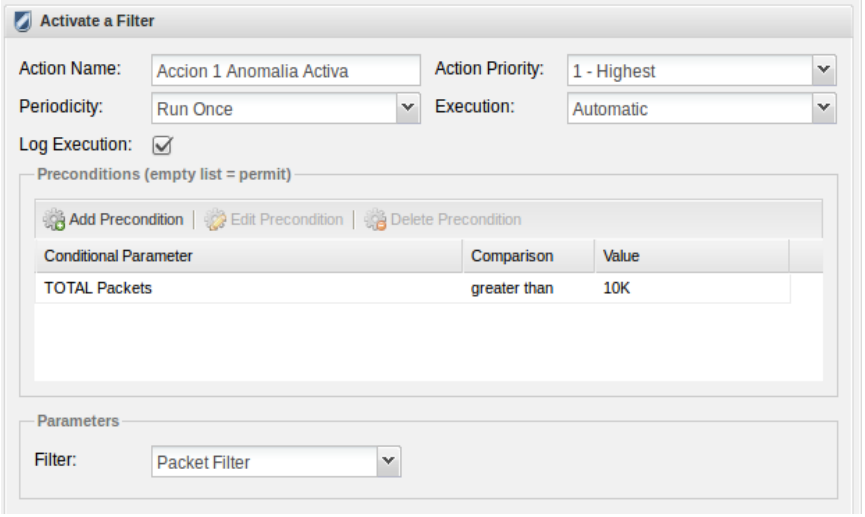


Figura 4.22 Parámetros de activación del Filtro de tráfico de red en la herramienta anti DDOS.
Fuente: Autoría propia

Se enviará una notificación vía email al administrador de la existencia de un evento DDoS desde su inicio.

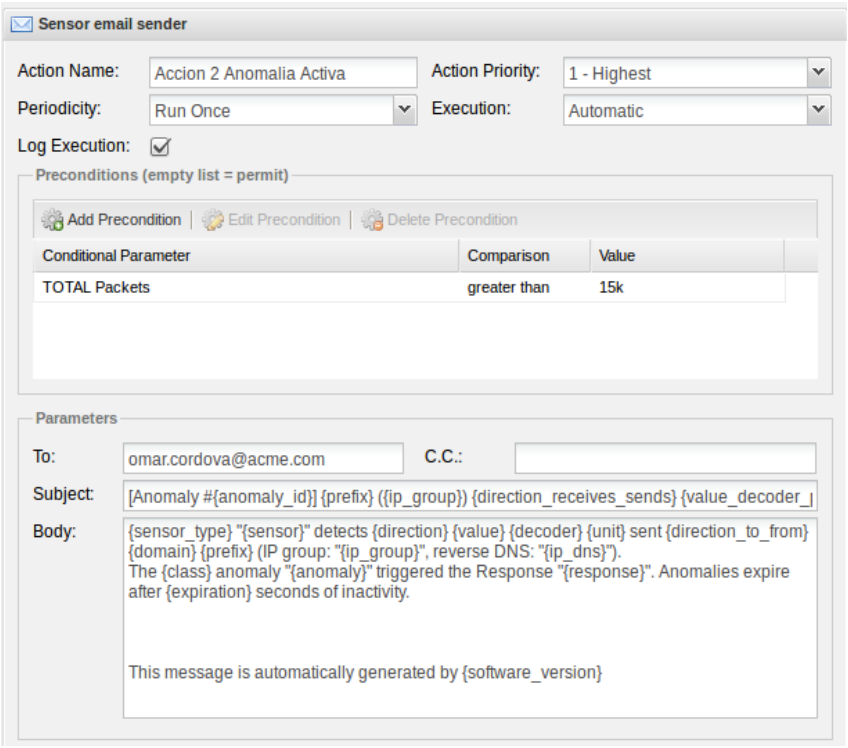


Figura 4.23 Parámetros de configuración en las alertas de anomalías detectadas en el tráfico de red en la herramienta anti DDOS.
Fuente: Autoría propia

Notificar vía email al administrador al finalizar cualquier eventualidad con un informe sobre el ataque mitigado.

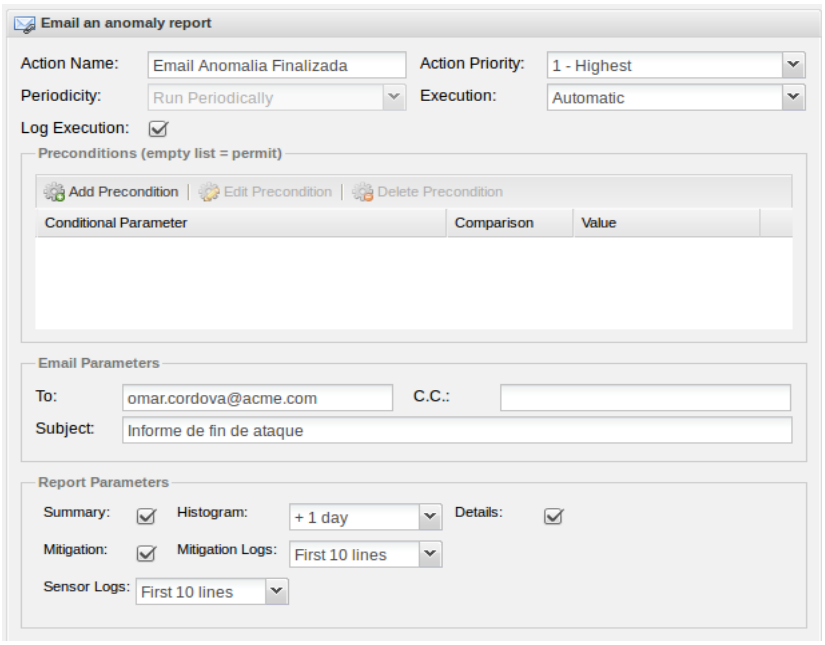


Figura 4.24 Parámetros de configuración de reporte al finalizar las anomalías detectadas en el tráfico de red en la herramienta anti DDOS.
Fuente: Autoría propia

4.3.2 Sensor

1. Se debe habilitar el sensor de paquetes definiendo la interfaz eth0 para capturar el tráfico entrante a la red empresarial.
2. Definir la velocidad de la interfaz de red de tráfico de entrante y saliente.
3. Definir la red a monitorear a través de una zona IP.
4. Definir el tipo de captura a la de mayor detalle (extended).

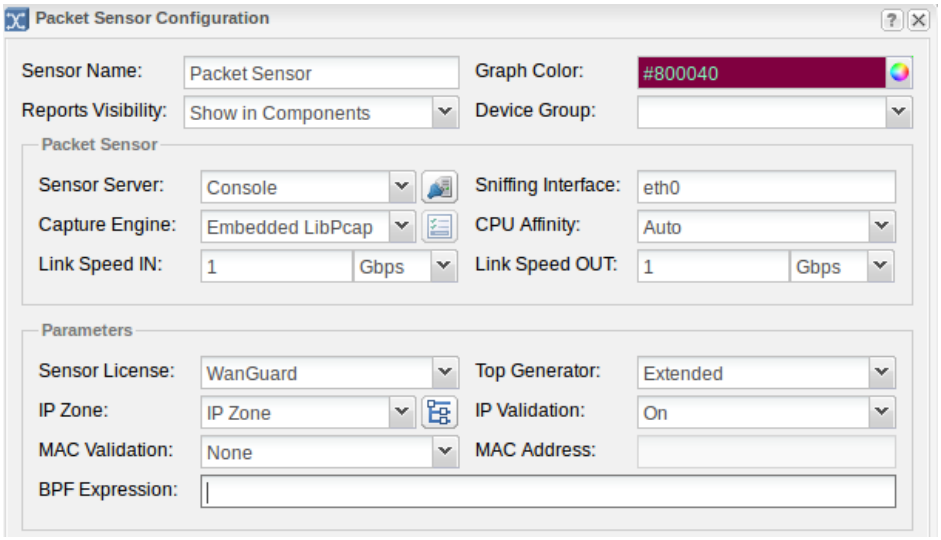


Figura 4.25 Parámetros de configuración del sensor de tráfico de red en la herramienta anti DDOS.
Fuente: Autoría propia

4.3.3 Filtro (Filter)

1. Definir el tipo de topología a usar, en este caso es filtrado en línea (Inline Filtering).
2. Definir la Interfaz de ingreso de tráfico (br0).
3. Definir la interfaz de salida de tráfico (eth1).
4. Definir los parámetros del firewall con el que cuenta la empresa.

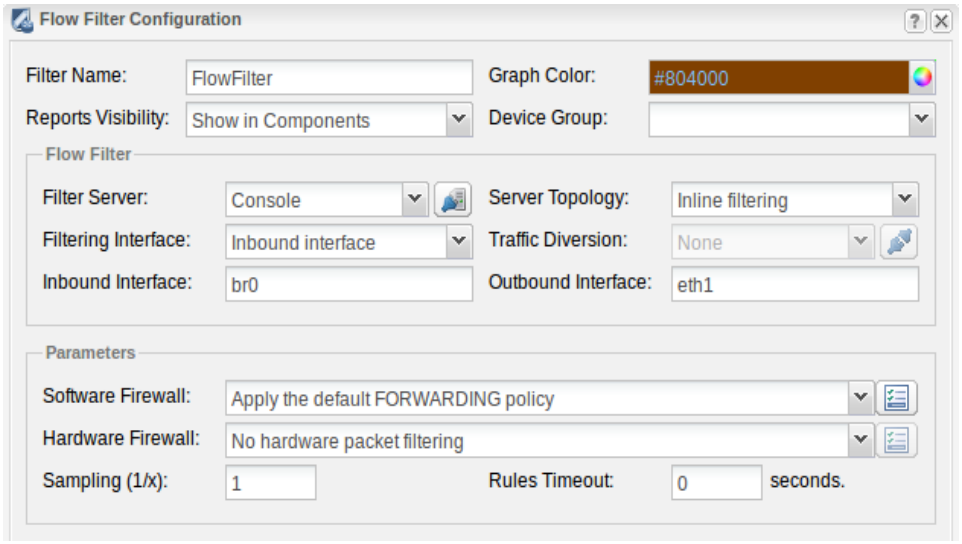


Figura 4.26 Parámetros de configuración del Filtro de tráfico de red en la herramienta anti DDOS.
Fuente: Autoría propia

4.4 Detección: Análisis de las comunicaciones

En esta fase se establecieron qué mecanismos se van a usar para detectar el ataque DDOS, las herramientas que intervendrán, los servicios que debemos considerar y qué parámetros deben cumplir para saber si se trata de un DDOS, como obtener información de fuentes externas para estar al día de los nuevos ataques y los comportamientos que tienen, como se analizaron estos hallazgos, que tipo de respuesta se ejecutará, cuál será el equipo de personas que monitorean o si una persona del equipo actual realizará esta función, analizar la posibilidad de implementar un CERT a futuro o ser parte de uno dependiendo de las posibilidades de la empresa.

4.4.1 Detectar si existe un ataque presente.

Para determinar si se está bajo un ataque se han de recoger que los datos de utilización de recursos como la CPU, memoria, red (latencias y ancho de banda utilizado), disco, etc., de los equipos implicados y compararlos con los valores "normales" que suele tener el servicio, incluyendo su crecimiento. Con esta información se puede llegar a asegurar que un ataque se está produciendo, pero en muchos casos no se aporta suficiente información para determinar el origen (distinguiendo de los usuarios lícitos) ni el tipo de ataque que se está produciendo.

Esto se puede realizar mediante el estudio de los datos obtenidos mediante la monitorización de la plataforma, la cual puede ser tomada con herramienta como Netflow (herramienta para obtener información sobre cantidades de tráfico, así como número de conexiones IP origen/destino) obtención de valores SNMP o las capturas de trazas TCPdump del tráfico existente. Esto incluye el monitoreo del tráfico encriptado y tunelizado, ya que la visibilidad de este tipo de conexiones es importante para divisar posibles ataques que utilicen esos medios para alcanzar a la víctima.

Dentro de las soluciones de detección y mitigación que ofrecen los fabricantes utilizan una combinación de los métodos de monitorización mencionados en dispositivos que trabajan en tiempo real como en los que importan datos colectados, algunos modelos incluyen los medios necesarios para acceder a los túneles cifrados con SSL y de ese modo inspeccionar el tráfico que pasa a través de ellos.

Detectar los orígenes del ataque puede ser muy complicado ya que, se puede tratar de los ataques reflexivos o la utilización de botnets complica la localización de las IPs desde las que se lanzan las peticiones de ataque, al estar estas enmascaradas con el tráfico lícito de otros clientes.

Para el análisis se pueden considerar los mismos parámetros que los fabricantes usan en sus equipos.

- Medición de la tasa actual (rate), es decir, número de peticiones por cliente, tráfico generado, etc. para descubrir los ataques basados en "volumen" (ataques por flooding)

- Clasificación de clientes, mediante puntuaciones que se realizan atendiendo al país de procedencia, rangos de IPs públicas, etc. Estas puntuaciones se modifican dinámicamente re-alimentándose de los datos obtenidos por los propios algoritmos.
- Análisis del comportamiento de cada cliente. Ya que las botnets no son peticiones realizadas por clientes reales, sino que son producidas por software, en ocasiones se repiten ciertos patrones que dan un indicio de que las peticiones de una cierta IP no son "reales". Si se tiene esta sospecha se podría directamente marcar a un cliente como atacante, o modificar los puntos de su clasificación (punto anterior). Por otra parte, también se puede utilizar el conocimiento adquirido sobre los comportamientos "normales" de los clientes, por ejemplo, si habitualmente los clientes que realizan una petición a un servicio web X, también abren conexiones sobre otro servicio web Y, y existen multitud de conexiones desde un cliente al servicio X pero ninguna desde él al servicio Y, puede hacer sospechar que no es un comportamiento "normal" y que es parte de un ataque DDoS.

Es posible desarrollar scripts propios que ayuden a general a monitorear estos puntos y determinar los rangos y comportamientos del tráfico en circulación para determinar las IPs que están realizando ataques por flooding.

Finalmente, una vez que se tienen acotados los posibles orígenes del ataque, se realiza un estudio más detallado (revisando las capturas de paquetes o flujos de tráfico) para determinar el tipo de ataque que se está sufriendo. Estos procedimientos son parecidos a las que realizan otros elementos como IPS o firewalls de aplicación, incluso hay fabricantes que recogen la información de estos para poder deducir el tipo de ataque DoS que se está efectuando. Para ello utilizan una serie de firmas que verifican el vector de ataque.

4.5 Respuesta: Acciones en Respuesta a un incidente

Una respuesta eficaz e inmediata puede realizarse de primera instancia con los equipos de protección que disponga la empresa, para este caso será la solución que recomendaremos, sin embargo, cuando el ataque de DDoS es de alta capacidad, se debe incluir el trabajo de terceros, tales como proveedores de Internet y los especialistas de mitigación de DDoS,

ya que tienen infraestructuras a gran escala y el uso de una variedad de tecnologías para la identificación, contención y remediación. Es posible que los ataques DDoS puedan ser identificados y mitigados antes de llegar a las instalaciones de la organización. Pero esto puede representar costos que la empresa pueda o no estar consciente de la inversión que debe realizar y dependerá de los ejecutivos para su decisión, sin embargo, los siguientes puntos describen las acciones a seguir de forma general ante una eventualidad de ataque DDoS.

4.5.1 Paso 1. Preparación.

Lo importante es establecer contactos, definir los procedimientos, y recopilar información para ahorrar tiempo durante un ataque.

Contactos y procedimientos:

- Establecer una lista de contactos de personas dentro y fuera de la empresa que sean especialistas en diferentes líneas de defensa. Además, incluir abogados relacionados a delitos informáticos.

- Establecer varios mecanismos de comunicación, transferencia de datos o medios de llamadas de voz confiables entre el personal involucrado para la defensa.
- Establecer, y frecuentemente actualizar, el plan de Continuidad y recuperación para eventos DDoS. Definiendo una clara línea de responsabilidades y escalación.
- Asegurarse de que la capacidad de toda la infraestructura no se encuentra limitada o restringida a un número de recursos.
- Definir y dedicar hardware/software para mitigaciones de DDoS, esto es computadores, servidores, equipos de monitoreo y herramientas de análisis.
- Disponer de una conexión a Internet redundante.
- Establecer contactos con especialistas para sus IDS, equipos cortafuegos, sistemas y redes.
- Colaborar con las líneas de negocio de la empresa para entender las implicaciones y criticidad de la misma en escenarios probables de ataque DDoS (por ejemplo, pérdida de dinero).

Infraestructura de red:

- Redirigir el tráfico de los servicios hacia los equipos de protección y filtrado de contenido que ingrese o salga de la red durante el ataque.
- Crear una lista blanca de las direcciones IP y protocolos que se deben priorizar en el tráfico durante un ataque (ACLs).
- Configurar una comunicación alternativa como una VPN, en los servicios críticos.
- Establecer doble tipo de autenticación, combinando una forma débil, luego una segunda forma fuerte y confiable.
- Establecer límites para paquetes ICMP, SYNC, en los servidores expuestos al internet.
- Defina el parámetro time-to-live (TTL) en la configuración de los sistemas DNS que podrían ser atacados. disminuir los valores, si es necesario, para facilitar la redirección de DNS si las direcciones IP críticas están siendo atacados. 600 es un buen valor TTL.
- Documentar los datos de su infraestructura de TI, direcciones IP y los servicios en ejecución, la configuración de enrutamiento, preparar un diagrama de topología de la red y un inventario de activos.

- Controlar y hacer cumplir la configuración de seguridad de los componentes de red, sistemas operativos y aplicaciones que pueden ser blanco de ataques DDoS.
- Si su negocio depende de internet, debe considerar la compra de productos y servicios especializados en mitigación de DDoS.
- En función de la criticidad de sus servicios, considere configuración de una copia de seguridad que puede restablecer en caso de problema.

Apoyo de especialistas internos o externos:

- Se debe consultar al ISP para conocer de los servicios de mitigación de DDoS que ofrece de forma gratuita dentro de un contrato o de pago.
- Definir claramente los tiempos de respuestas (SLAs) en cada contrato y su inmediata vigencia de los servicios incluidos.
- Obtener los datos del rendimiento de su infraestructura actual, para que pueda identificar anormalidades que ayuden a detener el ataque con mayor precisión y rapidez.

- Establecer contacto de proveedores especialistas en mitigación de DDoS. Generalmente con las marcas de nombre reconocido en el mercado.

4.5.2 Paso 2. Identificación.

Detectar el incidente, determinar su alcance, e involucrar a las partes apropiadas.

Detección y Alertas:

- Comprender el flujo lógico del ataque DDoS e identificar los componentes de la infraestructura afectada por el mismo. El uso de firmas puede ayudar a detectar el ataque.
- Comparar parámetros y comportamiento observado entre el tráfico normal de la red y el tráfico mientras está recibiendo el ataque.
- Contactar a los especialistas en cuanto se detecta alguna anomalía o algún indicador en los equipos de monitoreo se alerte.

Analizar del ataque:

- Revise la carga que tienen los servidores, routers, firewalls, aplicaciones y otro tipo de infraestructura afectada.
- Entender si usted es el objetivo del ataque o una víctima colateral
- Póngase en contacto con el equipo interno de seguridad informática para aprender sobre la visibilidad en el ataque.
- Obtener un listado de las IPs que están efectuando el ataque revisando en los registros de logs.
- Definir las características del ataque mediante el uso de herramientas de monitoreo análisis de la red.
- Identificar qué aspectos del tráfico DDoS diferencian de tráfico normal. Entre ellas las direcciones IP Fuente, Destino, los puertos de destino, URL, banderas de protocolos
- Las herramientas de análisis de red que se puede utilizar para revisar el tráfico: TCPdump, Tshark, Snort, Argus, Ntop, Aguri, MRTG.

Identifique la motivación:

- Realice una lista de las posibles causas que hayan iniciado el ataque DDoS.
- Investigue los posibles motivos.
- Averigüe si la compañía recibió una demanda de extorsión como un precursor del ataque.
- Buscar si alguien tendría ningún interés en que amenaza su empresa, tales como competidores, grupos ideológicamente motivados (hacktivistas), o tal vez ex empleados.

Mitigación:

- Póngase en contacto con su ISP para pedir ayuda. Sea específico sobre el tráfico desea controlar: bloques de red involucrados, direcciones IP fuente, protocolos.
- Solicitar una evaluación durante el ataque.
- Proponer medidas de remediación.
- Notificar a los ejecutivos de la empresa y a los respectivos servicios de ley.

Rastreo / Seguimiento:

- Identificar, de ser posible, los puntos de ingreso a través de herramientas como NetFlow.
- Si es posible, crear una firma NIDS y centrarse en diferenciar entre el tráfico benigno y maligno.

4.5.3 Paso 3. Contención

Mitigar los efectos del ataque en el medio de destino.

Modificaciones en la red de datos:

- Mover la ejecución de los servicios al sitio alterno usando re direccionamiento de DNS o cualquier otro mecanismo.
- Distribuya el tráfico atacante entre los centros de datos disponibles.
- Direccionar el tráfico depurado de los servicios y productos.

Control de la entrega de contenido:

- Use los servicios de almacenamiento temporal (caching) y uso de proxy.
- Proporcione un canal de comunicación alternativo para los clientes importantes a través de una canal VPN.

Control de tráfico:

- Terminar conexiones no deseadas o procesos en los servidores y routers y ajustar sus parámetros de TCP / IP.
- Configure filtros de salida para bloquear el tráfico de sus sistemas y pueden enviar en respuesta al tráfico DDoS, para evitar con esto la adición de paquetes innecesarios a la red.
- Controle el contenido que se entrega a los usuarios y sesiones a detalle.

En caso de un intento de extorsión, trata de ganar tiempo con el estafador. Por ejemplo, explicar que necesita más tiempo con el fin de obtener la aprobación de gestión.

Si se detecta un cuello de botella en el ISP, sólo el ISP puede tomar medidas eficientes. En ese caso, trabajar en estrecha colaboración con su proveedor de Internet y asegúrese de que usted comparte información del problema de comunicación.

4.5.4 Paso 4. Remediación

Tomar acciones para detener la condición de denegación de servicio.

Póngase en contacto con sus proveedores/especialistas, en las soluciones donde ha sido efectuado el ataque y asegúrese de que hace cumplir las medidas de remediación. Mantener activo los equipos de protección de primer nivel que dispone la empresa para la defensa de un ataque DDoS. Para obtener más información, aquí están algunas de las posibles medidas:

- Filtrado (si es posible a nivel de Tier 1 o 2)
- Limpieza de Tráfico
- Enrutamiento específico.

Si se han identificado los causantes del ataque de DDoS, se deben efectuar medidas que la ley local cubra.

Esto lo debe realizar el equipo de ejecutivos y representantes legales de la empresa.

4.5.5 Paso 5. Recuperación

Volver al estado funcional anterior.

Evaluar el final de la condición DDoS

- Asegúrese de que los servicios afectados son accesibles de nuevo.
- Asegúrese de que el rendimiento de su infraestructura vuelve al rendimiento de referencia.

Deshacer las medidas de mitigación

- Cambie de nuevo el tráfico a su red original.
- Reinicie servicios detenidos.

Asegúrese de que las acciones relacionadas con la recuperación se deciden de acuerdo con su equipo de trabajo.

Devolver los servicios a su estado normal podría tener efectos secundarios inesperados.

4.5.6 Paso 6. Secuelas o repercusiones pos-ataque

Documentar los detalles del incidente, discutir las lecciones aprendidas, y ajustar los planes y las defensas.

- Considere que pasos de preparación podría haber adoptado para responder al incidente más rápido y eficaz.
- Si es necesario, ajuste los procedimientos en base a las decisiones tomadas durante la preparación incidente DDoS.
- Evaluar la eficacia de su proceso de respuesta DDoS, la participación de personas y comunicaciones.
- Considere las relaciones que dentro y fuera de su empresa podrían ayudar con incidentes en el futuro.
- Colaborar con los equipos legales si una acción legal está en proceso.

4.6 Diseño del Plan de Pruebas

El diseño de Plan de Pruebas contempla la ejecución de ataques de DDOS sobre un ambiente controlado en la red empresarial.

Se levantarán ambientes paralelos y similares a los ambientes de producción para no afectar la operatividad de la empresa y no dañar los recursos de la red.

Los servicios considerados dentro del plan de pruebas son el Correo Electrónico y El servidor Web donde se aloja la página web de la empresa.

Los escenarios a considerar en el plan de pruebas son los siguientes:

- Ejecución controlada de ataques de DDOS a un servidor de correo electrónico
    - Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood)
    - Ataque de envío masivo de correo electrónico no deseado (SPAM)

- Ejecución controlada de ataques de DDOS a un servidor web
    - Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood)
    - Ataque de inundación de peticiones HTTP mediante el método de envío de parámetros por dirección web (HTTP GET Flood)

Las métricas que se consideran para medir la efectividad de las pruebas son las siguientes:

- Efectividad del Bloqueo, donde se medirá la capacidad del dispositivo de seguridad para detectar y bloquear el ataque.
- Precisión de la Detección, se medirá la capacidad del dispositivo en detectar el tráfico legítimo del no legítimo y minimizar los falsos positivos que se generan.
- Robustez, mide las técnicas usadas por el dispositivo para evadir el ataque.
- Rendimiento, en este punto se medirán los parámetros definidos como el número máximo de conexiones soportadas, ancho de banda, volumen de tráfico (throughput), tiempos de respuesta que serán medidos con y sin amenazas existentes.

- Estabilidad, se medirá la capacidad de la infraestructura para mantener los niveles de protección estables.

En el Anexo 4 Matriz de pruebas para un ambiente con y sin ataques DDOS, se muestra la matriz de pruebas a utilizar para la ejecución de pruebas, el cual será aplicado en un ambiente con y sin amenazas de ataque.

CAPÍTULO 5

IMPLEMENTACIÓN Y PRUEBAS

5.1 Implementación del Diseño propuesto

Previo a la implementación de los equipos en la red, se realizó un análisis del tráfico diario en el periodo de un mes que genera y recibe la empresa. Con ello se definieron los parámetros necesarios que serán configurados en el equipo anti DDOS.

Se obtuvieron datos tanto del tráfico normal como del consumo de los recursos de los equipos de comunicación, con la finalidad de contar con una fotografía del estado actual de la red que pueda ser comparada posterior a la implementación del diseño propuesto. El detalle puede ser observado en el Anexo 5.

El equipo anti DDOS basa su principal característica en no necesitar aprender de la red una vez puesto en producción, basa su funcionalidad en umbrales definidos por el usuario obtenidos del análisis realizado de la red y a las buenas prácticas en la seguridad.

Con la autorización de la empresa y en horarios de pocas transacciones de los usuarios para no afectar la operación diaria, se procede a instalar el equipo en la red.

Una vez colocado el equipo anti DDOS en la red, se procede a configurar los parámetros definidos en el numeral 4.3 Protección: Configuración de equipos en la red.

Establecimos un periodo de una semana de monitoreo para ajustar el comportamiento del equipo anti DDOS, tiempo en el cual no fue necesario realizar ajustes en el equipo y no se reportaron inconformidades por parte de los usuarios.

Luego de la semana se afinamiento, se coordinaron las pruebas controladas sobre dos equipos replica que simulaban los servicios de correo electrónico y página web. Estos equipos tienen las mismas

configuraciones de los equipos en producción y servirán para realizar las pruebas en un ambiente controlado, ya que de hacerlas en el ambiente original podríamos provocar daños irreparables que pondría en riesgo la operación de la empresa.

5.2 Ejecución del Plan de Pruebas

En este apartado, mostraremos la etapa 1 del Plan de Pruebas para ataques DDOS en la red empresarial.

Para las etapas 2 y 3 del plan de pruebas, los datos obtenidos serán mostrados en el punto 5.3 de Validación de pruebas.

Cabe mencionar que los ataques realizados son repetibles, lo que facilita a la empresa revalidar en cualquier momento las actividades realizadas y tomar acciones necesarias para mejora de su seguridad perimetral.

Tabla 9 Datos obtenidos de la primera etapa del plan de pruebas, conforme al Plan de Pruebas para ataques DDOS sobre la red empresarial.

Plan de pruebas para ataques de DDOS sobre la red empresarial			
Actividad/Ataque	**Ejecutado / Fallido**	**Datos Obtenidos**	**Comentarios**
Definir los Servicios a probar	Ejecutado	- Correo Electrónico - Portal Web	--
Definir IP o rangos de IP	Ejecutado	- 192.168.150.80 - 192.168.150.176	--
Definir los tipos de ataques a realizar	Ejecutado	- TCP SYN Flood - SPAM - HTTP GET Flood	--
Definir las variables de rendimiento - Ancho de banda: - Aplicaciones: - Conexiones recurrentes: - Ataques recurrentes:	Ejecutado	 - 4MB - HTTP, HTTPS, SMTP - 100 - 1	--
Establecer tiempo de ejecución	Ejecutado	- 1 minuto por ataque	--
Rendimiento de equipos sin ataques			

- Equipo Anti DDOS
  - Memoria:
  - Procesador:
	Ejecutado	
		- 3%
		- 2%
			--

- Sistema de Detección de Intrusos
  - Memoria:
  - Procesador:
	Ejecutado	
		
		- 5%
		- 7%
			--

- Cortafuegos
  - Memoria:
  - Procesador:
	Ejecutado	
		- 3%
		- 10%
			--

- Router
  - Memoria:
  - Procesador:
	Ejecutado	
		- 23%
		- 6%
			--

5.2.1 Ejecución controlada de ataques de DDOS a un servidor de correo electrónico.

Consideramos realizar cada ataque DDOS por separado con la finalidad de determinar los valores reales de rendimiento de los equipos para cada ataque.

5.2.1.1 Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood)

Para la realización de este ataque se utilizaron comandos ejecutados desde equipos bots con sistema operativo Linux y no se consideró el uso de aplicaciones propietarias.

El ataque TCP SYN Flood se llevó a cabo con el siguiente comando desde equipos externos a la red empresarial:

hping3 -i u1 -S -p 25 <IP pública de 192.168.150.80>

La descripción del comando hping3 se detalla en la Tabla 10.

Tabla 10 Descripción de parámetros del comando hping3.

Parámetros	Descripción
-i u1	Espera por 1 microsegundo entre cada paquete enviado
-S	Indica bandera SYN
-p 25	Puerto de destino 25
<IP publica de 192.168.150.80>	Dirección IP objeto del ataque

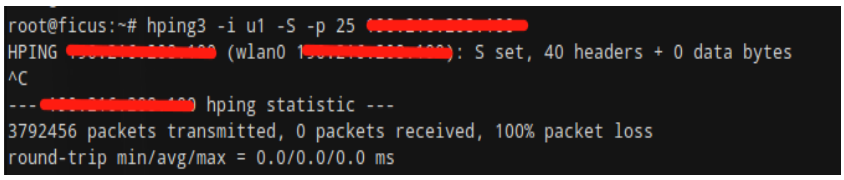


Figura 5.27 Ejecución de comando para ataque TCP SYN Flood hacia el servicio de correo electrónico.
Fuente: Autoría propia

La ejecución del comando tuvo una duración de un minuto, luego del cual al finalizar el ataque se tiene como resultado 3572934 paquetes transmitidos, 0 paquetes recibidos, 100% de paquetes perdidos.

5.2.1.2 Ataque de envío masivo de correo electrónico no deseado (SPAM)

Para la realización de este ataque se utilizó una herramienta de distribución libre llamada MESS BOMBER [12], la cual pone a prueba la capacidad del servidor de manejar ataques sobre la capa de Aplicación del modelo OSI.

Esta herramienta fue creada por Messhacker [13] y puede ser descargada desde la misma página.

El ataque SPAM se llevó a cabo con la herramienta MESS BOMBER desde 2 equipos bot externos hacia la red empresarial. Cada equipo envía hasta 1000 correos electrónicos por cada ejecución hacia la cuenta invitado@acme.sytes.net, en un intervalo de 60 a 65 correos por segundo por cada equipo. El dominio acme.sytes.net fue creado temporalmente para no atacar el dominio actual de la empresa. Así como también se creó una cuenta temporal llamada invitado. El dominio acme.sytes.net esta direccionado a nuestro servidor de

correo electrónico que fue clonado del servidor de producción, pero con una IP publica diferente. La empresa sytes.net provee de dominios por tres días sin costo, tiempo suficiente para nuestra prueba.

Figura 5.28 Envío de parámetros para ejecución de ataque de envío masivo de correo electrónico no deseado (SPAM) mediante la herramienta MESS BOMBER
Fuente: Autoría propia

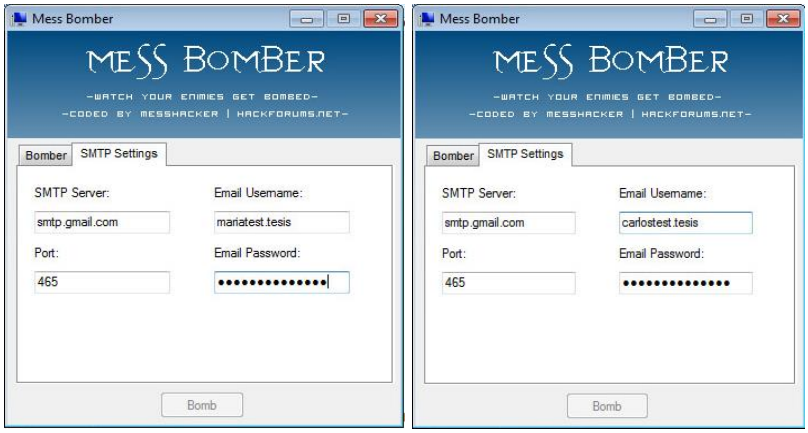


Figura 5.29 Cuentas de correo electrónico que se usaron para el envío de SPAM mediante la herramienta MESS BOMBER.
Fuente: Autoría propia

Para la prueba del ataque fueron creadas dos cuentas de correo electrónico desde donde se hace el envío de correos SPAM masivos. Las cuentas creadas son carlostest.tesis@gmail.com y mariatest.tesis@gmail.com.

La descripción de los parámetros utilizados por la herramienta MESS BOMBER se detalla en la Tabla 11:

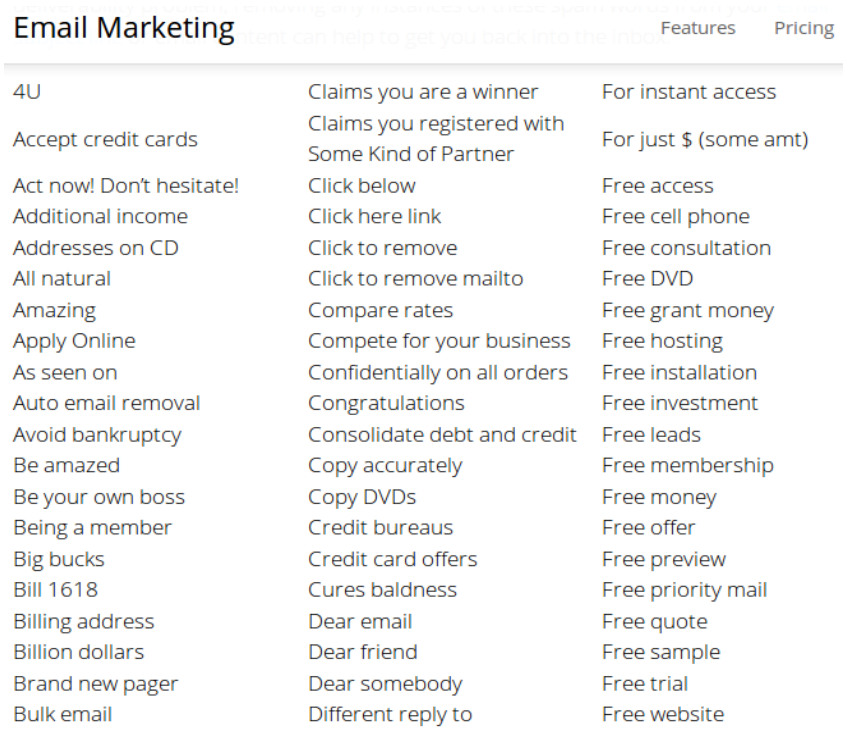
Tabla 11 Descripción de parámetros de la herramienta MASS BOMBER.

Parámetros	**Descripción**
to:	Dirección de correo objetivo
How many times	Cantidad de emails a enviar como spam
Subject	Descripción del mensaje
Message	Mensaje con las palabras identificadas como SPAM por las herramientas de correo.
SMTP SETTINGS	Se definen las cuentas desde donde se envían los emails.

La ejecución del ataque tuvo un tiempo de duración de 16 segundos, en donde el equipo de protección identificó el ataque bajo el concepto de alto volumen de tráfico de correo electrónico (SMTP).

El contenido de cada correo electrónico incluye palabras identificadas como las más usadas para detectar un correo SPAM, esta definición de palabras ha sido publicada por la página emailmarketing.comm100.com [14].

A continuación, se adjunta un extracto de las palabras publicadas por emailmarketing.comm100.com:



Email Marketing

Features Pricing

4U	Claims you are a winner	For instant access
Accept credit cards	Claims you registered with Some Kind of Partner	For just $ (some amt)
Act now! Don't hesitate!	Click below	Free access
Additional income	Click here link	Free cell phone
Addresses on CD	Click to remove	Free consultation
All natural	Click to remove mailto	Free DVD
Amazing	Compare rates	Free grant money
Apply Online	Compete for your business	Free hosting
As seen on	Confidentially on all orders	Free installation
Auto email removal	Congratulations	Free investment
Avoid bankruptcy	Consolidate debt and credit	Free leads
Be amazed	Copy accurately	Free membership
Be your own boss	Copy DVDs	Free money
Being a member	Credit bureaus	Free offer
Big bucks	Credit card offers	Free preview
Bill 1618	Cures baldness	Free priority mail
Billing address	Dear email	Free quote
Billion dollars	Dear friend	Free sample
Brand new pager	Dear somebody	Free trial
Bulk email	Different reply to	Free website

Figura 5.30 Ejemplo de palabras más usadas en un correo SPAM publicadas por EmailMarketing
Fuente: Autoría propia

En las configuraciones del servidor de correo electrónico de la Empresa de Servicios, se ha considerado una escala de puntuación para correos recibidos, donde a cada uno se le asigna un valor al cumplir con ciertos parámetros definidos previamente. Si la suma de este puntaje sobrepasa los 6.6 puntos entonces es considerado como SPAM. Durante nuestro ataque de SPAM, el puntaje promedio para cada

correo fue de 12.678, con lo cual el tráfico que logró pasar fue detectado por el servidor de correos como malicioso.

```
Return-Path: carlostest.tesis@gmail.com
Received: from mail.acme.com (LHLO mail.acme.com) (192.168.150.80) by
 mail.acme.com with LMTP; Sun, 8 Nov 2015 02:05:34 -0500 (ECT)
Received: from localhost (localhost [127.0.0.1])
        by mail.acme.com (Postfix) with ESMTP id 5416BA1D80
        for <invitado@acme.sytes.net>; Sun,  8 Nov 2015 02:05:34 -0500 (ECT)
X-Virus-Scanned: amavisd-new at mail.acme.com
X-Spam-Flag: YES
X-Spam-Score: 12.678
X-Spam-Level: ************
X-Spam-Status: Yes, score=12.678 tagged_above=-10 required=6.6
        tests=[BAD_CREDIT=2.415, BAYES_50=0.8, DIET_1=0.001, DKIM_SIGNED=0.1,
        DKIM_VALID=-0.1, DKIM_VALID_AU=-0.1, DRUGS_ERECTILE=1.994,
        FIN_FREE=2.7, FREEMAIL_FROM=0.001, HTML_MESSAGE=0.001,
        JOIN_MILLIONS=1.026, NO_DNS_FOR_FROM=0.001, NO_MEDICAL=1.773,
        ONLINE_PHARMACY=0.65, TVD_VISIT_PHARMA=1.406,
        T_FILL_THIS_FORM_SHORT=0.01] autolearn=no autolearn_force=no
Authentication-Results: mail.acme.com (amavisd-new); dkim=pass (2048-bit key)
        header.d=gmail.com
Received: from mail.acme.com ([127.0.0.1])
        by localhost (mail.acme.com [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id 2I1UO-9m2TIe for <invitado@acme.sytes.net>;
        Sun,  8 Nov 2015 02:05:34 -0500 (ECT)
Received: from mail-ig0-f176.google.com (mail-ig0-f176.google.com [209.85.213.176])
        by mail.acme.com (Postfix) with ESMTPS id 5A183A1C23
        for <invitado@acme.sytes.net>; Sun,  8 Nov 2015 02:05:34 -0500 (ECT)
```

Figura 5.31 Detalle de la cabecera de correo de un SPAM recibido
Fuente: Autoría propia

Durante la ejecución del ataque, se logra evidenciar en los registros del servidor de correos los correos electrónicos que él clasifica como SPAM y que logran llegar a su destino producto del umbral definido en Andrisoft.

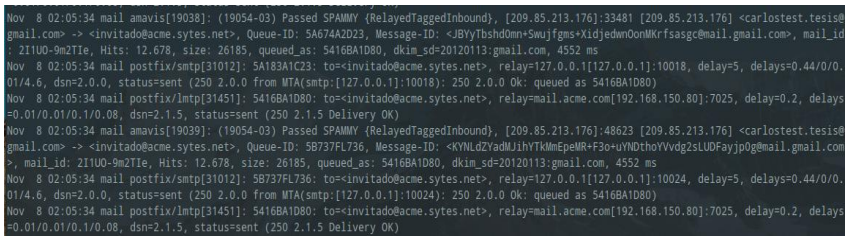


Figura 5.32 Detalle de emails que el servidor de correos identifica como correo basura (SPAM)
Fuente: Autoría propia

Los correos que lograron llegar a la cuenta del usuario invitado@acme.sytes.net, fueron enviados directamente a la bandeja de correo basura.

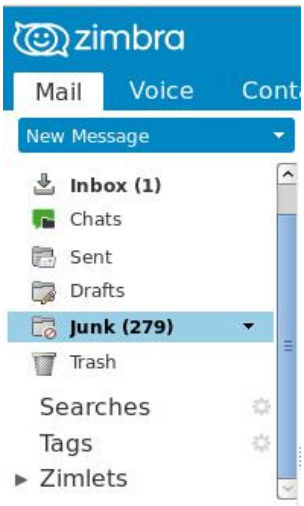


Figura 5.33 Muestra de la cantidad de correos basura que recibe el usuario invitado@acme.sytes.net durante el ataque.
Fuente: Autoría propia

5.2.2 Ejecución controlada de ataques de DDOS a un servidor web

Al igual que los ataques anteriores, para los ataques al servidor web fueron realizados por separado, tiempo en el cual los recursos del servidor volverán a su estado normal.

5.2.2.1 Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood)

Para la realización de este ataque se utilizó la herramienta de distribución libre Wbox [15], la cual está escrita en lenguaje ANSI C y puede ser ejecutada en ambientes Windows.

Esta herramienta está bajo licencia BSD (Berkeley Software Distribution), la cual tiene menos restricciones que otras licencias como GNU GPL (GNU General Public License), casi cercana al dominio público.

El ataque TCP SYN Flood se llevó a cabo con el siguiente comando desde equipos bots externos a la red empresarial:

wbox <IP pública de 192.168.150.176> clients 5000 dump

El comando wbox tiene la Tabla 12:

Tabla 12 Descripción de parámetros del comando wbox.

Parámetros	Descripción
<IP publica de 192.168.150.176>	Dirección IP objeto del ataque
clients 5000	Cantidad de solicitudes que se van a enviar
dump	Obtener la cabecera de HTTP reply

A continuación, se muestra una captura de pantalla de la ejecución del ataque, el cual tuvo una duración de un minuto aproximadamente:

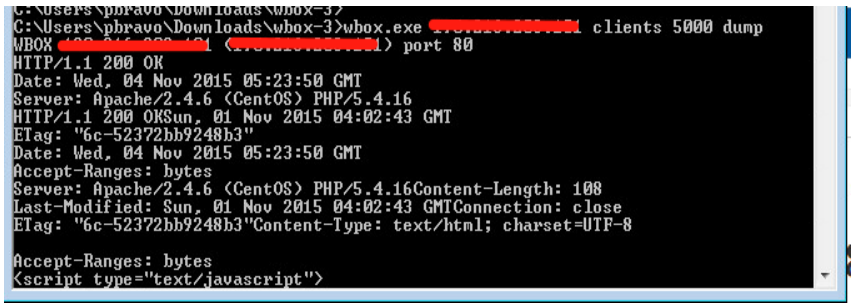


Figura 5.34 Ejecución de comando para ataque TCP SYN Flood hacia el servidor web
Fuente: Autoría propia

5.2.2.2 Ataque de inundación de peticiones HTTP mediante el método de envío de parámetros por dirección web (HTTP GET Flood)

El ataque HTTP GET Flood fue generado desde equipos bots externos a la red empresarial, fue generado mediante la herramienta LOIC, la cual es una herramienta desarrollada por Praetox Technologies que se usa para realizar ataques de denegación de servicio distribuido a un solo objetivo, y dispone las opciones de ejecutar el ataque del tipo TCP, UDP, y HTTP.

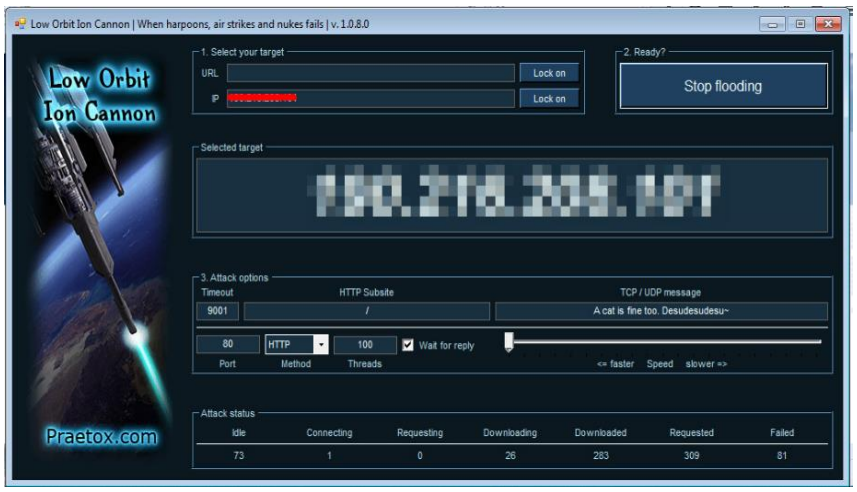


Figura 5.35 Ejecución de herramienta LOIC para ataque HTTP GET Flood hacia el servidor web
Fuente: Autoría propia

En la herramienta se define la IP Pública del sitio web, así como también el puerto, el tipo de ataque que para este caso es del tipo HTTP y finalmente la cantidad de amenazas que se van a interactuar durante el ataque.

5.3 Validación de Pruebas

Se mostrarán los datos obtenidos de las pruebas realizadas conforme a la actividad detectada por la herramienta Andrisoft y las acciones tomadas por la misma.

5.3.1 Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood) Mail

La herramienta Andrisoft nos ayuda a detectar la anomalía que se ha generado hacia el servidor de correos. Los detalles de la anomalía presentada se muestran a continuación:

- Se detecta una anomalía del tipo TCP+SYN.
- El tiempo de la anomalía fue de 1 minuto con 21 segundos.
- La IP a quien va dirigido el tráfico es la 192.168.150.80.

- El umbral definido para este comportamiento se activa para tráfico superior a 0.5K paquetes por segundo (pkts/s). El ataque realizado fue de 0.9K paquetes por segundo (pkts/s).

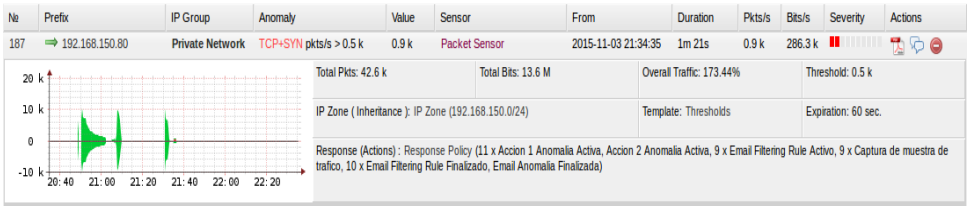


Figura 5.36 Detalle de la anomalía que la herramienta Andrisoft detectó durante el ataque.
Fuente: Autoría propia

Durante el ataque, se realizó una captura de paquetes como muestra del comportamiento.

Aquí notamos que el puerto objetivo es el 25 TCP correspondiente al protocolo SMTP, la IP pública que genera el ataque es la 200.69.170.86. Los paquetes enviados son del tipo SYN, sin la bandera de ACK definida.

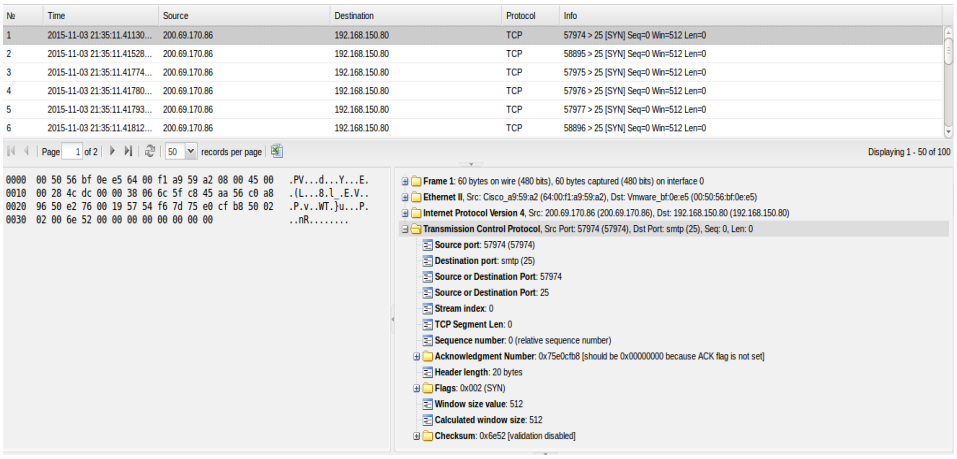


Figura 5.37 Detalle de uno de los paquetes capturados durante la detección de la anomalía.
Fuente: Autoría propia

Se realizaron pruebas de acceso al buzón de correo electrónico y envío de correo a un usuario de prueba sin inconvenientes, como se puede evidenciar en los registros del servidor:

```
Nov  3 21:34:55 mail postfix/smtp[16854]: AA8D1A1390: from=<omar.cordova@acme.com>, relay=127.0
.0.1[127.0.0.1]:10026, to=<karol.briones@acme.com> delay=0.15, delays=0.01/0/0/0.14, dsn=2.0.0,
 status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10030): 250 2.0.0 Ok: queued as C0B5DA16BB)
Nov  3 21:34:55 mail postfix/qmgr[5061]: AA8D1A1390: removed
```

Figura 5.38 Evidencia de la disponibilidad del servicio de correo electrónico durante el ataque TCP+SYN Flood, en los registros del servidor.
Fuente: Autoría propia

En la Tabla 13 se mostrarán los datos obtenidos del ataque realizado para cada una de las mediciones consideradas:

Tabla 13 Datos obtenidos del ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood) para el servicio de Correo Electrónico, conforme al Plan de Pruebas para ataques DDOS sobre la red empresarial.

Plan de pruebas para ataques de DDOS sobre la red empresarial			
Actividad/Ataque	**Ejecutado / Fallido**	**Datos Obtenidos**	**Comentarios**
Ejecución de pruebas de rendimiento con ataques			
- Ejecución controlada de ataques de DDOS a un servidor de correo electrónico	Ejecutado	--	--
- Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood)	Ejecutado	- Total Pkts: 42.6 k detectados - Duración 1m 21s - 11 interacciones del tipo tcp+syn	--
- Efectividad	Ejecutado	Se detecta una anomalía No.187 mostrada en la Figura 5.36	--
- Precisión	Ejecutado	Se identifica la anomalía del tipo TCP+SYN pkts/s > 0.5 k	--
- Robustez	Ejecutado	Acciones en respuesta de la anomalía: - 11 Acciones detectadas dentro de la anomalía. - Envío de alerta de email por presencia de anomalía. - Activación de reglas de filtrado	--

		y notificación de las mismas. -Captura de muestra de tráfico. - Envío de Email finalizada las reglas de Filtrado. - Envío de Email por Anomalía Finalizada	

- Rendimiento
  - Número máximo de conexiones soportadas
  - Ancho de banda
  - Throughput
  - Tiempos de respuesta
	Ejecutado	- 11 conexiones identificadas
		- Ancho de banda usado 286.3 kbits/s
		- Throughput usado 0.9 k pkts/s
		- Tiempo de respuesta <5sec
			--

- Estabilidad	Ejecutado	Servicio de email disponible para usuarios.	La prueba se realizó con un usuario de prueba accediendo al correo electrónico. Ver Figura 5.38.

5.3.2 Ataque de envío masivo de correo electrónico no deseado (SPAM)

La herramienta Andrisoft nos ayuda a detectar la anomalía que se ha generado hacia el servidor de correos. Los detalles de la anomalía presentada se muestran a continuación:

- Se detecta una anomalía del tipo MAIL SPAM.
- El tiempo de la anomalía fue de 16 segundos.
- La IP a quien va dirigido el tráfico es la 192.168.150.80.
- El umbral definido para este comportamiento se activa para tráfico superior a 4.0M bits por segundo (bits/s). El ataque realizado fue de 26.3M bits por segundo (bits/s).

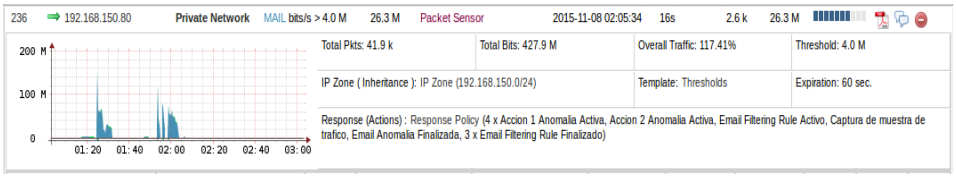


Figura 5.39 Detalle de la anomalía que la herramienta Andrisoft detectó durante el ataque.
Fuente: Autoría propia

Durante el ataque, se realizó una captura de paquetes como muestra del comportamiento. Aquí notamos que el puerto objetivo

es el 25 TCP correspondiente al protocolo SMTP, las IPs públicas que generan el ataque son 209.85.213.176 y 10.36.104.213.

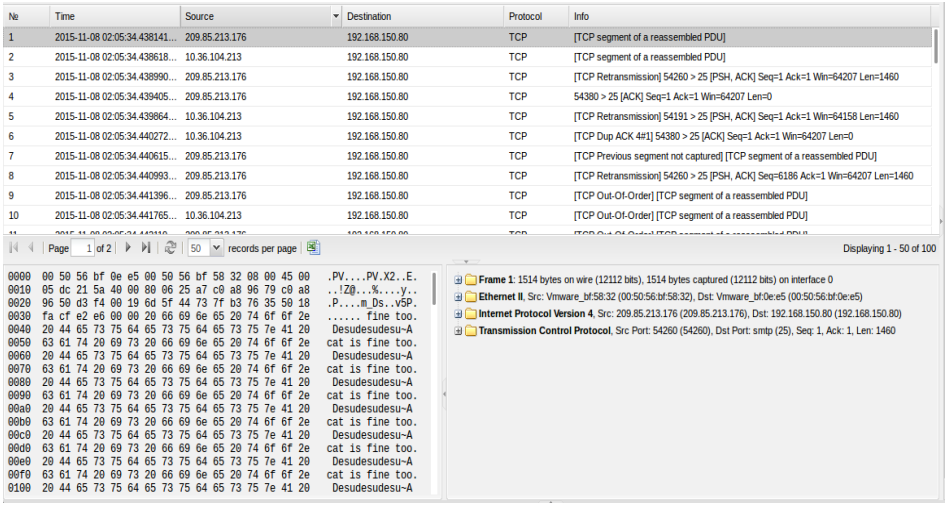


Figura 5.40 Detalle de uno de los paquetes capturados durante la detección de la anomalía.
Fuente: Autoría propia

Se realizaron pruebas de acceso al buzón de correo electrónico y envío de correo a un usuario de prueba sin inconvenientes, como se puede evidenciar en los registros del servidor:

```
Nov  8 02:05:38 mail postfix/qmgr[5061]: 9F1ABA1EFF: from=<karolitab@gmail.com>, size=3092, nrcpt=1 (queue active)
Nov  8 02:05:38 mail amavis[17879]: (17879-05) xogV-x0Rvl_1 FWD from <karolitab@gmail.com> -> <invitado@acme.sytes.net>, BODY=7
BIT 250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 9F1ABA1EFF
Nov  8 02:05:38 mail amavis[17879]: (17879-05) Passed CLEAN {RelayedInbound}, [209.85.223.171]:36542 [209.85.223.171] <karolita
b@gmail.com> -> <invitado@acme.sytes.net>, Queue-ID: 08929A1EE4, Message-ID: <CAGRC_W=V1R4e1Z+7dpAB-87x41pC2yiBk6m=5EnFjTE1qCkc
Jw@mail.gmail.com>, mail_id: xogV-x0Rvl_1, Hits: 0.703, size: 2265, queued_as: 9F1ABA1EFF, dkim_sd=20120113:gmail.com, 352 ms
```

Figura 5.41 Evidencia de la disponibilidad del servicio de correo electrónico durante el ataque de envío masivo de correo electrónico no deseado (SPAM), en los registros del servidor.
Fuente: Autoría propia

En la Tabla 14 se mostrarán los datos obtenidos del ataque realizado para cada una de las mediciones consideradas.

Tabla 14 Datos obtenidos del ataque de envío masivo de correo electrónico no deseado (SPAM) para el servicio de Correo Electrónico, conforme al Plan de Pruebas para ataques DDOS sobre la red empresarial.

Plan de pruebas para ataques de DDOS sobre la red empresarial			
Actividad/Ataque	**Ejecutado / Fallido**	**Datos Obtenidos**	**Comentarios**
Ejecución de pruebas de rendimiento con ataques			
- Ejecución controlada de ataques de DDOS a un servidor de correo electrónico	Ejecutado	--	--
- Ataque de envío masivo de correo electrónico no deseado (SPAM)	Ejecutado	- Total Pkts: 41.9 k detectados - Duración 16s - 4 interacciones del tipo Mail	--
- Efectividad	Ejecutado	Se detecta una anomalía No.236 mostrada en la Figura 5.39	--
- Precisión	Ejecutado	Se identifica la anomalía del tipo MAIL bits/s > 4.0 M	--
- Robustez	Ejecutado	Acciones en respuesta de la anomalía: - 4 Acciones detectadas	--

		dentro de la anomalía. - Envío de alerta de email por presencia de anomalía. - Activación de reglas de filtrado y notificación de las mismas. -Captura de muestra de tráfico. - Envío de Email finalizada las reglas de Filtrado. - Envío de Email por Anomalía Finalizada	

- Rendimiento
  - Número máximo de conexiones soportadas
  - Ancho de banda
  - Throughput
  - Tiempos de respuesta
	Ejecutado	- 3 conexiones identificadas (2 por ataque)
		- Ancho de banda usado 4.3 Mbits/s
		- Throughput usado 41.9 kpkts
		- Tiempo de respuesta <5sec
			--

- Estabilidad	Ejecutado	Servicio de email disponible para usuarios.	La prueba se realizó con un usuario de prueba accediendo al correo electrónico. Ver Figura 5.41.

5.3.3 Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood) para el Servidor Web

La herramienta Andrisoft nos ayuda a detectar la anomalía que se ha generado hacia el servidor web. Los detalles de la anomalía presentada se muestran a continuación:

- Se detecta una anomalía del tipo TCP+SYN.
- El tiempo de la anomalía fue de 1 minuto con 21 segundos.
- La IP a quien va dirigido el tráfico es la 192.168.150.176.
- El umbral definido para este comportamiento se activa para tráfico superior a 1K paquetes por segundo (pkts/s). El ataque realizado fue de 1.2K paquetes por segundo (pkts/s).

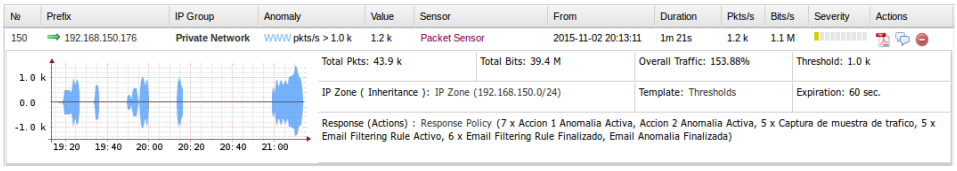
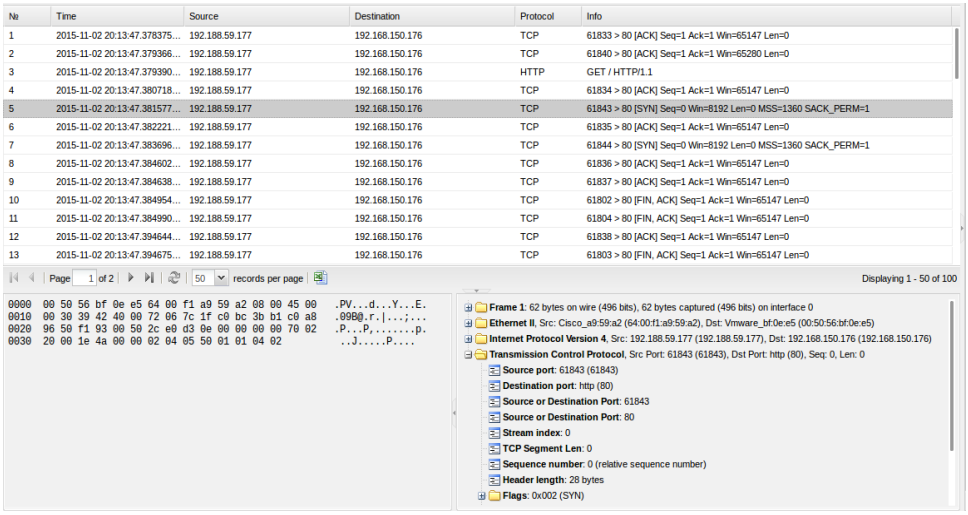


Figura 5.42 Detalle de la anomalía que la herramienta Andrisoft detectó durante el ataque.
Fuente: Autoría propia

Durante el ataque, se realizó una captura de paquetes como muestra del comportamiento. Aquí notamos que el puerto objetivo es el 80 TCP correspondiente al protocolo HTTP, la IP pública que genera el ataque es la 192.188.59.177. Los paquetes enviados son del tipo SYN, sin la bandera de ACK definida.



№	Time	Source	Destination	Protocol	Info
1	2015-11-02 20:13:47.378375…	192.188.59.177	192.168.150.176	TCP	61833 > 80 [ACK] Seq=1 Ack=1 Win=65147 Len=0
2	2015-11-02 20:13:47.379366…	192.188.59.177	192.168.150.176	TCP	61840 > 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
3	2015-11-02 20:13:47.379390…	192.188.59.177	192.168.150.176	HTTP	GET / HTTP/1.1
4	2015-11-02 20:13:47.380718…	192.188.59.177	192.168.150.176	TCP	61834 > 80 [ACK] Seq=1 Ack=1 Win=65147 Len=0
5	2015-11-02 20:13:47.381577…	192.188.59.177	192.168.150.176	TCP	61843 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 SACK_PERM=1
6	2015-11-02 20:13:47.382221…	192.188.59.177	192.168.150.176	TCP	61835 > 80 [ACK] Seq=1 Ack=1 Win=65147 Len=0
7	2015-11-02 20:13:47.383696…	192.188.59.177	192.168.150.176	TCP	61844 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 SACK_PERM=1
8	2015-11-02 20:13:47.384602…	192.188.59.177	192.168.150.176	TCP	61836 > 80 [ACK] Seq=1 Ack=1 Win=65147 Len=0
9	2015-11-02 20:13:47.384638…	192.188.59.177	192.168.150.176	TCP	61837 > 80 [ACK] Seq=1 Ack=1 Win=65147 Len=0
10	2015-11-02 20:13:47.384954…	192.188.59.177	192.168.150.176	TCP	61802 > 80 [FIN, ACK] Seq=1 Ack=1 Win=65147 Len=0
11	2015-11-02 20:13:47.384990…	192.188.59.177	192.168.150.176	TCP	61804 > 80 [FIN, ACK] Seq=1 Ack=1 Win=65147 Len=0
12	2015-11-02 20:13:47.394644…	192.188.59.177	192.168.150.176	TCP	61838 > 80 [ACK] Seq=1 Ack=1 Win=65147 Len=0
13	2015-11-02 20:13:47.394675…	192.188.59.177	192.168.150.176	TCP	61803 > 80 [FIN, ACK] Seq=1 Ack=1 Win=65147 Len=0

Page 1 of 2 | 50 records per page | Displaying 1 - 50 of 100

```
0000  00 50 56 bf 0e e5 64 00 f1 a9 59 a2 08 00 45 00   .PV...d...Y...E.
0010  00 30 39 42 40 00 72 06 7c 1f c0 bc 3b b1 c0 a8   .09B@.r.|...;...
0020  96 50 f1 93 00 50 2c e0 d3 0e 00 00 00 00 70 02   .P...P,.......p.
0030  20 00 1e 4a 00 00 02 04 05 50 01 01 04 02         ..J.....P....
```

- **Frame 1**: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
- **Ethernet II**, Src: Cisco_a9:59:a2 (64:00:f1:a9:59:a2), Dst: Vmware_bf:0e:e5 (00:50:56:bf:0e:e5)
- **Internet Protocol Version 4**, Src: 192.188.59.177 (192.188.59.177), Dst: 192.168.150.176 (192.168.150.176)
- **Transmission Control Protocol**, Src Port: 61843 (61843), Dst Port: http (80), Seq: 0, Len: 0
  - **Source port**: 61843 (61843)
  - **Destination port**: http (80)
  - **Source or Destination Port**: 61843
  - **Source or Destination Port**: 80
  - **Stream index**: 0
  - **TCP Segment Len**: 0
  - **Sequence number**: 0 (relative sequence number)
  - **Header length**: 28 bytes
  - **Flags**: 0x002 (SYN)

Figura 5.43 Detalle de uno de los paquetes capturados durante la detección de la anomalía.
Fuente: Autoría propia

Se realizaron pruebas de acceso a la página web empresarial sin inconvenientes, como se puede evidenciar en la siguiente captura de pantalla:

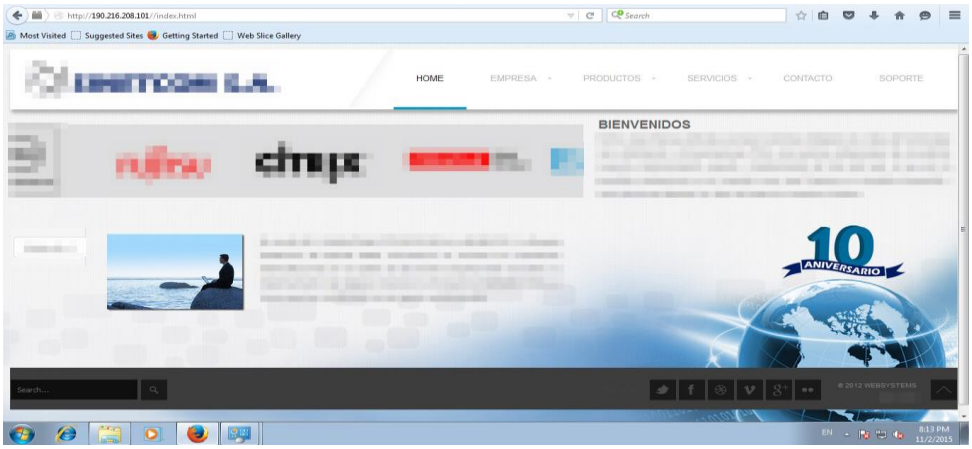


Figura 5.44 Evidencia de la disponibilidad de la página web empresarial de pruebas durante el ataque TCP+SYN Flood.
Fuente: Autoría propia

En la Tabla 15 se mostrarán los datos obtenidos del ataque realizado para cada una de las mediciones consideradas:

Tabla 15 Datos obtenidos del ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood) para el Servidor Web, conforme al Plan de Pruebas para ataques DDOS sobre la red empresarial.

Plan de pruebas para ataques de DDOS sobre la red empresarial			
Actividad/Ataque	**Ejecutado / Fallido**	**Datos Obtenidos**	**Comentarios**
Ejecución de pruebas de rendimiento con ataques			
- Ejecución controlada de ataques de DDOS a un servidor web	Ejecutado	--	--
- Ataque de envío masivo de solicitudes de conexión	-	- Total Total Pkts: 43.9 k detectados - Duración 1m 21s - 7 anomalías detectadas del tipo	--

TCP (TCP SYN Flood)		WWW (TCP + SYN)	
- Efectividad	Ejecutado	Se detecta una anomalía No.150 mostrada en la Figura 5.42	--
- Precisión	Ejecutado	Se identifica la anomalía del tipo WWW pkts/s > 1.0 k	--
- Robustez	Ejecutado	Acciones en respuesta de la anomalía: - 7 Acciones detectadas dentro de la anomalía. - Envío de alerta de email por presencia de anomalía. - Activación de reglas de filtrado y notificación de las mismas. - 6 Capturas de muestra de tráfico. - Envío de Email finalizada las reglas de Filtrado. - Envío de Email por Anomalía Finalizada	--
- Rendimiento - Número máximo de conexiones soportadas - Ancho de banda - Throughput - Tiempos de respuesta	Ejecutado	- 7 conexiones identificadas - Ancho de banda usado 1.1 Mbits/s - Throughput usado 1.2 k pkts/s - Tiempo de respuesta <5sec	--
- Estabilidad	Ejecutado	Servicio de la página web disponible.	La prueba se realizó accediendo a la página web. Ver Figura 5.44.

5.3.4 Ataque de inundación de peticiones HTTP mediante el método de envío de parámetros por dirección web (HTTP GET Flood).

En la herramienta Andrisoft se ha detectado una anomalía dirigida al servidor web. La anomalía presenta los siguientes datos en detalle:

- Se detecta una anomalía del tipo HTTP.
- El tiempo de la anomalía fue de 15 segundos.
- La IP a quien va dirigido el tráfico es la 192.168.150.176.
- El umbral definido para este comportamiento se activa para tráfico superior a 2K paquetes por segundo (pkts/s). El ataque realizado fue de 7.8 K paquetes por segundo (pkts/s).

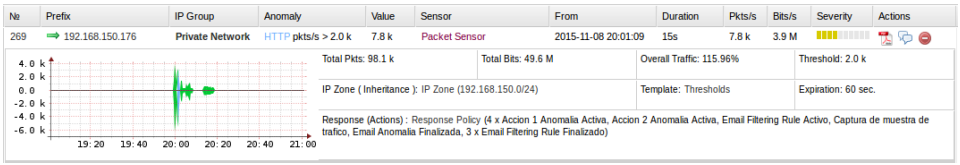
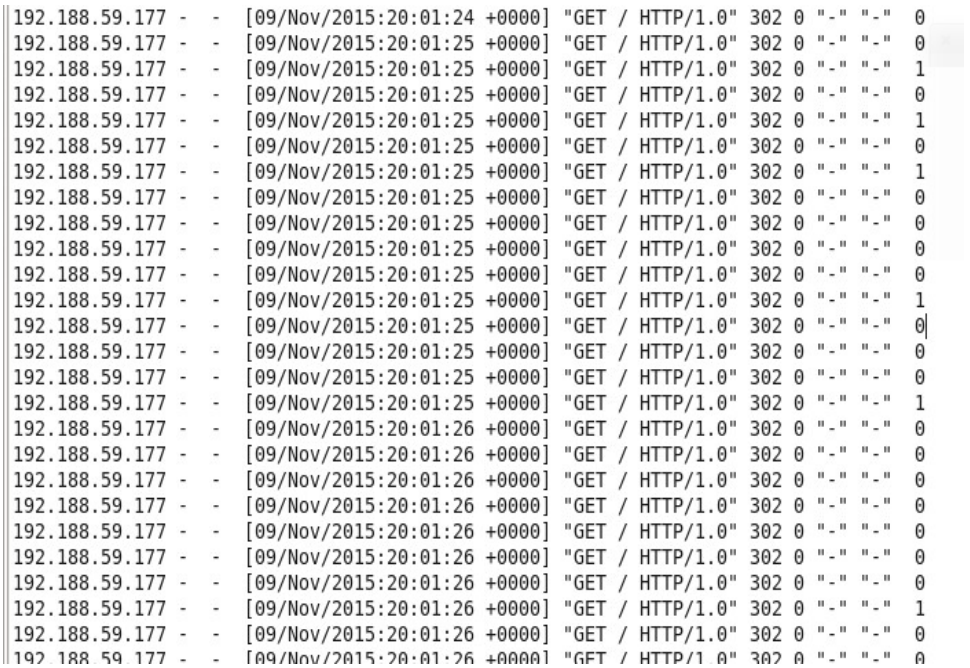


Figura 5.45 Detalle de la anomalía que la herramienta Andrisoft detectó durante el ataque de HTTP GET.
Fuente: Autoría propia

Este comportamiento se pudo ver el log del servicio web, en el cual se listan una serie de peticiones hacia el servidor como se muestra a continuación en la Figura 5.46.



```
192.188.59.177 -  -  [09/Nov/2015:20:01:24 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  1
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  1
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  1
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  1
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:25 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  1
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  1
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
192.188.59.177 -  -  [09/Nov/2015:20:01:26 +0000] "GET / HTTP/1.0" 302 0 "-" "-"  0
```

Figura 5.46 Muestra del log del servidor durante el ataque de HTTP GET.
Fuente: Autoría propia

Durante el ataque, se realizó una captura de paquetes desde la herramienta Andriosoft como muestra de la anomalía. Aquí notamos que el puerto objetivo es el 80 TCP correspondiente al protocolo HTTP, la IP pública que genera el ataque es la 192.188.59.177. Las

solicitudes capturadas son del tipo GET HTTP, y por cada solicitud hay una respuesta válida de ACK.

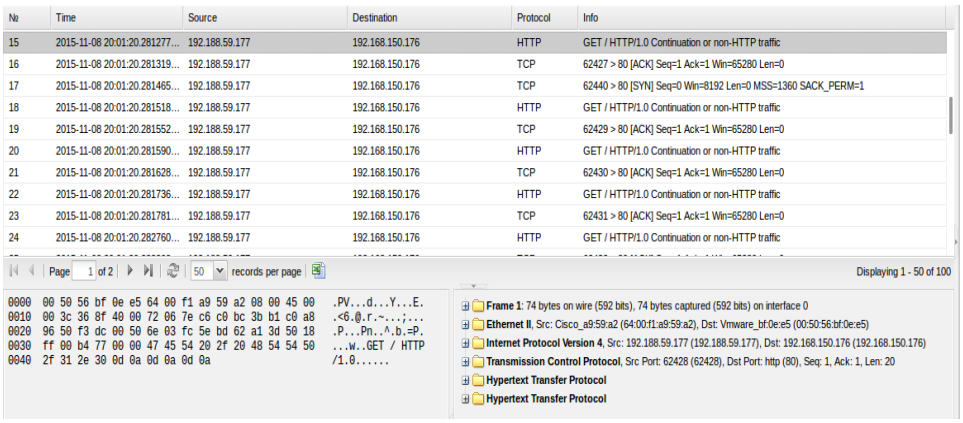


Figura 5.47 Detalle de uno de los paquetes capturados durante la detección de la anomalía.
Fuente: Autoría propia

Mientras el ataque se ejecutaba se procedió a hacer la prueba de acceso a la página web empresarial de la cual no se accedió sin novedades, como se puede evidenciar en la siguiente captura de pantalla:

Figura 5.48 Evidencia de la disponibilidad de la página web empresarial de pruebas durante el ataque TCP+SYN Flood
Fuente: Autoría propia

En la Tabla 16 se mostrarán los datos obtenidos del ataque realizado para cada una de las mediciones consideradas:

Tabla 16 Datos obtenidos del ataque de inundación de peticiones HTTP mediante el método de envío de parámetros por dirección web (HTTP GET Flood) para el Servidor Web, conforme al Plan de Pruebas para ataques DDOS sobre la red empresarial.

Plan de pruebas para ataques de DDOS sobre la red empresarial			
Actividad/Ataque	**Ejecutado / Fallido**	**Datos Obtenidos**	**Comentarios**
Ejecución de pruebas de rendimiento con ataques			
- Ejecución controlada de ataques de DDOS a un servidor web	Ejecutado	--	--
- Ataque de inundación de	-	- Total Pkts: 98.1 k detectados	--

peticiones HTTP mediante el método de envío de parámetros por dirección web (HTTP GET Flood)		- Duración 15s - 4 anomalías detectadas del tipo HTTP	
- Efectividad	Ejecutado	Se detecta una anomalía No.269 mostrada en la Figura 5.45	--
- Precisión	Ejecutado	Se identifica la anomalía del tipo HTTP pkts/s > 2.0 k	--
- Robustez	Ejecutado	Acciones en respuesta de la anomalía: - 4 Acciones detectadas dentro de la anomalía. - Envío de alerta de email por presencia de anomalía. - Activación de reglas de filtrado y notificación de las mismas. - 1 Captura de muestra de tráfico. - Envío de Email finalizada las reglas de Filtrado. - Envío de Email por Anomalía Finalizada	--
- Rendimiento - Número máximo de conexiones soportadas - Ancho de banda - Throughput - Tiempos de respuesta	Ejecutado	- 3 Conexiones identificadas. - Ancho de banda usado 3.9 Mbits/s - Throughput usado 7.8 k pkts/s - Tiempo de respuesta <5sec	--
- Estabilidad	Ejecutado	Servicio de la página web disponible.	La prueba se realizó accediendo a la página web. Ver Figura 5.48.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 Análisis de Pruebas

Las pruebas realizadas se basaron en el Plan de pruebas para ataques de DDOS sobre la red empresarial en un ambiente controlado, con y sin ataques DDOS, correspondiente al punto 4.6 Diseño del Plan de Pruebas del presente trabajo de Titulación.

Los cuatro casos de ataques planteados para los dos servicios más importantes de la Empresa de Servicios, Correo Electrónico y Página Web empresarial, fueron realizados en un ambiente controlado sin afectar los equipos en producción de la empresa.

En la herramienta Andrisoft se definieron umbrales de ataques, que fueron establecidos de acuerdo al análisis del tráfico normal de la empresa durante un mes y a la capacidad de ancho de banda actual de 4 Mbps.

6.2 Análisis de Resultados

Los resultados obtenidos en cada una de las pruebas ejecutadas fueron los esperados, dado que se configuraron los umbrales de aceptación de tráfico ajustándonos a los recursos actuales de la empresa.

A continuación, se detallarán los valores calculados para cada ataque y se determinará el fundamento para el comportamiento de la herramienta.

6.2.1 Ataque TCP SYN Flood realizado al servidor de correo electrónico

El ataque TCP SYN Flood realizado al servidor de correo electrónico, ejecutado mediante el comando hping3 desde equipos externos a la red empresarial, generó un total de 42.6K paquetes

(pkts) y un total de 13.6M bits transmitidos en un periodo de 1 minuto con 21 segundos.

El umbral definido en Andrisoft fue de 500 paquetes por segundo (pkts/s), por lo que todo tráfico superior a esta configuración será descartado.

Cada paquete enviado tuvo un peso de 60 bytes (480 bits). De acuerdo a los valores capturados por la herramienta Anti DDOS se recibieron aproximadamente 900 paquetes por segundo (pkts/s) activando así las reglas de Anti DDOS en el equipo Andrisoft.

6.2.2 Ataque SPAM realizado al servidor de correo electrónico

El ataque SPAM realizado al servidor de correo electrónico, ejecutado con la herramienta MESS BOMBER desde 2 equipos externos a la red empresarial, realizó un envío de hasta 1000 correos electrónicos por cada ejecución con un intervalo de 60 a 65 correos por segundo.

El umbral definido en Andrisoft fue de 4M bits por segundo (bits/s), por lo que un tráfico superior a este será descartado, permitiendo

únicamente el ingreso de tráfico legítimo dentro del rango de los 4M bits por segundo (bits/s).

Cada correo electrónico enviado tuvo un peso aproximado de 27KB lo que equivale a 0.221184M bits por segundo (bits/s) de transmisión.

De acuerdo a los valores capturados por Andrisoft, se tuvo un total de 26.3M bits por segundo (bits/s) recibidos equivalentes a aproximadamente 118 correos electrónicos recibidos por segundo (26.3M bits/s / 0.221184M bits/s = 118 correos).

La configuración del umbral permitido en Andrisoft tomando en consideración el tamaño de correo enviado, equivale a un total de 18 correos permitidos por segundo (4M bits/s 0.221184M bits/s = 18 correos), por el tiempo de 16 segundos que duró el ataque dan un total aproximado de 288 correos (18 correos por segundo * 16 segundos = 288 correos) recibidos por el usuario catalogados como SPAM, de los cuales se reflejan 279 recibidos en su bandeja de correos no deseados.

Cabe indicar que los correos que provienen de una sola fuente origen con archivos adjuntos no son afectados, ya que llegan a su destino como paquetes fragmentados, los cuales no superan los 4M bits por segundo (bits/s).

El límite configurado en el servidor de correos para recepción de archivos es de 5MB, mientras que para el envío es de 7MB, tanto para correos internos como externos.

6.2.3 Ataque TCP SYN Flood realizado al servidor web

El ataque TCP SYN Flood realizado al servidor web, fue ejecutado por la herramienta Wbox generó un total de tráfico de 43.9K paquetes (pkts) y un total de 39.4M bits (bits).

El umbral definido en Andrisoft fue de 1K paquetes por segundo (pkts/s), debido a que su página web es estática y el promedio normal de interacciones con la misma no supera el umbral configurado.

Conforme a los datos capturados por la herramienta, se tiene un tráfico de 1.2K bits por segundo (bits/s) activando las reglas Anti DDOS definidas y eliminando el tráfico excedente.

6.2.4 Ataque HTTP GET Flood realizado al servidor web

El ataque HTTP GET Flood generados por la herramienta LOIC hacia el servidor web, generó un tráfico total de 98.1K paquetes (pkts) y un total de 49.6M bits durante un periodo de 15 segundos.

El umbral definido en Andrisoft fue de 2K bits por segundo (bits/s) por lo que todo tráfico superior a éste será descartado conforme al análisis que realiza la herramienta.

De acuerdo a los datos capturados por la herramienta, el valor recibido por segundo fue de 7.8K bits, activando las reglas Anti DDOS.

6.3 Falsos Positivos

Luego de la implementación y configuración de la herramienta WanGuard de Andrisoft se definieron los umbrales para cada uno de los protocolos a analizar, entre ellos de TCP, HTTP, SMTP, así como también se configuraron acciones cuando existe un volumen de tráfico que alcanza el máximo que el proveedor ofrece a la empresa. Debido al servicio que ambos servidores ofrecen, tienen permitido el acceso web a través del puerto 80. Los ataques se han efectuado desde el internet o red local hacia el servidor destino. Sin embargo, se ha presentado una alerta cuando el servidor web o de correo electrónico inicia su proceso de actualización de sistema operativo, pues realizan una descarga de contenido desde el internet.

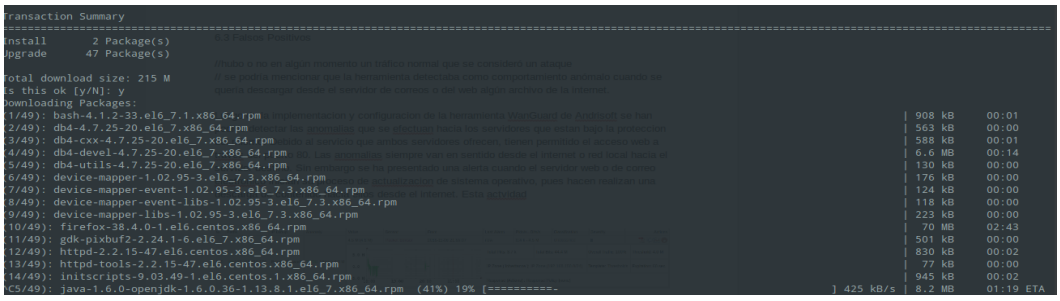


Figura 6.49 Proceso de actualización del servidor Linux donde se ejecuta el servicio de página web.
Fuente: Autoría propia

Esta actividad fue detectada por la herramienta Andrisoft como un ataque del tipo volumétrico dirigido al servidor. Sin embargo, conocemos que es una actividad normal que se ejecuta.

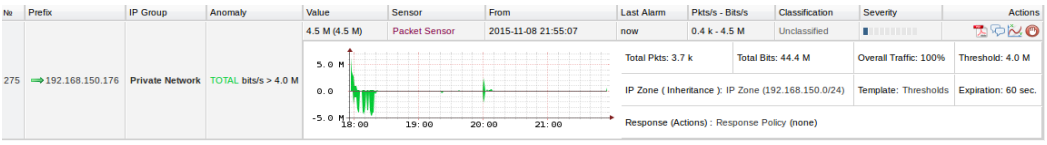


Figura 6.50 Detalle de una alerta por falso positivo generada por el servidor web
Fuente: Autoría propia

La alerta mostrada en la Figura 6.50 indica la presencia de un ataque que supera los 4M bits por segundo (bits/s) que se definieron como umbral para la empresa. Este comportamiento puede ser interrumpido por la herramienta, sin embargo, lo que se ha definido una lista blanca para todos los sitios de los cuales se confía su paso de datos. Esta lista blanca debe ser habilitada con contenido temporal ya que no se espera que siempre sea confiable la dirección autorizada.

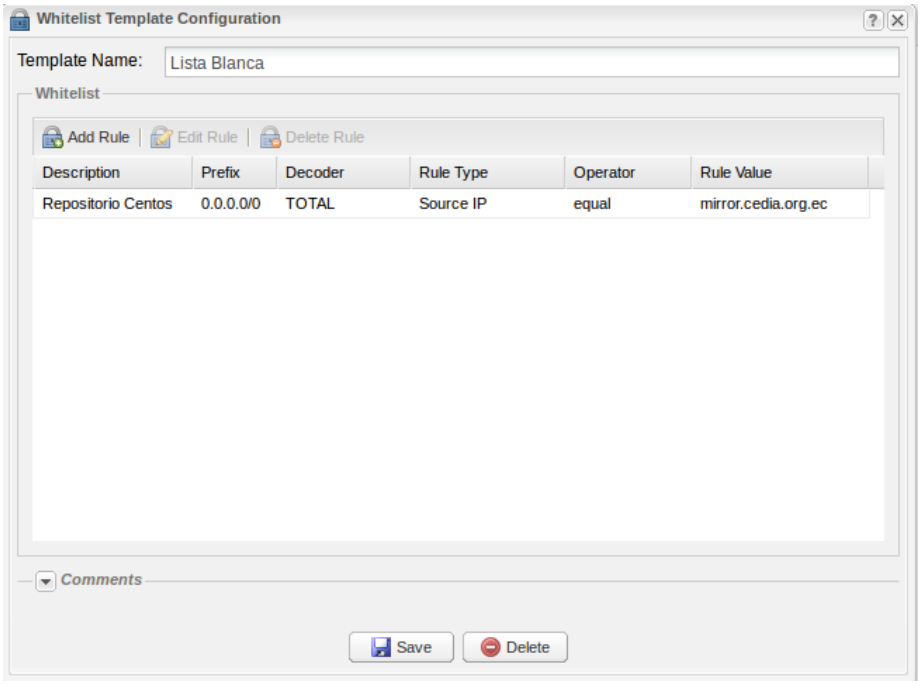


Figura 6.51 Muestra de las direcciones que se deben agregar como conocidas para una actividad específica del servidor
Fuente: Autoría propia

Para el caso, Figura 6.51, de las actualizaciones de los sistemas operativos se ha configurado el repositorio de CentOS, en este caso mirror.cedia.org.ec, para permitir el paso de todo el tráfico sin que sea limitado o bloqueado.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Durante el desarrollo del presente trabajo se logró evidenciar que la empresa estuvo bajo ataques de DDOS, que, a pesar de no ser de gran volumen en comparación a los ataques dirigidos a grandes instituciones en el área de Banca o Gobierno, fueron provocadas por personas que generan situaciones que llegan a desestabilizar la operatividad normal de la empresa.

Por lo tanto, podemos concluir lo siguiente:

1. La empresa de Servicios se encuentra protegida ante cualquier eventualidad del tipo DDOS tanto en su servidor de correo electrónico y el

servicio web, de esta manera los usuarios y clientes podrán operar de forma normal sin interrupciones a partir de esta implementación.

2. Se estableció la base teórica que sirvió de guía para la implementación de la solución AntiDDoS, con la cual se entendió el negocio y la situación de la Empresa de Servicios.

3. Se diseñó una solución anti DDOS ajustada a la realidad actual de la empresa, que se integra a las soluciones de seguridad con las que ya contaba y de esta forma las complementa con políticas de seguridad que permiten una mejor gestión en el manejo de seguridades perimetrales.

4. Se implementó la solución anti DDOS llamada Andrisoft, la cual es sencilla de implementar e intuitiva de administrar para el usuario, haciendo el enfoque en la escalabilidad modular de la herramienta en caso de crecimiento de la empresa.

5. Se tiene una mejor visibilidad de lo que sucede en la red a través del avanzado sensor que incluye la herramienta Andrisoft, permitiendo así poder efectuar acciones frente a un comportamiento que no es adecuado para los servicios de la empresa.

6. La empresa de servicios debe mantenerse con la actual implementación de la herramienta Andrisoft, ya que el tráfico actual se encuentra en niveles bajos los cuales son soportados por la herramienta, sin embargo, debe considerar modificar los umbrales al incrementar el ancho de banda.

7. Se garantiza una alta disponibilidad de los servicios de la empresa durante la presencia de un ataque, esto es la ventaja de disponer una protección antiDDoS.

8. La protección de la empresa no se encuentra limitada estrictamente a las pruebas que se han realizado, sino que la herramienta está configurada para actuar ante a cualquier otra eventualidad destinada a limitar el servicio de correo electrónico y página web.

RECOMENDACIONES

Como resultado del trabajo realizado, podemos mencionar las siguientes recomendaciones, que pueden ser aplicadas a corto o largo plazo, conforme a las necesidades y prioridades de la empresa de Servicios:

1. Establecer de manera formal e institucional las políticas recomendadas en el presente trabajo de titulación para su cumplimiento a nivel empresarial.

2. Realizar mantenimientos constantes a las configuraciones realizadas en la solución Anti DDOS, conforme al crecimiento en la infraestructura de comunicaciones de la empresa.

3. Establecer un plan de respuesta a incidentes conforme a las recomendaciones dadas en el presente trabajo y mantenerlo actualizado conforme a las necesidades de la empresa.

4. Preparar a un grupo selecto de personal para el manejo de incidentes informáticos.

5. Mantener capacitado al personal de la empresa en temas de seguridad, y mantener una cultura organizacional apoyada en la Seguridad de la Información.

6. Adoptar medidas preventivas para cualquier tipo de eventualidad informática de manera que se pueda minimizar el impacto en los servicios de la empresa.

7. Hacer partícipe de la seguridad de la información a todas las áreas de la empresa, trabajando en conjunto con Recursos Humanos.

8. Incluir un segundo proveedor de servicio de internet, especialmente que incluya dentro de sus servicios la protección de segundo nivel ante ataques dirigidos hacia los servicios de la empresa.

9. Establecer puntos de recuperación basado en copias de seguridad de la información de la empresa de manera periódica para sus servicios críticos, así protege su información ante cualquier ataque dirigido a afectar la información.

10. Monitorear constantemente los recursos usados por el dispositivo tanto en memoria, CPU y capacidad de almacenamiento, con la finalidad de tomar

los correctivos necesarios en caso de escases de recursos y de esta manera asegurar la disponibilidad de la protección Anti DDOS.

11. Actualizar constantemente la herramienta Anti DDOS a su última versión de software disponible y estable con los parches de seguridad adecuados, con la finalidad de minimizar los fallos de seguridad que permitan que el equipo este expuesto a diversos ataques que pongan en riesgo su disponibilidad.

12. Renovar el licenciamiento de la herramienta conforme al tiempo establecido en los contratos, para evitar que deje de funcionar y se pierda la protección Anti DDOS.

13. Proveer de redundancia de alimentación energética al equipo Anti DDOS, para de esta forma mantener la disponibilidad del servicio y evitar daños en el equipo ante los cortes de energía.

BIBLIOGRAFÍA

[1]. CERT (Coordination Center in response to the Morris worm incident), Division of the Software Engineering Institute (SEI). (1997), http://www.cert.org/historical/tech_tips/denial_of_service.cfm, fecha de consulta noviembre 2015.

[2]. Open Rights Group, Police and Justice Act 2006, https://wiki.openrightsgroup.org/wiki/Police_and_Justice_Act_2006, fecha de consulta noviembre 2015.

[3]. Department of Justice, Criminal CCIPS, http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf, fecha de consulta noviembre 2015.

[4]. CERT, Division of the Software Engineering Institute (SEI). (1997), http://www.cert.org/historical/advisories/CA-1999-17.cfm, fecha de consulta noviembre 2015.

[5]. CERT, National Vulnerability Database 2013, http://web.nvd.nist.gov/view/vuln/search?execution=e2s1, fecha de consulta noviembre 2015.

[6]. SEYMOUR BOSWORTH; M.E. KABAY. “Computer Security Handbook”, 6th Edition, JOHN WILEY & SONS, INC. 2014.

[7]. Lawrence C. Miller. “DDOS for Dummies”. New Jersey: John Wiley & Sons, Inc., 2012.

[8]. Radware, “DDOS Survival Handbook”, Radware, 2013.

[9]. SEYMOUR BOSWORTH; M.E. KABAY. “Computer Security Handbook”, 6th Edition. JOHN WILEY & SONS, INC. 2014.

[10]. EC-Council, “Ethical Hacking & Countermeasures Threats & Defense Mechanisms”, EC-Council, 2010.

[11]. Wikipedia, Character Generator Protocol, https://en.wikipedia.org/wiki/Character_Generator_Protocol, fecha de consulta noviembre 2015.

[12]. Hackforums, http://hackforums.net/showthread.php?tid=49441, fecha de consulta noviembre 2015.

[13]. Hackforums, http://hackforums.net, fecha de consulta noviembre 2015.

[14]. Email Marketing, A List of Common Spam Words, http://emailmarketing.comm100.com/email-marketing-ebook/spam-words.aspx, fecha de consulta noviembre 2015.

[15] Wbox, HTTP testing tool, http://www.hping.org/wbox/, fecha de consulta noviembre 2015.

[16]. National Institute of Standards and Technology (NIST), Guidelines on Firewalls and Firewall Policy:
Recommendations of NIST Special Publication 800-41 Revision 1 2009, http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf, fecha de consulta noviembre 2015.

[17]. Google Books, MF0488_3: Gestion de incidents de Seguridad Informatica, 2014, https://books.google.com.ec/books?id=y63KCQAAQBAJ&pg=PT58&lpg=PT58&dq=politicas+ids+ips&source=bl&ots=zmCyr6I9hQ&sig=QQ07qqNQyHDqKsLWOzxB7vkHvls&hl=en&sa=X&redir_esc=y#v=onepage&q&f=false, fecha de consulta noviembre 2015.

[18]. Secur-IT @C.R.S, Intrusion Prevention System, https://securitcrs.wordpress.com/knowledge-base/ips-intrusion-prevention-system/, fecha de consulta noviembre 2015.

[19]. Gestión de Riesgo en la Seguridad Informática, Matriz de Riesgo, https://protejete.wordpress.com/gdr_principal/matriz_riesgo/, fecha de consulta noviembre 2015.

[20]. Interempresas.Net, Feria Virtual, https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/219836/Testing-Inteligente-de-infraestructuras-de-Seguridad1.pdf, fecha de consulta noviembre 2015.

ANEXOS

ANEXO 1

Formularios Matriz Análisis de Riesgo.

Matriz de Análisis de Riesgos: Datos e Información.

- Promedio de datos colectados.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Clasificación: Obligación por ley / Contrato / Convenio	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Finanzas	x	x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicios bancarios		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
RR.HH	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Directorio de Contactos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Correo electrónico	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos internos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos externos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos colaborativos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web interna (Intranet)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web externa			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Respaldos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Infraestructura (Planes, Documentación, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Informática (Planes, Documentación, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Base de datos de Contraseñas	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Datos e información no institucionales	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Navegación en Internet			x	3	3	3	3	6	3	3	3	3	12	12	12	12	12
Chat interno	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat externo			x	3	3	3	3	6	3	3	3	3	12	12	12	12	12
Llamadas telefónicas internas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Llamadas telefónicas externas			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16

Sucesos de origen físico o natural

Datos e Información	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	6	3	6	3	3	9	9	6	6
Finanzas	8	4	8	4	4	12	12	8	8
Servicios bancarios	4	2	4	2	2	6	6	4	4
RR.HH	2	1	2	1	1	3	3	2	2
Directorio de Contactos	8	4	8	4	4	12	12	8	8
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	6	3	6	3	3	9	9	6	6
Correo electrónico	8	4	8	4	4	12	12	8	8
Bases de datos internos	8	4	8	4	4	12	12	8	8
Bases de datos externos	8	4	8	4	4	12	12	8	8
Bases de datos colaborativos	2	1	2	1	1	3	3	2	2
Página Web interna (Intranet)	2	1	2	1	1	3	3	2	2
Página Web externa	8	4	8	4	4	12	12	8	8
Respaldos	4	2	4	2	2	6	6	4	4
Infraestructura (Planes, Documentación, etc.)	4	2	4	2	2	6	6	4	4
Informática (Planes, Documentación, etc.)	4	2	4	2	2	6	6	4	4
Base de datos de Contraseñas	4	2	4	2	2	6	6	4	4
Datos e información no institucionales	2	1	2	1	1	3	3	2	2
Navegación en Internet	6	3	6	3	3	9	9	6	6
Chat interno	2	1	2	1	1	3	3	2	2
Chat externo	6	3	6	3	3	9	9	6	6
Llamadas telefónicas internas	2	1	2	1	1	3	3	2	2
Llamadas telefónicas externas	8	4	8	4	4	12	12	8	8

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Datos e Información	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Finanzas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicios bancarios	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
RR.HH	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Directorio de Contactos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Correo electrónico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos internos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos externos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos colaborativos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web interna (Intranet)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web externa	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Respaldos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Infraestructura (Planes, Documentación, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Informática (Planes, Documentación, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Base de datos de Contraseñas	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Datos e información no institucionales	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Navegación en Internet	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Chat interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat externo	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Llamadas telefónicas internas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Llamadas telefónicas externas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16

- Usuario Administrativo.

Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Clasificación: Obligación por ley / Contrato / Convenio	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Finanzas	x	x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicios bancarios		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
RR.HH	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Directorio de Contactos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Correo electrónico	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos internos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos externos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos colaborativos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web interna (Intranet)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web externa			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Respaldos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Infraestructura (Planes, Documentación, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Informática (Planes, Documentación, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Base de datos de Contraseñas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Datos e información no institucionales	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Navegación en Internet			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Chat interno	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat externo			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Llamadas telefónicas internas	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Llamadas telefónicas externas			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16

Sucesos de origen físico o natural

Datos e Información	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	6	3	6	3	3	9	9	6	6
Finanzas	8	4	8	4	4	12	12	8	8
Servicios bancarios	8	4	8	4	4	12	12	8	8
RR.HH	6	3	6	3	3	9	9	6	6
Directorio de Contactos	8	4	8	4	4	12	12	8	8
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	4	2	4	2	2	6	6	4	4
Correo electrónico	8	4	8	4	4	12	12	8	8
Bases de datos internos	8	4	8	4	4	12	12	8	8
Bases de datos externos	8	4	8	4	4	12	12	8	8
Bases de datos colaborativos	2	1	2	1	1	3	3	2	2
Página Web interna (Intranet)	2	1	2	1	1	3	3	2	2
Página Web externa	8	4	8	4	4	12	12	8	8
Respaldos	2	1	2	1	1	3	3	2	2
Infraestructura (Planes, Documentación, etc.)	4	2	4	2	2	6	6	4	4
Informática (Planes, Documentación, etc.)	4	2	4	2	2	6	6	4	4
Base de datos de Contraseñas	2	1	2	1	1	3	3	2	2
Datos e información no institucionales	4	2	4	2	2	6	6	4	4
Navegación en Internet	8	4	8	4	4	12	12	8	8
Chat interno	2	1	2	1	1	3	3	2	2
Chat externo	8	4	8	4	4	12	12	8	8
Llamadas telefónicas internas	4	2	4	2	2	6	6	4	4
Llamadas telefónicas externas	8	4	8	4	4	12	12	8	8

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Datos e Información	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Finanzas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicios bancarios	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
RR.HH	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Directorio de Contactos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Correo electrónico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos internos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos externos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos colaborativos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web interna (Intranet)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web externa	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Respaldos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Infraestructura (Planes, Documentación, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Informática (Planes, Documentación, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Base de datos de Contraseñas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Datos e información no institucionales	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Navegación en Internet	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Chat interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Llamadas telefónicas internas	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Llamadas telefónicas externas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16

- Usuario Técnico

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Finanzas	x	x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicios bancarios		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
RR.HH	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Directorio de Contactos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Correo electrónico	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos internos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos externos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos colaborativos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web interna (Intranet)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web externa			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Respaldos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Infraestructura (Planes, Documentación, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática (Planes, Documentación, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Base de datos de Contraseñas	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Datos e información no institucionales	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Navegación en Internet			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat interno	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat externo			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Llamadas telefónicas internas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Llamadas telefónicas externas			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16

Sucesos de origen físico o natural

Datos e Información	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	8	4	8	4	4	12	12	8	8
Finanzas	8	4	8	4	4	12	12	8	8
Servicios bancarios	2	1	2	1	1	3	3	2	2
RR.HH	2	1	2	1	1	3	3	2	2
Directorio de Contactos	8	4	8	4	4	12	12	8	8
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	6	3	6	3	3	9	9	6	6
Correo electrónico	8	4	8	4	4	12	12	8	8
Bases de datos internos	8	4	8	4	4	12	12	8	8
Bases de datos externos	8	4	8	4	4	12	12	8	8
Bases de datos colaborativos	2	1	2	1	1	3	3	2	2
Página Web interna (Intranet)	2	1	2	1	1	3	3	2	2
Página Web externa	8	4	8	4	4	12	12	8	8
Respaldos	8	4	8	4	4	12	12	8	8
Infraestructura (Planes, Documentación, etc.)	2	1	2	1	1	3	3	2	2
Informática (Planes, Documentación, etc.)	2	1	2	1	1	3	3	2	2
Base de datos de Contraseñas	8	4	8	4	4	12	12	8	8
Datos e información no institucionales	2	1	2	1	1	3	3	2	2
Navegación en Internet	2	1	2	1	1	3	3	2	2
Chat interno	2	1	2	1	1	3	3	2	2
Chat externo	8	4	8	4	4	12	12	8	8
Llamadas telefónicas internas	2	1	2	1	1	3	3	2	2
Llamadas telefónicas externas	8	4	8	4	4	12	12	8	8

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Datos e Información	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Finanzas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicios bancarios	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
RR.HH	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Directorio de Contactos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Correo electrónico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos internos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos externos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos colaborativos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web interna (Intranet)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web externa	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Respaldos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Infraestructura (Planes, Documentación, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática (Planes, Documentación, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Base de datos de Contraseñas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Datos e información no institucionales	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Navegación en Internet	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Llamadas telefónicas internas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Llamadas telefónicas externas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16

- Usuario Técnico Oficina Remota.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Clasificación: Obligación por ley / Contrato / Convenio	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común, motivación política, Hackers: Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Finanzas	x	x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Servicios bancarios		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
RR.HH	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Directorio de Contactos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Correo electrónico	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos internos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos externos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos colaborativos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web interna (Intranet)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web externa			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Respaldos	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Infraestructura (Planes, Documentación, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Informática (Planes, Documentación, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Base de datos de Contraseñas	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Datos e información no institucionales	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Navegación en Internet			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Chat interno	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat externo			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Llamadas telefónicas internas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Llamadas telefónicas externas			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16

Datos e Información	Sucesos de origen físico o natural: Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	8	4	8	4	4	12	12	8	8
Finanzas	6	3	6	3	3	9	9	6	6
Servicios bancarios	4	2	4	2	2	6	6	4	4
RR.HH	2	1	2	1	1	3	3	2	2
Directorio de Contactos	8	4	8	4	4	12	12	8	8
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	6	3	6	3	3	9	9	6	6
Correo electrónico	8	4	8	4	4	12	12	8	8
Bases de datos internos	8	4	8	4	4	12	12	8	8
Bases de datos externos	8	4	8	4	4	12	12	8	8
Bases de datos colaborativos	2	1	2	1	1	3	3	2	2
Página Web interna (Intranet)	2	1	2	1	1	3	3	2	2
Página Web externa	8	4	8	4	4	12	12	8	8
Respaldos	6	3	6	3	3	9	9	6	6
Infraestructura (Planes, Documentación, etc.)	4	2	4	2	2	6	6	4	4
Informática (Planes, Documentación, etc.)	4	2	4	2	2	6	6	4	4
Base de datos de Contraseñas	8	4	8	4	4	12	12	8	8
Datos e información no institucionales	2	1	2	1	1	3	3	2	2
Navegación en Internet	8	4	8	4	4	12	12	8	8
Chat interno	2	1	2	1	1	3	3	2	2
Chat externo	8	4	8	4	4	12	12	8	8
Llamadas telefónicas internas	2	1	2	1	1	3	3	2	2
Llamadas telefónicas externas	8	4	8	4	4	12	12	8	8

Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales: Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Finanzas	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Servicios bancarios	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
RR.HH	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Directorio de Contactos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Correo electrónico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos internos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos externos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos colaborativos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web interna (Intranet)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web externa	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Respaldos	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Infraestructura (Planes, Documentación, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Informática (Planes, Documentación, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Base de datos de Contraseñas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Datos e información no institucionales	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Navegación en Internet	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Chat interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Llamadas telefónicas internas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Llamadas telefónicas externas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16

- Usuario Preventa.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Clasificación: Obligación por ley / Contrato / Convenio	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Finanzas	x	x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Servicios bancarios		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
RR.HH	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Directorio de Contactos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Correo electrónico	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos internos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos externos	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Bases de datos colaborativos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web interna (Intranet)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web externa			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Respaldos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Infraestructura (Planes, Documentación, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Informática (Planes, Documentación, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Base de datos de Contraseñas	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Datos e información no institucionales	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Navegación en Internet			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Chat interno	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat externo			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Llamadas telefónicas internas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Llamadas telefónicas externas			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16

Sucesos de origen físico o natural

Datos e Información	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	4	2	4	2	2	6	6	4	4
Finanzas	4	2	4	2	2	6	6	4	4
Servicios bancarios	4	2	4	2	2	6	6	4	4
RR.HH	2	1	2	1	1	3	3	2	2
Directorio de Contactos	8	4	8	4	4	12	12	8	8
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	8	4	8	4	4	12	12	8	8
Correo electrónico	8	4	8	4	4	12	12	8	8
Bases de datos internos	8	4	8	4	4	12	12	8	8
Bases de datos externos	6	3	6	3	3	9	9	6	6
Bases de datos colaborativos	2	1	2	1	1	3	3	2	2
Página Web interna (Intranet)	2	1	2	1	1	3	3	2	2
Página Web externa	8	4	8	4	4	12	12	8	8
Respaldos	8	4	8	4	4	12	12	8	8
Infraestructura (Planes, Documentación, etc.)	6	3	6	3	3	9	9	6	6
Informática (Planes, Documentación, etc.)	6	3	6	3	3	9	9	6	6
Base de datos de Contraseñas	8	4	8	4	4	12	12	8	8
Datos e información no institucionales	2	1	2	1	1	3	3	2	2
Navegación en Internet	8	4	8	4	4	12	12	8	8
Chat interno	2	1	2	1	1	3	3	2	2
Chat externo	8	4	8	4	4	12	12	8	8
Llamadas telefónicas internas	2	1	2	1	1	3	3	2	2
Llamadas telefónicas externas	8	4	8	4	4	12	12	8	8

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Datos e Información	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Finanzas	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Servicios bancarios	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
RR.HH	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Directorio de Contactos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Correo electrónico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos internos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos externos	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Bases de datos colaborativos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web interna (Intranet)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web externa	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Respaldos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Infraestructura (Planes, Documentación, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Informática (Planes, Documentación, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Base de datos de Contraseñas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Datos e información no institucionales	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Navegación en Internet	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Chat interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Llamadas telefónicas internas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Llamadas telefónicas externas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16

- Usuario de Ventas.

Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Clasificación: Obligación por ley / Contrato / Convenio	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Finanzas	x	x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicios bancarios		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
RR.HH	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Directorio de Contactos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Correo electrónico	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos internos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos externos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos colaborativos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web interna (Intranet)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web externa			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Respaldos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Infraestructura (Planes, Documentación, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática (Planes, Documentación, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Base de datos de Contraseñas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Datos e información no institucionales	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Navegación en Internet			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Chat interno	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat externo			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Llamadas telefónicas internas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Llamadas telefónicas externas			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16

Sucesos de origen físico o natural

Datos e Información	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	6	3	6	3	3	9	9	6	6
Finanzas	8	4	8	4	4	12	12	8	8
Servicios bancarios	6	3	6	3	3	9	9	6	6
RR.HH	2	1	2	1	1	3	3	2	2
Directorio de Contactos	8	4	8	4	4	12	12	8	8
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	8	4	8	4	4	12	12	8	8
Correo electrónico	8	4	8	4	4	12	12	8	8
Bases de datos internos	8	4	8	4	4	12	12	8	8
Bases de datos externos	8	4	8	4	4	12	12	8	8
Bases de datos colaborativos	2	1	2	1	1	3	3	2	2
Página Web interna (Intranet)	2	1	2	1	1	3	3	2	2
Página Web externa	8	4	8	4	4	12	12	8	8
Respaldos	2	1	2	1	1	3	3	2	2
Infraestructura (Planes, Documentación, etc.)	2	1	2	1	1	3	3	2	2
Informática (Planes, Documentación, etc.)	2	1	2	1	1	3	3	2	2
Base de datos de Contraseñas	2	1	2	1	1	3	3	2	2
Datos e información no institucionales	2	1	2	1	1	3	3	2	2
Navegación en Internet	8	4	8	4	4	12	12	8	8
Chat interno	2	1	2	1	1	3	3	2	2
Chat externo	8	4	8	4	4	12	12	8	8
Llamadas telefónicas internas	2	1	2	1	1	3	3	2	2
Llamadas telefónicas externas	8	4	8	4	4	12	12	8	8

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Datos e Información	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Finanzas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicios bancarios	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
RR.HH	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Directorio de Contactos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Correo electrónico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos internos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos externos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos colaborativos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web interna (Intranet)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web externa	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Respaldos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Infraestructura (Planes, Documentación, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática (Planes, Documentación, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Base de datos de Contraseñas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Datos e información no institucionales	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Navegación en Internet	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Chat interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Llamadas telefónicas internas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Llamadas telefónicas externas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16

- Usuario Subgerente preventa.

Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común, motivación política, Hackers												
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Finanzas	x	x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicios bancarios		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
RR.HH	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Directorio de Contactos	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Correo electrónico	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos internos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos externos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos colaborativos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web interna (Intranet)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Página Web externa			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Respaldos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Infraestructura (Planes, Documentación, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Informática (Planes, Documentación, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Base de datos de Contraseñas	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Datos e información no institucionales	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Navegación en Internet			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Chat interno	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat externo			x	3	3	3	3	6	3	3	3	3	12	12	12	12	12
Llamadas telefónicas internas	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Llamadas telefónicas externas			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16

Datos e Información	Sucesos de origen físico o natural								
	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	8	4	8	4	4	12	12	8	8
Finanzas	8	4	8	4	4	12	12	8	8
Servicios bancarios	4	2	4	2	2	6	6	4	4
RR.HH	2	1	2	1	1	3	3	2	2
Directorio de Contactos	6	3	6	3	3	9	9	6	6
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	2	1	2	1	1	3	3	2	2
Correo electrónico	8	4	8	4	4	12	12	8	8
Bases de datos internos	8	4	8	4	4	12	12	8	8
Bases de datos externos	8	4	8	4	4	12	12	8	8
Bases de datos colaborativos	2	1	2	1	1	3	3	2	2
Página Web interna (Intranet)	4	2	4	2	2	6	6	4	4
Página Web externa	8	4	8	4	4	12	12	8	8
Respaldos	2	1	2	1	1	3	3	2	2
Infraestructura (Planes, Documentación, etc.)	4	2	4	2	2	6	6	4	4
Informática (Planes, Documentación, etc.)	4	2	4	2	2	6	6	4	4
Base de datos de Contraseñas	4	2	4	2	2	6	6	4	4
Datos e información no institucionales	4	2	4	2	2	6	6	4	4
Navegación en Internet	8	4	8	4	4	12	12	8	8
Chat interno	2	1	2	1	1	3	3	2	2
Chat externo	6	3	6	3	3	9	9	6	6
Llamadas telefónicas internas	4	2	4	2	2	6	6	4	4
Llamadas telefónicas externas	8	4	8	4	4	12	12	8	8

Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																									
	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos criticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos criticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Finanzas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicios bancarios	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
RR.HH	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Directorio de Contactos	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Correo electrónico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos internos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos externos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos colaborativos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web interna (Intranet)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Página Web externa	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Respaldos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Infraestructura (Planes, Documentación, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Informática (Planes, Documentación, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Base de datos de Contraseñas	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Datos e información no institucionales	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Navegación en Internet	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Chat interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat externo	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Llamadas telefónicas internas	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Llamadas telefónicas externas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16

- Usuario Subgerente Técnico.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Clasificación: Obligación por ley / Contrato / Convenio	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Finanzas	x	x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicios bancarios		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
RR.HH	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Directorio de Contactos	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Correo electrónico	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos internos	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Bases de datos externos	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Bases de datos colaborativos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web interna (Intranet)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Página Web externa			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Respaldos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Infraestructura (Planes, Documentación, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática (Planes, Documentación, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Base de datos de Contraseñas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Datos e información no institucionales	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Navegación en Internet			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat interno	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Chat externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Llamadas telefónicas internas	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Llamadas telefónicas externas			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16

Sucesos de origen físico o natural

Datos e Información	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	8	4	8	4	4	12	12	8	8
Finanzas	8	4	8	4	4	12	12	8	8
Servicios bancarios	4	2	4	2	2	6	6	4	4
RR.HH	2	1	2	1	1	3	3	2	2
Directorio de Contactos	6	3	6	3	3	9	9	6	6
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	2	1	2	1	1	3	3	2	2
Correo electrónico	8	4	8	4	4	12	12	8	8
Bases de datos internos	8	4	8	4	4	12	12	8	8
Bases de datos externos	6	3	6	3	3	9	9	6	6
Bases de datos colaborativos	2	1	2	1	1	3	3	2	2
Página Web interna (Intranet)	2	1	2	1	1	3	3	2	2
Página Web externa	8	4	8	4	4	12	12	8	8
Respaldos	2	1	2	1	1	3	3	2	2
Infraestructura (Planes, Documentación, etc.)	2	1	2	1	1	3	3	2	2
Informática (Planes, Documentación, etc.)	2	1	2	1	1	3	3	2	2
Base de datos de Contraseñas	2	1	2	1	1	3	3	2	2
Datos e información no institucionales	2	1	2	1	1	3	3	2	2
Navegación en Internet	2	1	2	1	1	3	3	2	2
Chat interno	2	1	2	1	1	3	3	2	2
Chat externo	2	1	2	1	1	3	3	2	2
Llamadas telefónicas internas	2	1	2	1	1	3	3	2	2
Llamadas telefónicas externas	8	4	8	4	4	12	12	8	8

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Datos e Información	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Finanzas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicios bancarios	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
RR.HH	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Directorio de Contactos	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Correo electrónico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos internos	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Bases de datos externos	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Bases de datos colaborativos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web interna (Intranet)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Página Web externa	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Respaldos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Infraestructura (Planes, Documentación, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática (Planes, Documentación, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Base de datos de Contraseñas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Datos e información no institucionales	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Navegación en Internet	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Chat externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Llamadas telefónicas internas	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Llamadas telefónicas externas	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16

Matriz de Análisis de Riesgos: Sistemas e Infraestructura.

- Promedio de datos colectados.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Sistemas e Infraestructura	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común, motivación política, Hackers												
	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Cortafuego	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servidores	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Computadoras		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Programas de administración (contabilidad, manejo de personal, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de manejo de proyectos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de producción de datos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Impresoras		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Memorias portátiles	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
PBX (Sistema de telefonía convencional)		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Celulares	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Vehículos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sistemas e Infraestructura	Sucesos de origen físico o natural								
	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Equipos de la red cableada (router, switch, etc.)	8	4	8	4	4	12	12	8	8
Equipos de la red inalámbrica (router, punto de acceso, etc.)	6	3	6	3	3	9	9	6	6
Cortafuego	8	4	8	4	4	12	12	8	8
Servidores	8	4	8	4	4	12	12	8	8
Computadoras	6	3	6	3	3	9	9	6	6
Portátiles	8	4	8	4	4	12	12	8	8
Programas de administración (contabilidad, manejo de personal, etc.)	4	2	4	2	2	6	6	4	4
Programas de manejo de proyectos	4	2	4	2	2	6	6	4	4
Programas de producción de datos	4	2	4	2	2	6	6	4	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	8	4	4	12	12	8	8
Impresoras	4	2	4	2	2	6	6	4	4
Memorias portátiles	4	2	4	2	2	6	6	4	4
PBX (Sistema de telefonía convencional)	4	2	4	2	2	6	6	4	4
Celulares	4	2	4	2	2	6	6	4	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	6	3	6	3	3	9	9	6	6
Vehículos	2	1	2	1	1	3	3	2	2

Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																									
	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Equipos de la red cableada (router, switch, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Cortafuego	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servidores	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Computadoras	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Portátiles	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Programas de administración (contabilidad, manejo de personal, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de manejo de proyectos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de producción de datos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Impresoras	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Memorias portátiles	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
PBX (Sistema de telefonía convencional)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Celulares	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Vehículos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Administrativo.

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																																															
	Clasificación				Actos originados por la criminalidad común, motivación política, Hackers													Sucesos de origen físico o natural									Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																									
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
					1	1	1	2	1	1	1	1	4	4	4	4	4	2	1	2	1	1	3	3	2	2	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Equipos de la red cableada (router, switch, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12	6	3	6	3	3	9	9	6	6	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12	6	3	6	3	3	9	9	6	6	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Cortafuego	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servidores	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Computadoras		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Programas de administración (contabilidad, manejo de personal, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8	4	2	4	2	2	6	6	4	4	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de manejo de proyectos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8	4	2	4	2	2	6	6	4	4	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de producción de datos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8	4	2	4	2	2	6	6	4	4	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Impresoras		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Memorias portátiles	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8	4	2	4	2	2	6	6	4	4	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
PBX (Sistema de telefonía convencional)		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Celulares	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16	8	4	8	4	4	12	12	8	8	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Vehículos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4	2	1	2	1	1	3	3	2	2	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Técnico

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Sistemas e Infraestructura	Clasificación: Acceso exclusivo	Clasificación: Acceso ilimitado	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Cortafuego	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servidores	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Computadoras		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Programas de administración (contabilidad, manejo de personal, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de manejo de proyectos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de producción de datos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Impresoras		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Memorias portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
PBX (Sistema de telefonía convencional)		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Celulares	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Vehículos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Sistemas e Infraestructura	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Equipos de la red cableada (router, switch, etc.)	8	4	8	4	4	12	12	8	8
Equipos de la red inalámbrica (router, punto de acceso, etc.)	6	3	6	3	3	9	9	6	6
Cortafuego	8	4	8	4	4	12	12	8	8
Servidores	8	4	8	4	4	12	12	8	8
Computadoras	4	2	4	2	2	6	6	4	4
Portátiles	8	4	8	4	4	12	12	8	8
Programas de administración (contabilidad, manejo de personal, etc.)	4	2	4	2	2	6	6	4	4
Programas de manejo de proyectos	4	2	4	2	2	6	6	4	4
Programas de producción de datos	4	2	4	2	2	6	6	4	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	8	4	4	12	12	8	8
Impresoras	2	1	2	1	1	3	3	2	2
Memorias portátiles	8	4	8	4	4	12	12	8	8
PBX (Sistema de telefonía convencional)	2	1	2	1	1	3	3	2	2
Celulares	2	1	2	1	1	3	3	2	2
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	4	2	4	2	2	6	6	4	4
Vehículos	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Sistemas e Infraestructura	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Equipos de la red cableada (router, switch, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Cortafuego	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servidores	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Computadoras	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Portátiles	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Programas de administración (contabilidad, manejo de personal, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de manejo de proyectos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de producción de datos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Impresoras	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Memorias portátiles	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
PBX (Sistema de telefonía convencional)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Celulares	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Vehículos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Técnico Oficina Remota.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Sistemas e Infraestructura	Clasificación: Acceso exclusivo	Clasificación: Acceso ilimitado	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Cortafuego	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servidores	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Computadoras		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Programas de administración (contabilidad, manejo de personal, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de manejo de proyectos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de producción de datos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Impresoras		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Memorias portátiles	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
PBX (Sistema de telefonía convencional)		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Celulares	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Vehículos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Sistemas e Infraestructura	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Equipos de la red cableada (router, switch, etc.)	8	4	8	4	4	12	12	8	8
Equipos de la red inalámbrica (router, punto de acceso, etc.)	8	4	8	4	4	12	12	8	8
Cortafuego	8	4	8	4	4	12	12	8	8
Servidores	8	4	8	4	4	12	12	8	8
Computadoras	6	3	6	3	3	9	9	6	6
Portátiles	8	4	8	4	4	12	12	8	8
Programas de administración (contabilidad, manejo de personal, etc.)	4	2	4	2	2	6	6	4	4
Programas de manejo de proyectos	4	2	4	2	2	6	6	4	4
Programas de producción de datos	4	2	4	2	2	6	6	4	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	8	4	4	12	12	8	8
Impresoras	2	1	2	1	1	3	3	2	2
Memorias portátiles	4	2	4	2	2	6	6	4	4
PBX (Sistema de telefonía convencional)	2	1	2	1	1	3	3	2	2
Celulares	6	3	6	3	3	9	9	6	6
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	4	2	4	2	2	6	6	4	4
Vehículos	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Sistemas e Infraestructura	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Equipos de la red cableada (router, switch, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Cortafuego	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servidores	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Computadoras	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Portátiles	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Programas de administración (contabilidad, manejo de personal, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de manejo de proyectos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de producción de datos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Impresoras	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Memorias portátiles	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
PBX (Sistema de telefonía convencional)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Celulares	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Vehículos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Preventa.

Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Sistemas e Infraestructura	Clasificación: Acceso exclusivo	Clasificación: Acceso ilimitado	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Cortafuego	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servidores	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Computadoras		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Programas de administración (contabilidad, manejo de personal, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Programas de manejo de proyectos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Programas de producción de datos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Impresoras		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Memorias portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
PBX (Sistema de telefonía convencional)		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Celulares	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Vehículos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Sistemas e Infraestructura	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Equipos de la red cableada (router, switch, etc.)	8	4	8	4	4	12	12	8	8
Equipos de la red inalámbrica (router, punto de acceso, etc.)	8	4	8	4	4	12	12	8	8
Cortafuego	8	4	8	4	4	12	12	8	8
Servidores	8	4	8	4	4	12	12	8	8
Computadoras	8	4	8	4	4	12	12	8	8
Portátiles	8	4	8	4	4	12	12	8	8
Programas de administración (contabilidad, manejo de personal, etc.)	2	1	2	1	1	3	3	2	2
Programas de manejo de proyectos	2	1	2	1	1	3	3	2	2
Programas de producción de datos	2	1	2	1	1	3	3	2	2
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	8	4	4	12	12	8	8
Impresoras	2	1	2	1	1	3	3	2	2
Memorias portátiles	8	4	8	4	4	12	12	8	8
PBX (Sistema de telefonía convencional)	6	3	6	3	3	9	9	6	6
Celulares	6	3	6	3	3	9	9	6	6
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	4	2	4	2	2	6	6	4	4
Vehículos	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Sistemas e Infraestructura	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Equipos de la red cableada (router, switch, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Cortafuego	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servidores	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Computadoras	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Portátiles	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Programas de administración (contabilidad, manejo de personal, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Programas de manejo de proyectos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Programas de producción de datos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Impresoras	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Memorias portátiles	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
PBX (Sistema de telefonía convencional)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Celulares	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Vehículos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario de Ventas.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Sistemas e Infraestructura	Clasificación: Acceso exclusivo	Clasificación: Acceso ilimitado	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Cortafuego	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servidores	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Computadoras		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Programas de administración (contabilidad, manejo de personal, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Programas de manejo de proyectos	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Programas de producción de datos	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Impresoras		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Memorias portátiles	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
PBX (Sistema de telefonía convencional)		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Celulares	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Vehículos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Sistemas e Infraestructura	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Equipos de la red cableada (router, switch, etc.)	6	3	6	3	3	9	9	6	6
Equipos de la red inalámbrica (router, punto de acceso, etc.)	6	3	6	3	3	9	9	6	6
Cortafuego	8	4	8	4	4	12	12	8	8
Servidores	8	4	8	4	4	12	12	8	8
Computadoras	8	4	8	4	4	12	12	8	8
Portátiles	8	4	8	4	4	12	12	8	8
Programas de administración (contabilidad, manejo de personal, etc.)	6	3	6	3	3	9	9	6	6
Programas de manejo de proyectos	6	3	6	3	3	9	9	6	6
Programas de producción de datos	6	3	6	3	3	9	9	6	6
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	8	4	4	12	12	8	8
Impresoras	6	3	6	3	3	9	9	6	6
Memorias portátiles	2	1	2	1	1	3	3	2	2
PBX (Sistema de telefonía convencional)	4	2	4	2	2	6	6	4	4
Celulares	4	2	4	2	2	6	6	4	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	6	3	6	3	3	9	9	6	6
Vehículos	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Sistemas e Infraestructura	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Equipos de la red cableada (router, switch, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Equipos de la red inalámbrica (router, punto de acceso, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Cortafuego	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servidores	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Computadoras	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Portátiles	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Programas de administración (contabilidad, manejo de personal, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Programas de manejo de proyectos	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Programas de producción de datos	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Impresoras	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Memorias portátiles	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
PBX (Sistema de telefonía convencional)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Celulares	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Vehículos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Subgerente preventa.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Sistemas e Infraestructura	Clasificación: Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Cortafuego	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servidores	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Computadoras		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Portátiles	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Programas de administración (contabilidad, manejo de personal, etc.)	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de manejo de proyectos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de producción de datos	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Impresoras		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Memorias portátiles	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
PBX (Sistema de telefonía convencional)		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Celulares	x			2	2	2	2	4	2	2	2	2	8	8	8	8	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Vehículos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Sistemas e Infraestructura	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Equipos de la red cableada (router, switch, etc.)	6	3	6	3	3	9	9	6	6
Equipos de la red inalámbrica (router, punto de acceso, etc.)	6	3	6	3	3	9	9	6	6
Cortafuego	8	4	8	4	4	12	12	8	8
Servidores	8	4	8	4	4	12	12	8	8
Computadoras	6	3	6	3	3	9	9	6	6
Portátiles	6	3	6	3	3	9	9	6	6
Programas de administración (contabilidad, manejo de personal, etc.)	4	2	4	2	2	6	6	4	4
Programas de manejo de proyectos	4	2	4	2	2	6	6	4	4
Programas de producción de datos	4	2	4	2	2	6	6	4	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	6	3	6	3	3	9	9	6	6
Impresoras	2	1	2	1	1	3	3	2	2
Memorias portátiles	2	1	2	1	1	3	3	2	2
PBX (Sistema de telefonía convencional)	4	2	4	2	2	6	6	4	4
Celulares	4	2	4	2	2	6	6	4	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	8	4	8	4	4	12	12	8	8
Vehículos	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Sistemas e Infraestructura	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Equipos de la red cableada (router, switch, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Equipos de la red inalámbrica (router, punto de acceso, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Cortafuego	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servidores	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Computadoras	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Portátiles	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Programas de administración (contabilidad, manejo de personal, etc.)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de manejo de proyectos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de producción de datos	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Impresoras	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Memorias portátiles	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
PBX (Sistema de telefonía convencional)	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Celulares	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Vehículos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Subgerente Técnico.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Sistemas e Infraestructura	Clasificación: Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Cortafuego	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servidores	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Computadoras		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Portátiles	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Programas de administración (contabilidad, manejo de personal, etc.)	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Programas de manejo de proyectos	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Programas de producción de datos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Impresoras		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Memorias portátiles	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
PBX (Sistema de telefonía convencional)		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Celulares	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Vehículos	x			1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Sistemas e Infraestructura	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Equipos de la red cableada (router, switch, etc.)	8	4	8	4	4	12	12	8	8
Equipos de la red inalámbrica (router, punto de acceso, etc.)	2	1	2	1	1	3	3	2	2
Cortafuego	8	4	8	4	4	12	12	8	8
Servidores	8	4	8	4	4	12	12	8	8
Computadoras	8	4	8	4	4	12	12	8	8
Portátiles	8	4	8	4	4	12	12	8	8
Programas de administración (contabilidad, manejo de personal, etc.)	2	1	2	1	1	3	3	2	2
Programas de manejo de proyectos	6	3	6	3	3	9	9	6	6
Programas de producción de datos	2	1	2	1	1	3	3	2	2
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	8	4	4	12	12	8	8
Impresoras	2	1	2	1	1	3	3	2	2
Memorias portátiles	2	1	2	1	1	3	3	2	2
PBX (Sistema de telefonía convencional)	2	1	2	1	1	3	3	2	2
Celulares	2	1	2	1	1	3	3	2	2
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	8	4	8	4	4	12	12	8	8
Vehículos	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Sistemas e Infraestructura	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Equipos de la red cableada (router, switch, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Cortafuego	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servidores	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Computadoras	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Portátiles	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Programas de administración (contabilidad, manejo de personal, etc.)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Programas de manejo de proyectos	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Programas de producción de datos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Impresoras	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Memorias portátiles	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
PBX (Sistema de telefonía convencional)	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Celulares	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Vehículos	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

Matriz de Análisis de Riesgos: Personal Laboral.

- Promedio de datos colectados.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Junta Directiva	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Dirección / Coordinación	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Administración		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Personal técnico			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Recepción			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Piloto / conductor			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática / Soporte técnico interno			x	3	3	3	3	6	3	3	3	3	12	12	12	12	12
Soporte técnico externo		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicio de limpieza de planta		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Servicio de limpieza externo		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de propio			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Personal	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Junta Directiva	8	4	8	4	4	12	12	8	8
Dirección / Coordinación	6	3	6	3	3	9	9	6	6
Administración	6	3	6	3	3	9	9	6	6
Personal técnico	8	4	8	4	4	12	12	8	8
Recepción	2	1	2	1	1	3	3	2	2
Piloto / conductor	2	1	2	1	1	3	3	2	2
Informática / Soporte técnico interno	6	3	6	3	3	9	9	6	6
Soporte técnico externo	8	4	8	4	4	12	12	8	8
Servicio de limpieza de planta	4	2	4	2	2	6	6	4	4
Servicio de limpieza externo	2	1	2	1	1	3	3	2	2
Servicio de mensajería de propio	2	1	2	1	1	3	3	2	2
Servicio de mensajería de externo	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Personal	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Junta Directiva	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Dirección / Coordinación	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Administración	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Personal técnico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Recepción	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Piloto / conductor	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática / Soporte técnico interno	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Soporte técnico externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicio de limpieza de planta	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Servicio de limpieza externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de propio	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Administrativo.

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]												
Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común, motivación política, Hackers												
	Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Junta Directiva	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Dirección / Coordinación	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Administración		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Personal técnico			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Recepción			x	3	3	3	3	6	3	3	3	3	12	12	12	12	12
Piloto / conductor			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática / Soporte técnico interno			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Soporte técnico externo		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicio de limpieza de planta		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Servicio de limpieza externo		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de propio			x	3	3	3	3	6	3	3	3	3	12	12	12	12	12
Servicio de mensajería de externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4

Personal	Sucesos de origen físico o natural								
	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Junta Directiva	8	4	8	4	4	12	12	8	8
Dirección / Coordinación	8	4	8	4	4	12	12	8	8
Administración	8	4	8	4	4	12	12	8	8
Personal técnico	8	4	8	4	4	12	12	8	8
Recepción	6	3	6	3	3	9	9	6	6
Piloto / conductor	2	1	2	1	1	3	3	2	2
Informática / Soporte técnico interno	8	4	8	4	4	12	12	8	8
Soporte técnico externo	8	4	8	4	4	12	12	8	8
Servicio de limpieza de planta	6	3	6	3	3	9	9	6	6
Servicio de limpieza externo	2	1	2	1	1	3	3	2	2
Servicio de mensajería de propio	6	3	6	3	3	9	9	6	6
Servicio de mensajería de externo	2	1	2	1	1	3	3	2	2

Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																									
	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Junta Directiva	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Dirección / Coordinación	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Administración	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Personal técnico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Recepción	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Piloto / conductor	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática / Soporte técnico interno	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Soporte técnico externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicio de limpieza de planta	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Servicio de limpieza externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de propio	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Servicio de mensajería de externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Técnico

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Junta Directiva	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Dirección / Coordinación	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Administración		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Personal técnico			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Recepción			x	2	2	2	2	4	2	2	2	2	8	8	8	8	8
Piloto / conductor			x	2	2	2	2	4	2	2	2	2	8	8	8	8	8
Informática / Soporte técnico interno			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Soporte técnico externo		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Servicio de limpieza de planta		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de limpieza externo		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de propio			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Personal	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Junta Directiva	8	4	8	4	4	12	12	8	8
Dirección / Coordinación	6	3	6	3	3	9	9	6	6
Administración	6	3	6	3	3	9	9	6	6
Personal técnico	8	4	8	4	4	12	12	8	8
Recepción	4	2	4	2	2	6	6	4	4
Piloto / conductor	4	2	4	2	2	6	6	4	4
Informática / Soporte técnico interno	8	4	8	4	4	12	12	8	8
Soporte técnico externo	6	3	6	3	3	9	9	6	6
Servicio de limpieza de planta	2	1	2	1	1	3	3	2	2
Servicio de limpieza externo	2	1	2	1	1	3	3	2	2
Servicio de mensajería de propio	2	1	2	1	1	3	3	2	2
Servicio de mensajería de externo	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Personal	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Junta Directiva	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Dirección / Coordinación	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Administración	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Personal técnico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Recepción	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Piloto / conductor	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Informática / Soporte técnico interno	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Soporte técnico externo	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Servicio de limpieza de planta	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de limpieza externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de propio	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Técnico Oficina Remota.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común, motivación política, Hackers: Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Junta Directiva	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Dirección / Coordinación	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Administración		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Personal técnico			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Recepción			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Piloto / conductor			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática / Soporte técnico interno			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Soporte técnico externo		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicio de limpieza de planta		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de limpieza externo		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de propio			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4

Personal	Sucesos de origen físico o natural: Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Junta Directiva	8	4	8	4	4	12	12	8	8
Dirección / Coordinación	6	3	6	3	3	9	9	6	6
Administración	6	3	6	3	3	9	9	6	6
Personal técnico	8	4	8	4	4	12	12	8	8
Recepción	2	1	2	1	1	3	3	2	2
Piloto / conductor	2	1	2	1	1	3	3	2	2
Informática / Soporte técnico interno	8	4	8	4	4	12	12	8	8
Soporte técnico externo	8	4	8	4	4	12	12	8	8
Servicio de limpieza de planta	2	1	2	1	1	3	3	2	2
Servicio de limpieza externo	2	1	2	1	1	3	3	2	2
Servicio de mensajería de propio	2	1	2	1	1	3	3	2	2
Servicio de mensajería de externo	2	1	2	1	1	3	3	2	2

Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales: Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Junta Directiva	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Dirección / Coordinación	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Administración	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Personal técnico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Recepción	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Piloto / conductor	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática / Soporte técnico interno	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Soporte técnico externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicio de limpieza de planta	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de limpieza externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de propio	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Preventa.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Junta Directiva	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Dirección / Coordinación	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Administración		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Personal técnico			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Recepción			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Piloto / conductor			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática / Soporte técnico interno			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Soporte técnico externo		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicio de limpieza de planta		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de limpieza externo		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de propio			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	1	2	1	1	3	3	2	2
Junta Directiva	x			3	6	3	6	3	3	9	9	6	6
Dirección / Coordinación	x			3	6	3	6	3	3	9	9	6	6
Administración		x		2	4	2	4	2	2	6	6	4	4
Personal técnico			x	4	8	4	8	4	4	12	12	8	8
Recepción			x	1	2	1	2	1	1	3	3	2	2
Piloto / conductor			x	1	2	1	2	1	1	3	3	2	2
Informática / Soporte técnico interno			x	4	8	4	8	4	4	12	12	8	8
Soporte técnico externo		x		4	8	4	8	4	4	12	12	8	8
Servicio de limpieza de planta		x		1	2	1	2	1	1	3	3	2	2
Servicio de limpieza externo		x		1	2	1	2	1	1	3	3	2	2
Servicio de mensajería de propio			x	1	2	1	2	1	1	3	3	2	2
Servicio de mensajería de externo			x	1	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
					2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Junta Directiva	x			3	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Dirección / Coordinación	x			3	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Administración		x		2	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Personal técnico			x	4	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Recepción			x	1	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Piloto / conductor			x	1	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática / Soporte técnico interno			x	4	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Soporte técnico externo		x		4	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicio de limpieza de planta		x		1	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de limpieza externo		x		1	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de propio			x	1	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de externo			x	1	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario de Ventas.

Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común, motivación política, Hackers												
	Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Junta Directiva	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Dirección / Coordinación	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Administración		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Personal técnico			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Recepción			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Piloto / conductor			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática / Soporte técnico interno			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Soporte técnico externo		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicio de limpieza de planta		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Servicio de limpieza externo		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de propio			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4

Personal	Sucesos de origen físico o natural								
	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Junta Directiva	8	4	8	4	4	12	12	8	8
Dirección / Coordinación	8	4	8	4	4	12	12	8	8
Administración	8	4	8	4	4	12	12	8	8
Personal técnico	8	4	8	4	4	12	12	8	8
Recepción	2	1	2	1	1	3	3	2	2
Piloto / conductor	2	1	2	1	1	3	3	2	2
Informática / Soporte técnico interno	8	4	8	4	4	12	12	8	8
Soporte técnico externo	8	4	8	4	4	12	12	8	8
Servicio de limpieza de planta	4	2	4	2	2	6	6	4	4
Servicio de limpieza externo	2	1	2	1	1	3	3	2	2
Servicio de mensajería de propio	2	1	2	1	1	3	3	2	2
Servicio de mensajería de externo	2	1	2	1	1	3	3	2	2

Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																									
	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Junta Directiva	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Dirección / Coordinación	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Administración	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Personal técnico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Recepción	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Piloto / conductor	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática / Soporte técnico interno	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Soporte técnico externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicio de limpieza de planta	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Servicio de limpieza externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de propio	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Subgerente preventa.

Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Junta Directiva	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Dirección / Coordinación	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Administración		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Personal técnico			x	4	4	4	4	8	4	4	4	4	16	16	16	16	16
Recepción			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Piloto / conductor			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática / Soporte técnico interno			x	3	3	3	3	6	3	3	3	3	12	12	12	12	12
Soporte técnico externo		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicio de limpieza de planta		x		2	2	2	2	4	2	2	2	2	8	8	8	8	8
Servicio de limpieza externo		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de propio			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Personal	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Junta Directiva	8	4	8	4	4	12	12	8	8
Dirección / Coordinación	8	4	8	4	4	12	12	8	8
Administración	6	3	6	3	3	9	9	6	6
Personal técnico	8	4	8	4	4	12	12	8	8
Recepción	2	1	2	1	1	3	3	2	2
Piloto / conductor	2	1	2	1	1	3	3	2	2
Informática / Soporte técnico interno	6	3	6	3	3	9	9	6	6
Soporte técnico externo	8	4	8	4	4	12	12	8	8
Servicio de limpieza de planta	4	2	4	2	2	6	6	4	4
Servicio de limpieza externo	2	1	2	1	1	3	3	2	2
Servicio de mensajería de propio	2	1	2	1	1	3	3	2	2
Servicio de mensajería de externo	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Personal	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Junta Directiva	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Dirección / Coordinación	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Administración	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Personal técnico	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Recepción	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Piloto / conductor	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática / Soporte técnico interno	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Soporte técnico externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicio de limpieza de planta	4	2	6	2	4	6	6	8	8	8	8	6	2	2	6	2	4	4	4	2	2	2	8	8	6	8
Servicio de limpieza externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de propio	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

- Usuario Subgerente Técnico.

Matriz de Análisis de Riesgo — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común, motivación política, Hackers

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Virus / Ejecución no autorizado de programas	Ataques externos de Denegacion de Servicios Distribuidos	Ataques internos de Denegacion de Servicios Distribuidos
					1	1	1	2	1	1	1	1	4	4	4	4	4
Junta Directiva	x			4	4	4	4	8	4	4	4	4	16	16	16	16	16
Dirección / Coordinación	x			3	3	3	3	6	3	3	3	3	12	12	12	12	12
Administración		x		3	3	3	3	6	3	3	3	3	12	12	12	12	12
Personal técnico			x	3	3	3	3	6	3	3	3	3	12	12	12	12	12
Recepción			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Piloto / conductor			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Informática / Soporte técnico interno			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Soporte técnico externo		x		4	4	4	4	8	4	4	4	4	16	16	16	16	16
Servicio de limpieza de planta		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de limpieza externo		x		1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de propio			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4
Servicio de mensajería de externo			x	1	1	1	1	2	1	1	1	1	4	4	4	4	4

Sucesos de origen físico o natural

Personal	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	2	1	2	1	1	3	3	2	2
Junta Directiva	8	4	8	4	4	12	12	8	8
Dirección / Coordinación	6	3	6	3	3	9	9	6	6
Administración	6	3	6	3	3	9	9	6	6
Personal técnico	6	3	6	3	3	9	9	6	6
Recepción	2	1	2	1	1	3	3	2	2
Piloto / conductor	2	1	2	1	1	3	3	2	2
Informática / Soporte técnico interno	2	1	2	1	1	3	3	2	2
Soporte técnico externo	8	4	8	4	4	12	12	8	8
Servicio de limpieza de planta	2	1	2	1	1	3	3	2	2
Servicio de limpieza externo	2	1	2	1	1	3	3	2	2
Servicio de mensajería de propio	2	1	2	1	1	3	3	2	2
Servicio de mensajería de externo	2	1	2	1	1	3	3	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Personal	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Junta Directiva	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Dirección / Coordinación	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Administración	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Personal técnico	6	3	9	3	6	9	9	12	12	12	12	9	3	3	9	3	6	6	6	3	3	3	12	12	9	12
Recepción	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Piloto / conductor	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Informática / Soporte técnico interno	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Soporte técnico externo	8	4	12	4	8	12	12	16	16	16	16	12	4	4	12	4	8	8	8	4	4	4	16	16	12	16
Servicio de limpieza de planta	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de limpieza externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de propio	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4
Servicio de mensajería de externo	2	1	3	1	2	3	3	4	4	4	4	3	1	1	3	1	2	2	2	1	1	1	4	4	3	4

ANEXO 2

Direcciones IPv4 reservadas para redes privadas.

Rango de IP	Subred y Máscara	Número y clase de red
10.0.0.0-10.255.255.255	prefijo 10 /8	Clase A 1
172.16.0.0-172.31.255.255	prefijo 172.16 /12	Clase B 16
192.168.0.0-192.168.255.255	prefijo 192.168 /16	Clase C 256

ANEXO 3

Direcciones IPv4 que no se encuentran asignadas.

0.0.0.0 /32	Direcciones de difusión
127.0.0.0 /8	Identificador de red retroactivo
169.254.0.0 /16	Vínculo de redes locales
192.0.2.0 /24	Redes de pruebas
224.0.0.0 /4	Direcciones de multidifusión
240.0.0.0 /5	Rango reservado para uso futuro
255.255.255.255 /32	Difusión general

ANEXO 4

Matriz de pruebas para un ambiente con y sin ataques DDOS

Plan de pruebas para ataques de DDOS sobre la red empresarial			
Actividad/Ataque	**Ejecutado / Fallido**	**Datos Obtenidos**	**Comentarios**
Etapa 1			
Definir los Servicios a probar			
Definir rangos de IP			
Definir los tipos de ataques a realizar			
Definir las variables de rendimiento (Ancho de banda, aplicaciones, conexiones recurrentes, ataques recurrentes)			

Establecer tiempo de ejecución			
Rendimiento de equipos sin ataques			

• Equipo Anti DDOS
  ○ Memoria:
  ○ Procesador:			

• Sistema de Detección de Intrusos
  ○ Memoria:
  ○ Procesador:			

• Cortafuegos
  ○ Memoria:
  ○ Procesador:			

• Router
  ○ Memoria:
  ○ Procesador:			

Ejecución de pruebas de rendimiento con ataques			

Etapa 2			
Ejecución controlada de ataques de DDOS a un servidor de correo electrónico			
• Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood)			
• Ataque de envío masivo de correo electrónico no deseado (SPAM)			
Efectividad			
Precisión			

Robustez			
Rendimiento			
Estabilidad			
Etapa 3			
Ejecución controlada de ataques de DDOS a un servidor web			
• Ataque de envío masivo de solicitudes de conexión TCP (TCP SYN Flood)			
• Ataque de inundación de peticiones HTTP mediante el método de envío de parámetros			

por dirección web (HTTP GET Flood)			
Efectividad			
Precisión			
Robustez			
Rendimiento			
Estabilidad			
Fin de las pruebas			

ANEXO 5

Datos del consumo promedio de recursos de equipos de comunicación.

Los datos fueron obtenidos previamente a la implementación del equipo anti DDOS en la red.

Sistema de Detección de Intrusos

```
root@ids:~# top
top - 11:21:16 up 12 days,  12:04,  9 users,  load average: 0.99, 0.71, 0.43
Tasks: 269 total,   1 running, 268 sleeping,   0 stopped,   0 zombie
Cpu(s):  7.5%us,  1.7%sy,  0.0%ni, 90.7%id,  0.2%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   4053180k total,  121595k used,  3931585k free,    31696 buffers
Swap:  9999992k total,       68k used,  9999924k free,  2263740k cached
```

Uso de CPU: 7.5%
Uso de Memoria: 5%

Cortafuegos (Firewall)

```
root@firewall:~# top
top - 13:39:59 up 283 days, 12:24,  1 user,  load average: 0.28, 0.37, 0.34
Tasks: 318 total,   1 running, 317 sleeping,   0 stopped,   0 zombie
Cpu(s): 10.6%us,  2.0%sy,  0.0%ni, 86.3%id, 0.1%wa,  0.2%hi,  0.8%si,  0.0%st
Mem:   4053180k total,  121595k used,    3931585k free,   34684 buffers
Swap:  9936160k total,    12160k used,  9924000k free,  2290716k cached
```

Uso de CPU: 10%
Uso de Memoria: 3%

Router

Detalle de memoria

```
RV082#show memory free
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor   86616BC4   402560060   121297900   281262160   193558832   185498956
      I/O   1E600000    27262976     7911164    19351812    19258528    18983324
```

El valor de 121297900b representa el 30% del total de memoria 402560060

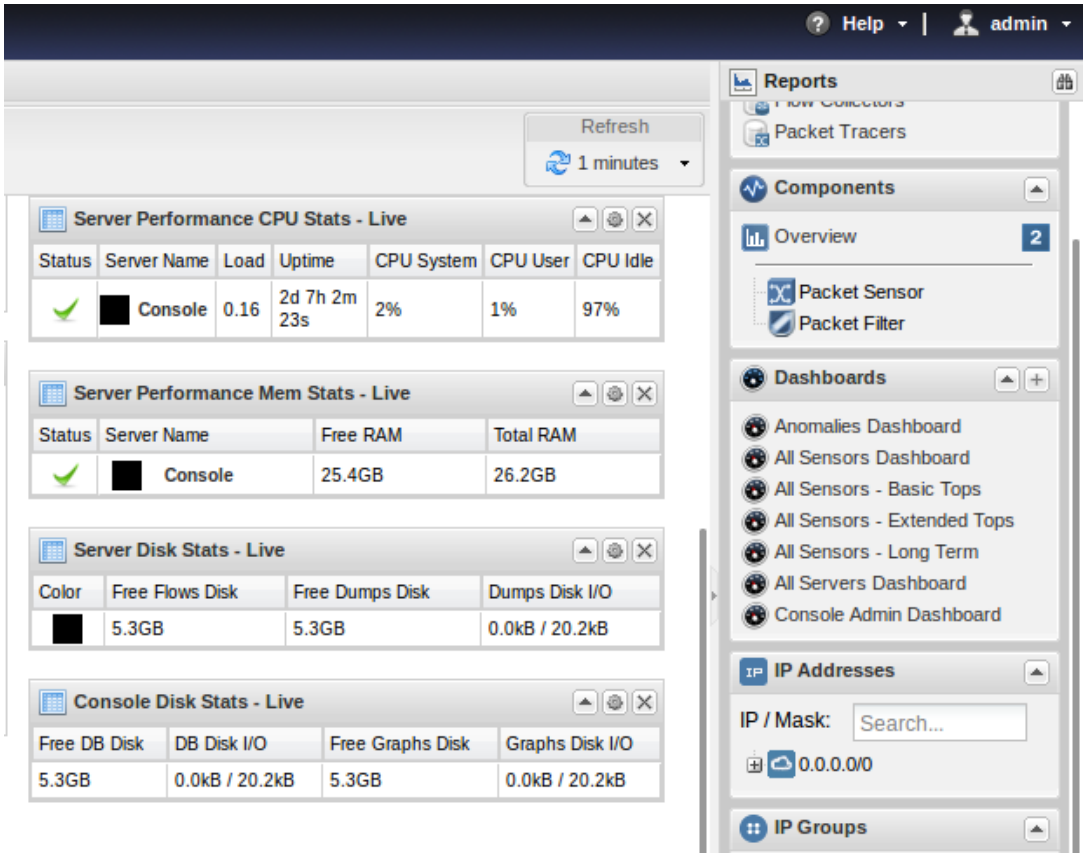
Detalle de procesador

```
RV082#show processes cpu sorted
CPU utilization for five seconds: 5%/0%; one minute: 8%; five minutes: 6%

PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 110    39178556   146224513        267  2.00%  3.23%  2.21%   0 IP Input
 337    14912552    10395627       1434  1.51%  1.26%  1.32%   0 DNS Server Input
 336     6533068    12748307        512  0.47%  0.48%  0.49%   0 DNS Server
  71     3261456    12066538        270  0.07%  0.18%  0.16%   0 Skinny Msg Serve
  27      734672     5372658        136  0.07%  0.02%  0.01%   0 ARP Input
```

El promedio del uso del CPU esta en 6%

Equipo ANTI DDOS



Uso de CPU: 2%
Uso de Memoria: 1%