DIAGNÓSTICO DE LA SEGURIDAD INFORMÁTICA DE LA RED DE DATOS DE LA EMPRESA SUNSHINE BOUQUET ZONA NORTE BOGOTÁ, COLOMBIA

ING. SILVIO HUMBERTO LÓPEZ ENRÍQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ZIPAQUIRÁ
2017

DIAGNÓSTICO DE LA SEGURIDAD INFORMÁTICA DE LA RED DE DATOS DE LA EMPRESA SUNSHINE BOUQUET ZONA NORTE BOGOTÁ, COLOMBIA

Presentado por:

ING. SILVIO HUMBERTO LÓPEZ ENRÍQUEZ

Propuesta de grado para optar por el título de especialista en seguridad informática

Director

Mg. LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

ZIPAQUIRÁ

2017

Nota de aceptación

_____

_____

_____

_____

_____

Firma del Director

_____

Firma del Asesor

_____

Firma del Jurado

CONTENIDO

Pág.

2 PLANTEAMIENTO DEL PROBLEMA 10
2.1 DESCRIPCIÓN DEL PROBLEMA 10
2.2 FORMULACIÓN DEL PROBLEMA 12
3 JUSTIFICACIÓN 13
4 OBJETIVOS 14
4.1 OBJETIVO GENERAL 14
4.2 OBJETIVOS ESPECÍFICOS 14
5 MARCOS DE REFERENCIA 15
5.1 MARCO DE ANTECEDENTES 15
5.2 MARCO TEÓR ICO 18
5.2.1 Open Web Application Security Project (OWASP).. 20
5.2.2 Verificar la seguridad antes y después. 21
5.2.3 Prevenir ataques de PHISHING.. 25
5.2.4 Pentesting. 27
5.2.5 Sistemas de monitoreo comparativa 32
5.3 MARCO CONCEPTUAL 34
5.4 MARCO LEGAL 37
5.4.1 Ley no 1273 del 5 de enero de 2009 37
5.4.2 Gobierno TI. 40
5.4.3 Documento conpes 3701.. 41
5.4.4 Norma Técnica Colombiana NTC 5254. 41
6 DISEÑO METODOLÓGICO 42
6.1 METODOLOGÍA DE INVESTIGACIÓN 42
6.2 METODOLOGÍA DE DESARROLLO 42
6.3 ALCANCE Y DELIMITACIÓN DEL PROYECTO 42
6.3.1 Alcance.. 42
6.3.2 Delimitaciones. 42
7 ACTIVIDADES 43
7.1 RECOPILACIÓN DE LA INFORMACIÓN 43
7.1.1 Entorno físico. 44

7.1.2 Topología. 45
7.1.3 Infraestructura.. 45
7.1.4 Puntos a observar. 45
7.1.5 Entrevista. 45
7.1.6 Formato de preguntas (Auxiliares y Ayudantes). 46
7.1.7 Análisis de requerimientos. 46
8 APLICANDO LA METODOLOGÍA MAGERIT V3. 47
8.1 ANÁLISIS Y TRATAMIENTO DE RIESGOS 47
8.1.1 Gestión del riesgo. 47
8.1.2 Actividades. 47
8.1.3 Identificando los activos. 47
8.1.4 Activos de Hardware (HW).. 47
8.1.5 Activos de Servicios Internos (SI). 50
8.1.6 Activos de Aplicaciones (SW). 51
8.1.7 Activos De Soporte De La Información (BKPS). 52
8.1.8 Activo de Equipamiento Auxiliar (EAUX). 52
8.1.9 Activo de Personal (P). 53
8.2 VALORANDO LOS ACTIVOS 54
8.2.1 Criterios de valoración. 54
8.2.2 Dimensiones. 54
8.2.3 Caracterización de las amenazas. 56
8.2.4 Valoración de las amenazas. 61
8.2.5 Valoración de las salvaguardas. 66
9 METODOLOGÍAS DE MONITOREO DE REDES 67
9.1 OSSTMM 67
9.2 ISSAF 69
9.3 OTP. 69
9.4 PTES 71
10 PROPUESTA 73
10.1 ¿Por qué OSSTMM? 73
10.1.1 Ventajas y Desventajas. 74
10.1.2 Ámbitos de actuación. 74
10.2 Tipos de auditoría 75

10.3 Fases de la metodología 75
10.4 Seguridad perimetral 77
11 CONCLUSIONES 83
12 RECOMENDACIONES 84
13 BILBIOGRAFÍA 85
14 ANEXOS 88
14.1 CARTA DE AVAL POR PARTE DE SUNSHINE BOUQUET 88
15 VERIFICACIÓN FÍSICA Y LÓGICA SISTEMAS DE INFORMACION 89
16 RESUMEN ANALÍTICO EN EDUCACIÓN - RAE 105

ÍNDICE DE TABLAS

Pag.

Tabla 1. Comparativa sistemas de monitoreo de redes 32
Tabla 2. Diseño metodológico. 43
Tabla 3. Formato Entrevistas Auxiliares y Ayudantes. 13
Tabla 4. Formato Entrevistas Administrador. 14
Tabla 5. Activos de Hardware. 16
Tabla 6. Activos de servicio Internos. 18
Tabla 7. Activos de Aplicaciones 18
Tabla 8. Activos de BAKUPS 19
Tabla 9. Activos Equipamiento Auxiliar 19
Tabla 10. Activos de Personal 20
Tabla 11. Criterios de valoración. 21
Tabla 12. Dimensiones (convenciones). 21
Tabla 13. (Continuación). 22
Tabla 14. Características de las amenazas (convenciones) 23
Tabla 15. Características de las amenazas. 24
Tabla 16. Valoración de las amenazas (convenciones). 28
Tabla 17. Valorando las amenazas. 29
Tabla 18. Valoración salvaguardas. 33
Tabla 19. Comparativas metodologías. 41
Tabla 20. Controles en redes de datos Sunshine Bouquet Zona Norte. 44
Tabla 21. Planilla de validación. 58
Tabla 23 Pen Testing 75
Tabla 23 Pen Testing (Continuación) 76
Tabla 23 Pen Testing (Continuación) 77
Tabla 23 Pen Testing (Continuación) 78

Tabla 23 Pen Testing (Continuación) 79
Tabla 23 Pen Testing (Continuación) 80
Tabla 23 Pen Testing (Continuación) 81
Tabla 23 Pen Testing (Continuación) 82
Tabla 23 Pen Testing (Continuación) 83
Tabla 23 Pen Testing (Continuación) 84
Tabla 23 Pen Testing (Continuación) 85
Tabla 23 Pen Testing (Continuación) 86
Tabla 23 Pen Testing (Continuación) 87
Tabla 23 Pen Testing (Continuación) 88
Tabla 24. Resumen Analítico en Educación RAE. 89
Tabla 24. Resumen Analítico en Educación RAE. (Continuación) 90
Tabla 24. Resumen Analítico en Educación RAE. (Continuación) 91
Tabla 24. Resumen Analítico en Educación RAE. (Continuación) 92
Tabla 24. Resumen Analítico en Educación RAE. (Continuación) 93
Tabla 24. Resumen Analítico en Educación RAE. (Continuación) 94

INTRODUCCIÓN

La información de cada organización es considerada un recurso valioso, un activo importante, el cual se cuida y se protege; por tanto, es indispensable crear estrategias de seguridad que ayuden organizándola y protegiéndola, tanto a esta como a cada uno de los medios y mecanismos implicados, como pueden ser físicos, lógicos, dispositivos de almacenamiento y redes de datos.

Se considera de vital importancia que, en las empresas, y específicamente en Sunshine Bouquet, se formule un sistema de monitoreo en redes de datos y estadística de ataques, la cual permitiría evaluar, someter, cuantificar, y dar a conocer a sus directivas cada una de las falencias y amenazas encontradas. Para ello se realizará un diagnóstico que permita obtener la información del estado actual de seguridad informática de la empresa, así como definir metodologías de análisis de riesgo y técnicas de Pentest.

La formulación de un diagnóstico y análisis de seguridad informática para la red de datos de la empresa Sunshine Bouquet zona norte Bogotá, Colombia garantizará la confidencialidad, integridad y acceso de la información, minimizando errores o pérdidas de información, respondiendo de forma adecuada y con prontitud ante un incidente.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

Sunshine Bouquet [1] es una empresa certificada y líder en producción limpia y elaboración de productos florales de excelente calidad, buscando la satisfacción total del cliente en la cadena, con costos competitivos a través de la efectividad de sus procesos y un equipo humano satisfecho.

Sunshine Bouquet en la actualidad tiene una sede en Colombia y una sede en EE. UU., su planta operativa es de un poco más de cuatro mil quinientos empleados. El departamento de TI (Tecnologías de la información), que es uno solo para los dos países cuenta con una planta operativa de veintidós colaboradores, aproximadamente 450 cuentas de correo corporativo y unos 600 usuarios de computadoras, estos están divididos en Computadoras de Escritorio, Portátiles, Tabletas y Smartphones. Un centro de datos de 11 servidores centralizados y unos seis servidores que se instalan en algunas de las fincas en las cuáles cumplen la función de firewall.

Es importante dejar en claro que la empresa Sunshine Bouquet está conformada por zonas y fincas en Colombia. El mayor porcentaje de estas fincas se encuentra en el departamento de Cundinamarca y dos fincas en Antioquia.

En Cundinamarca se han sectorizado por zonas, siendo estas zona norte, zona sur y zona occidente.

La problemática actual que enfrenta la compañía se relaciona con la ausencia de reportes y registros sobre las fallas y vulneración de la red de datos, ya que éstos son necesarios para realizar las actividades de la empresa de manera confiable y segura. La ausencia de un programa u organigrama de seguridad informática permite

[1] Sunshine Bouquet, SIGESTION. Sobre nuestra misión. Obtenido de: http://www.sunshinebouquet.com/about-us

identificar problemas a tiempo, sus causas y qué dispositivos son los más afectados, para que los encargados dentro de la empresa puedan tomar acciones correctivas y preventivas al respecto. Esto ha traído como consecuencia el constante ataque de virus informáticos a los dispositivos móviles, pérdida de información y la falta de control sobre el acceso de usuarios que laboran en la empresa a información restringida[2].

Es por esto por lo que la adecuada identificación del sistema de comunicaciones y de su desempeño necesita la evaluación de factores que incidan en su funcionamiento. De esta manera, al incluir procedimientos para determinar los parámetros más importantes, se puede establecer el estado de funcionamiento y rendimiento del sistema, haciendo posible la escalabilidad a sistemas que permitan obtener respuestas en tiempo real[3].

[2] Área de informática y sistemas, 2018. Empresa SUNSHINE BOUQUET. Bogotá, D.C.
[3] SERNA, Leonardo; MORANTES, Luis; DELGADO, Edilson, 2015. Transferencia óptima de datos para el monitoreo y control remoto de sistemas en Tiempo real. Editorial Instituto Tecnológico Metropolitano, pág. 3. Primera Edición.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo un diagnóstico y unas recomendaciones de seguridad informática en las redes de datos de Sunshine Bouquet, Bogotá zona norte ayudaría a identificar y proteger la información digital sensible frente a amenazas y accesos no autorizados?

2 JUSTIFICACIÓN

Sunshine Bouquet[4], es una empresa multinacional dedicada a la producción y exportación de flores; en su mayoría son arreglos florales, los cuales se denomina Bouquets, cuenta con sedes en Estados Unidos y en Colombia en los departamentos de Antioquia y Cundinamarca.

Sunshine Bouquet es una empresa en crecimiento constante, esto hace que algunas prácticas, para el caso frente a la gestión de la información no obedezcan a procesos sino a costumbres evidenciables en el área de sistemas.

Sus centros de operación están por zonas y a su vez por fincas, para el efecto de este trabajo se delimitará en la Zona Norte, del departamento de Cundinamarca.

Cada una de estas fincas maneja un gran volumen de información diaria, la cual requiere ser compartida con otras fincas y zonas a su vez, esto no solo requiere de una gran arquitectura sino de una gran demanda de tecnología,

Se pretende medir qué tan expuesta puede estar esta información y que consecuencias traería la fuga de esta, queremos exponer algunas de estas inquietudes y también plantear algunas soluciones y medidas preventivas.

Un análisis y diagnóstico en las redes de datos de la empresa Sunshine Bouquet, Bogotá zona norte, ayudaría a identificar y proteger la información digital sensible frente a ataques y accesos no autorizados disminuyendo tanto el riesgo como la posibilidad de pérdidas o fuga de información por causas de malas configuraciones y/o malas prácticas.

[4] Ibid.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar y diagnosticar el estado actual de la seguridad de la red de datos de la empresa Sunshine Bouquet zona norte Bogotá, Colombia

3.2 OBJETIVOS ESPECÍFICOS

Identificar el estado actual de la seguridad física y lógica de la red de datos de la empresa Sunshine Bouquet Zona Norte Bogotá Colombia.

Definir la metodología y herramientas informáticas enfocadas al análisis de riesgos y pruebas de penetración.

Realizar pruebas de penetración en la red de datos para definir el estado actual de su seguridad.

Presentar un informe y proponer recomendaciones a partir de los de resultados obtenidos en el análisis y diagnóstico del estado actual de la red de datos.

4 MARCOS DE REFERENCIA

4.1 MARCO DE ANTECEDENTES

Se toma como principal fuente de referencia la norma ISO/IEC 27001:2013[5] versión 2013. Para todo lo relacionado con el inventario de activos, gestión y tratamiento de los riesgos se usa como referencia la metodología MAGERIT[6], algunas otras de las referencias web, fueron las siguientes:

360 Security Group S.A: es una empresa Colombiana con más de 7 años en el mercado con un enfoque claro hacia la prestación de servicios de alto nivel en ciberseguridad, además de la provisión de productos de los fabricantes más reconocidos. Security Group presta servicios de Implementación, soporte y mantenimiento de soluciones tecnológicas en seguridad de la información, redes y desarrollo de software; tanto directamente como a través de socios tecnológicos, para organizaciones locales y multinacionales en diversos sectores de la industria y la sociedad. cuenta con personal certificado en: CSSLP, CISSP, CISM, GSEC.

Activos TI SAS: En su sitio web afirma ser una compañía de consultores cuya experiencia en seguridad de la información excede más de 15 años en diversas disciplinas. Algunas de ellas son: consultoría, gestión del riesgo, estándares internacionales, análisis forense, investigación de delitos informáticos y seguridad de la información en general. Su equipo de trabajo afirma estar conformado por profesionales con posgrado en seguridad de la información, Consultores

[5] ISO. 2013. Norma Técnica ISO 27001. ISO. 2013. págs. 67. Obtenido de: http://uct.unexpo.edu.ve/index.php/uct/article/view/805/648.
[6] MAGERIT. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Internacionales (Brasil, España, India, USA), Gerentes de Proyecto certificados (PMP), Auditores Líderes e Internos de ISO 27001 certificados, Especialistas en análisis de fraudes, Especialistas en Investigación Forense y especialistas en pruebas de calidad y seguridad de software.

IT FORENSIC: su brouchure dice de tener 10 años de experiencia, con certificación a nivel nacional internacional. Ofrece servicios de con consultorías en las áreas de Seguridad Informática, Hacking Ético (Pentesting), Implementación y Auditorias en Sistemas de Gestión de Seguridad de la Información ISO / IEC 27001:2013, Administración y servicios en tecnología informática (TI) y Computo Forense, delitos informáticos y aseguramiento de los activos de información. Poseen un Know How cuentan con la formación académica y técnica a través de un grupo de especialistas certificados y reconocidos internacionalmente por su trayectoria en el ámbito de la seguridad de los Datos". La empresa ha tenido continua presencia en Ecuador, Colombia, Panamá, Bolivia y Venezuela. Ha participado a través de proyectos de investigación y académicos en eventos Internacionales de Seguridad Informática y Computo Forense.

Netsecure: Empresa que cuenta con más de 17 años de experiencia en Seguridad de la Información, Sus productos y servicios de seguridad están respaldados por las principales y marcas del mercado. Ofrecen desde consultoría hasta administración de soluciones, Su portafolio de servicios está orientado a satisfacer las necesidades en Seguridad de la Información con servicios de calidad que afianzan las relaciones de largo plazo.

SISEL INGENIERIA: Es una compañía que presta servicios profesionales, de apoyo, soporte técnico y Administración en sistemas informáticos, asesoría, consultoría y reingeniería de proyectos, Sistema para la Gestión de la Información de Seguridad Informática. Algunos de sus proyectos los cuales hacen públicos son los siguientes:

Universidad de Ciencias Médicas de Holguín[7]**:** Se trata de una investigación a cargo de Y Díaz Ricardo, Y Pérez- del Cerro, donde abordan un proyecto realizado en la Universidad de Ciencias Médicas de Holguín, **SISEL INGENIERIA**, dio solución implementando una herramienta de apoyo para la gestión de reportes de incidentes, control del estado de protección de los medios informáticos, así como la mejor preparación de los trabajadores en aspectos relacionados con la seguridad informática.

Análisis y diseño de un prototipo para un sistema de gestión de eventos de seguridad informática utilizando OSSIM[8]**:** Este es un proyecto de grado presentado por Luzón Guzmán, Gina Ivanova (2017), quienes analizaron una herramienta para realizar la gestión, monitoreo y registro de eventos de seguridad de informática, usando herramientas de software libre, y que a su vez se ajuste a cualquier modelo de red y que sea de bajo costo. El propósito de este trabajo fue diseñar un prototipo portable (máquina virtual) basado en la plataforma de código abierto OSSIM, misma que permite una gestión centralizada e intuitiva, que facilita la detección de eventos y vulnerabilidades en la red. Se detalla la arquitectura, configuración y análisis de los resultados obtenidos con la herramienta, tomado en cuenta la aplicación de directrices de seguridad establecidos por entidades de normalización internacionales ISO/INEN.

[7] SISTEMA PARA LA GESTIÓN DE LA INFORMACIÓN DE SEGURIDAD INFORMÁTICA EN LA UNIVERSIDAD DE CIENCIAS MÉDICAS DE HOLGUÍN. Obtenido de: http://www.ciencias.holguin.cu/index.php/cienciasholguin/article/view/827

[8] OSSIM. AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM). [En línea] OSSIM. Disponible en: https://www.alienvault.com/products/ossim

4.2 MARCO TEÓR ICO

Para Rafael Arrascaeta la norma ISO 27001:2005[9], se ha diseñado esencialmente para optimizar la gestión de la seguridad de la información para ellos ha creado lo que hoy en día se denomina un SGSI, es decir, un Sistema de Gestión de Seguridad de la Información. Esto por su parte a traído dos puntos de vista por parte de las empresas, unas que consideran que es el verdadero salvavidas y potras que creen que será la una carga pesada de cargar.

Lo cierto es que el principio de la norma es ser la guía de apoyo al personal de TI para trabajar en su propia:

Para ello se cuenta con la siguiente norma: ISO 27001 la cual define la estructura de un Sistema de Gestión de la Seguridad de la Información (SGSI) y expone cada uno de los controles necesarios para garantizar la seguridad adecuada en la organización. También encontramos definidos los requisitos mínimos para establecer una óptima gestión de los incidentes de seguridad, y cubre desde las debilidades en materia de seguridad hasta el desarrollo del Plan de Continuidad de Negocio de la organización.

La implementación o adopción de este tipo de normas exige una inversión no solo económica por parte de las entidades sino también importantes recursos en cuanto a personal, tiempo, capacitaciones y una serie de procesos y procedimientos que se deben no solo aprender sino también administrar, socializar y poner en práctica.

ISO 27001 Es una norma la cual forma parte de los estándares de ISO, su publicación data del 01 de mayo de 2009, la segunda edición fue publicada el 01 de diciembre de 2012, mientras que la tercera edición fue publicada dos años después es decir en el 01 de enero de 2014 más exactamente. Esta norma proporciona una visión general sobre las normas que componen la serie 27000. En un compendio todas las definiciones para la serie de normas 27000 y describe las bases y conceptos de por

[9] ibid.

qué es importante la implantación de un SGSI, en cuanto al establecimiento, monitorización, mantenimiento y mejora.

Competitividad. Este un factor que no puede ser ajeno a ninguna empresa de hoy en día, esto hace que hoy en día los clientes exijan a ISO 207001 como un requisito para algunas relaciones comerciales.

Calidad a la seguridad. Con la implementación de un Sistema de monitoreo a las redes de datos y estadísticas de ataque la seguridad se transformará en una actividad de gestión que a su vez conduce en una garantía a la información de una entidad. Reducción de riesgos.

Uno de los propósitos fundamentales de la norma es la implementación de los controles y la mejora continua, reduciendo al mínimo todo riesgo por robo, fraude, error humano intencionado o no, mal uso de instalaciones y equipo a los cuales se expone la información.

Concientización y compromiso. Al tratarse de una norma, esto implica directamente a áreas y personal comprometido no solo a la gestión que la norma exige, sino también a su, mantenimiento y sostenimiento posterior.

Mejora continua. Esta es una actividad implícita a la norma, la implementación y puesta en marcha de un Sistema de monitoreo a las redes de datos y estadísticas de ataque, debe incluir programas de auditoría interna las cuales ofrecen una oportunidad de detectar debilidades del sistema y las áreas a mejorar para contribuir a la mejora continua de la empresa.

Firewall de aplicaciones web. Un firewall es una medida de seguridad usada por las diferentes empresas en función de proteger su información, este puede ser hardware, software o el trabajo conjunto de estos dos. Su función es la de añadir una capa más de seguridad a su red de datos, es pocas palabras es el centinela de la información pues bajo su responsabilidad está el registro de cada una de las peticiones entrantes

como también el registro de cada uno de los paquetes salientes en una red de datos.

Fuente: Elementos básicos de la seguridad perimetral

http://idgrup.com/servicios/servicios-gestionados-de-seguridad/seguridad-perimetral-como-servicio/

4.2.1 Open Web Application Security Project (OWASP). Es una de las organizaciones que trabajan en pro de la seguridad de la información es sin ánimo de lucro y a la fecha es uno de las entidades más relevantes autoridades en cuanto al desarrollo de aplicaciones seguras, para ellos dispone de un gran número de herramientas las cuales pueden ayudar a identificar vulnerabilidades en nuestro sitio o desarrollo web, sino también una gran cantidad de normativas, procesos y procedimientos en pro de las buenas prácticas del uso de las nuevas tecnologías.

Controles de seguridad según OWASP.

4.2.2 Verificar la seguridad antes y después. la seguridad es uno de los principales ítems a tener en cuenta y se debe estipular desde el inicio de concepción del proyecto.

- ✓ Bien es cierto que a la fecha no existe una tecnología que sea inmune a las vulnerabilidades. Desde el inicio se debe tener en cuenta que la aplicación debe quedar abiertas a actualizaciones y cambios de versión,
- ✓ Es importante selecciona una base tecnológica de fabricantes que suministran soporte.

PARAMETRIZAR LAS CONSULTAS

- ✓ Al momento del diseño y desarrollo de una consulta, es muy importante tener en cuenta que estas son vulnerables a ataques de inyección de código SQL.
- ✓ La inserción de un simple código SQL puede permitir que la base de datos entera sea robada, eliminada o modificada.
- ✓ Por lo general un Sistema de gestión de base de datos (SGB), suele manejar varias bases de datos, esto indica que, si se tiene acceso al SGBD, ya se tendría acceso a todas las bases de datos que dé el dependan.

CODIFICAR LOS DATOS

- ✓ Hoy en día es inconcebible él envió de datos no cifrados.

VALIDAR TODAS LAS ENTRADAS

- ✓ Los formularios validados son el mejor filtro a la hora de enviar o recibir datos.
- ✓ La validación debe ser sintáctica y semántica.
- ✓ La validación final siempre tiene que ejecutarse en el servidor de aplicaciones.

VALIDAR TODAS LAS ENTRADAS

- ✓ Campos de formularios.
- ✓ Encabezados HTTP
- ✓ Cookies.
- ✓ Parámetros GET y POST (incluyendo campos ocultos)
- ✓ Archivos.
- ✓ Servicios (Web service, XML-RPC)

VALIDAR TODAS LAS ENTRADAS

- ✓ Utiliza listas negras de contenido malicioso.
- ✓ Utiliza listas blancas de contenido “confiable”.
- ✓ Recuerda que la validación no hace necesariamente las entradas más seguras.
- ✓ La de la aplicación tiene que reforzarse donde las entradas son empleadas.

IMPLEMENTAR CONTROLES DE IDENTIDAD Y AUTENTICACIÓN

- ✓ Implementar un mecanismo racional ante ataques de fuerza bruta.
- ✓ Implementar un mecanismo seguro de recuperación de contraseñas.
- ✓ Evitar que las contraseñas sean recordadas y cacheadas.
- ✓ Repetir el proceso de autenticación ante operaciones sensibles como la confirmación de una compra o el cambio de contraseña.
- ✓ Enviar siempre las credenciales a través de canales seguros.
- ✓ Evitar usar credenciales por defecto y la predicción de las existentes.
- ✓ Evitar la enumeración de credenciales de usuarios.
- ✓ Evitar el envío constante de credenciales primarias de usuarios.
- ✓ Administrar las cookies de sesión

IMPLEMENTAR CONTROLES DE ACCESO

- ✓ No confundir la autorización con la autenticación.
- ✓ Los controles de acceso son simples: Solo tienen que decir si el usuario tiene o no acceso a un determinado recurso.
- ✓ Todas las peticiones deben pasar por un mecanismo único de autorización.
- ✓ Denegar el acceso a los recursos por defecto.
- ✓ Aplicar el principio de menor privilegio.
- ✓ Evitar mezclar el código de la lógica de procesos con el código de la lógica de autorización:
- ✓ Realizar chequeos de autorización dato/usuario en lugar de dato/rol.
- ✓ Los datos necesarios para la autorización deben provenir del servidor y no del cliente.

PROTEGER LOS DATOS

- ✓ Determinar cuáles son los datos sensibles y encríptalos (Ej. Contraseñas almacenadas en la Base de Datos)
- ✓ Encriptar los datos transmitidos usando mecanismo como TLS (HTTPS).
- ✓ Tratar de que los datos no sean expuestos accidentalmente.
- ✓ Evitar la captura de información mediante técnicas de enumeración.

4.2.2.1 Mecanismos de registro.

- ✓ Monitorear la aplicación
- ✓ Generar estadísticas de procesos.
- ✓ Hacer auditorías de informática.
- ✓ Implementar Detección de Intrusos (IDS)
- ✓ Implementar actividades forenses.
- ✓ No registrar datos confidenciales (Desde contraseñas de usuarios hasta información secreta)
- ✓ Estar al tanto de las alertas y registros de actividades.
- ✓ Implementar firewall de aplicaciones.

4.2.2.2 Fortalecer la seguridad de la tecnología base.

- ✓ Casi siempre la tecnología base viene con un conjunto de prácticas de seguridad implementadas.
- ✓ Se debe mantener un control sobre las vulnerabilidades descubiertas y liberan nuevas versiones para corregir estas.
- ✓ La tecnología base viene con una arquitectura de seguridad predeterminada, muchas de las veces con las configuraciones óptimas, en muchos de los caos en mejor no personalizarla a menos que se tenga un excelente dominio de esta.
- ✓ Una de la buena práctica en seguridad informática consiste en estar bien y periódicamente informado sobre las vulnerabilidades y actualizaciones disponibles para aplicar los parches necesarios.

- ✓ Bien sabido es que el rechazo al cambio es uno de los primeros tropiezos con las que lidiar en las áreas de tecnología, así que es mejor asumir el cambio como algo permanente.

4.2.2.3 Gestión de los errores.

- ✓ Los sistemas informáticos son desarrollados por seres humanos, es decir que no están exentos del error, es preciso estar preparados para ellos y saber que estos revelan el estado de codificación interna de las aplicaciones, esto a su vez permite tener un mejor conocimiento de estas.
- ✓ Una parte muy importante sobre los mensajes de error es que estos deben estar bien codificados, puesto que los mensajes de error pueden ser tomados y usados en nuestra propia contra.
- ✓ Un error mal manejado, puede dejar nuestro sistema en bloqueo so fuera de servicio.
- ✓ Es muy importante la validación al momento de la creación de los usuarios y sus respectivas contraseñas, un error común es que estas no coincidan ya sea el usuario o la contraseña.
- ✓ Los mensajes de errores deben hacer referencias a datos generales, sin descuidar que el usuario pueda guiarse.
- ✓ Es importante mantener una buena gestión los errores de esta forma lograremos evitar los errores duplicados.
- ✓ El manejo de Logs para el registro de errores es una de las practicas más recomendadas al momento del desarrollo de una aplicación[10].

[10] OWASAP. The free and open software security community. [En línea]. The Ten Most Critical Web Application Security Risks. Disponible en https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf

4.2.3 Prevenir ataques de PHISHING. El phishing es una práctica muy habitual por parte de los piratas o hackers informáticos, la cual consiste en la técnica de pesquisa, es decir envían códigos o menajes engañosos con el propósito de que un usuario incauto caiga en ellos y revele información relevante para el atacante. A continuación, veremos algunas pautas que pueden ayudar a no caer en ellos.

1. **Identificar correos electrónicos sospechosos**

- ✓ El phishing utiliza nombres, logos e imágenes de entidades reales y que se encuentren cerca de nuestra localización, todo esto gracias a la geolocalización
- ✓ Suelen llevar como remitente el nombre de la empresa o el de un empleado real de la empresa, esto hará que la víctima sea fácilmente engañada.
- ✓ Suelen clonar, por así decirlo sitios web corporativos, esto hará que a simple vista no se detecte el engaño.
- ✓ Otra técnica muy usada es mediante el envío de supuestos premios, regalos y un sinnúmero de engaños que se usan como gancho para engañar a los usuarios.

2. **Verifica la fuente de información de tus correos entrantes**

- ✓ Las entidades financieras o bancaras, no están autorizadas a pedir datos personales vía correo electrónico así que cualquier intento similar, puede ser un engaño, nunca envíe su usuario o contraseña vía correo si alguien desconocido se lo requiere, como tampoco sus datos personales.
- ✓ Nunca responda a este tipo encuestas, su primera reacción debe ser la de llamar directamente a la entidad que dice requerirla.

3. **Nunca ingrese al sitio web de su banco haciendo uso de los links incluidos en correo electrónico de dudosa procedencia.**

- ✓ Esta técnica suele camuflar las url y de esta forma redirigirlos a sitios fraudulentos.
- ✓ Es recomendable al momento de ingresar a una enditada financiera usar la barra de direcciones de su navegador de preferencia.
- ✓ Agregue sus sitios más frecuentes a la barra de favoritos, con esto no solo ingresa más rápido, sino que evitara escribir mal la dirección y terminar en sitios

no deseados. Los piratas informáticos saben del error y configura sitios fraudulentos con nombres similares.

4. **Refuerza la seguridad de tu ordenador**

✓ La seguridad en su computador debe ser en todos los aspectos:

- Antivirus
- Antispam,
- Antimalware
- Actualizaciones permanentes
- El pc que se dedica a los juegos no debe ser el mismo de las transacciones.

5. **Haga uso de sus datos confidenciales únicamente en webs seguras**

✓ Todo sitio web que use cifrado de datos empieza de la siguiente manera: **'https://www.sitioweb.com'** y debe aparecer en tu navegador el icono de un pequeño candado cerrado.

6. **Phishing está en todas partes**

✓ Si bien es cierto la mayor parte de ataques de phishing están dirigidas a entidades financieras, pero en realidad pueden utilizar cualquier otra web popular del momento como gancho para robar datos personales: el mejor escenario como siempre suelen ser las redes sociales, tiendas online entre otros.

7. **El phishing sabe idiomas**

✓ El phishing se vale de los mismos diccionarios en línea y puede llegar a atacar en cualquier idioma. Ya sabemos que este tipo de traducciones no es del cien por ciento acertada, así que este puede ser un indicador de sospecha.

✓ Si estamos en Colombia y además su navegador y sus sistemas operativos está en español, no tendría sentido que llegue un correo en otro idioma.

8. **Ante la mínima duda sea prudente y no se arriesgue**

- ✓ La mejor forma de actuar ante este tipo de amenazas es desconfiar, rechazar y eliminar cualquier correo electrónico o comunicado que le invite a revelar sus datos confidenciales[11].

4.2.4 Pentesting. Un Pentesting, que en la jerga informática se conoce como una prueba de penetración, haciendo referencia a la forma en que una persona con conocimientos informáticos logra romper algún nivel de seguridad en una red de datos y logra ingresar en ella, dejando evidencias de esta y soportándolas luego en un informe de gerencia[12].

4.2.4.1 Pasos de un Pentesting. *Blackbox*: Etapa conocida como la caja negra, es la parte en la que se dispone de poca información, en ocasiones se empieza desde cero con nuestro pensamiento al igual que lo haría un atacante real hasta llegar a un objetivo específico.

*Grey Box***:** Caja gris, esta es una etapa un nivel arriba de la caja negra, es decir que tendremos información mínima sobre la Infraestructura y podríamos disponer de un usuario con privilegios mínimos en la aplicación a analizar para ver si es posible el escalamiento de privilegios, es decir tenemos acceso a un nivel de la información.

White Box: También denominada la Caja blanca, en esta etapa que se denomina la etapa final o la etapa con mayor conocimiento de la infraestructura, el encargado del pentesting ha logrado tiene acceso a la información relevante y privada de la empresa.

4.2.4.2 Fases de un Pentesting.

1. *La firma del Contrato de Confidencialidad:* conocido como NDA (Non-Disclosure Agreement) en esta fase que es una de las iniciales es donde se define los directrices del servicio de pentesting a prestar, para ello es muy importante dejar

[11] PANDA SECURITY, Diez consejos para evitar ataques de pishinh. [En línea]. España: Panda. Disponible en: https://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

[12] GUTIERREZ DEL MORAL, Leonardo. Curso de seguridad y hacking ético 2013. [En línea]. España: 2014. Disponible en: https://books.google.com.co/books?id=sua0BAAAQBAJ&lpg=PA560&dq=QUE%20ES%20PENTESTING&pg=PA560#v=onepage&q&f=false

por escrito cada uno cada una de las actividades, tiempos estimados, alcances, personal involucrado, la recomendación es ser muy descriptivo y meticuloso en cada una de las actividades de servicio a prestar.

2. *Reconocimiento:* Esta fase describe la forma, la metodología en cuanto al reconocimiento del sitio en el que se va a realizar el Pentesting.

   Forma parte de las actividades pasivas las cuales determinan donde y como se dará el desarrollo del Pentesting, en esta etapa aún no se hace uso de herramientas.
3. *Enumeración:* Esta etapa ya se denomina activa, es decir ya se hace uso de herramientas para el desarrollo del Pentesting.
4. *Acceso:* En esta etapa es cuando habiendo usado herramientas y cada una de las fases anteriores se ha lo grado el ingreso a la infraestructura.
5. *Mantener Acceso:* Esta fase hace referencia al tiempo que se logre mantener el control de la red o equipos informáticos intervenidos, como también dejar la evidencia de este hecho.
6. *Borrar Rastros:* En esta fase es donde el atacante borra cada una de las huellas que puedo haber dejado por efectos de la perpetración, también denominada etapa antiforense,
7. *Generar Informe:* En esta fase se debe generar el informe de gerencias, el cual explica cada uno de los hallazgos durante el ejercicio de Pentesting, pero sin utilizar lenguaje técnico, es decir se trata de un informe entendible, completo y conciso.
8. *Informe Técnico:* Hace referencia un informe donde se describe cada uno de los pasos y hallazgos de forma descriptiva y técnica, es decir se escribe no solo las herramientas que se utilizaron sino las forma en que se hicieron las cosas.

4.2.4.3 Herramientas KALI LINUX para PENTESTING. NMAP es una herramienta no está desarrollada para realizar un escaneo de los puertos de una máquina remota. Una de las formas más comunes es la de enviar un paquete SYN, es decir, se intenta establecer una conexión TCP a un puerto específico escaneado. Y estar atento a la respuesta que este envíe para hacer uso de esto según su vulnerabilidad Empezaríamos, haciendo un escaneo a un servidor web, lo más probable es que estén abiertos los puertos 21(FTP), 53(DNS), 80(HTTP) y el puerto 443(HTTPS)[13].

- ✓ **SQLMAP**. El tema de inyección SQL es muy conocido en el campo de la seguridad informática, y esta herramienta es una de las favoritas. El propósito de la herramienta es la inyección de código malicioso en una base de datos y de esta forma lograr extraer información relevante[14].
- ✓ **HASHCAT**. Eta herramienta por su parte intenta revelar un contenido cifrado[15].
- ✓ **METASPLOIT FRAMEWORK**. Cuando se habla de un framework no solo se habla de una herramienta sino de un conjunto de herramientas dedicadas cada una de ellas a diferentes propósitos y esta es algo así como una navaja suiza dedicadas al uso de los exploits[16].
- ✓ **NESSUS**. Es una plataforma de análisis de vulnerabilidades que se ha convertido en una de las favoritas al momento de un análisis o auditoria de seguridad. Nessus incluye soporte para una variedad de sistemas operativos, y dispositivos como bases de datos, tabletas / teléfonos, servidores web entre otros[17].

---

[13] NMAP. Guía de referencia de Nmap. [En línea]. Nmap Network Scanning Disponible en: https://nmap.org/man/es/index.html

[14] SQLMAP. SQLMAP. [En línea]. Automatic SQL injection and database takeover tool Disponible en: http://sqlmap.org

[15] HASHCAT. Advanced Password Recovery. [En línea]. Disponible en https://hashcat.net/hashcat/

[16] METASPLOIT FRAMEWORK. [En línea]. The world's most used penetration testing framework. Disponible en https://www.metasploit.com

[17] NESSUS. Guía de seguridad. [en línea]. Redhat. Disponible en https://access.redhat.com/documentation/es-

- ✓ **W3AF**. Se trata de otro framework muy popular por su flexibilidad y potencia y flexible a la hora de buscar vulnerabilidades en aplicaciones web. Es muy fácil de utilizar y se apoya en diversos plugins que lo complementan[18].
- ✓ **HYDRA**. Esta es una herramienta usada para descifrar contraseñas multihilo, tiene la opción de fuerza bruta o a través de diccionarios, soporta los siguientes servicios: TELNET, POP3, SMTP, SMB, SSH V1 Y V2 TEC[19].
- ✓ **JHON O JHON THE RIPPER**. Otra de las aplicaciones de gran preferencia en la seguridad informática, su uso está orientado a revelar contenido cifrado, comúnmente denominado hash[20].
- ✓ **WIRESHARK**. Eta herramienta denominada un analizador de paquetes hace parte del conjunto de herramientas de Kali Linux, aunque también se puede descargar e instalar por separado, funciona en sistemas operativos Windows Linux y Mac[21].
- ✓ **PRTG Network Monitor**. Es una aplicación que tiene presentaciones tanto en iCloud como para escritorio, su función está orientada al monitoreo de redes supervisando sistemas, dispositivos y aplicaciones de una infraestructura de TI mediante las siguientes tecnologías. puede analizar segmentos de red haciendo ping a intervalos de IP definidos. De este modo, PRTG reconocerá automáticamente una amplia gama de dispositivos y sistemas y creará sensores a partir de plantillas de dispositivos predefinidos. Así se ahorra una gran cantidad de trabajo de configuración y puede iniciar la supervisión de forma inmediata[22].

ES/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-es-ES.pdf

[18] W3AF. Open Source Web Application Security Scanner. [En línea]. disponible en http://w3af.org

[19] HIDRA. Herramientas para hacking. “Fuera Bruta”. Disponible en: http://sectools.org/tool/hydra/

[20]JHON. Jhon the Ripper. Kali-Linux en español. [En línea]. John The Ripper. disponible en https://kali-linux.net/article/jhon-the-ripper/

[21] WIRESAHARK. Analizador de red al detalle. [En línea]. Seguridad en Línux. Disponible en https://www.solvetic.com/tutoriales/article/2610-wireshark-analizador-de-red-al-detalle/

[22] PAESSLER. Compañía de monitoreo de redes. [En línea]. PRTG. Disponible en https://www.es.paessler.com/prtg

- ✓ **SNMP**: listo para usar y con opciones de personalización Contadores de rendimiento de Windows y WMI
    - SSH: para sistemas Linux/Unix y MacOS
    - Analizador de flujos y paquetes
    - Peticiones HTTP
    - Cualquier API REST que devuelva XML o JSON
    - Ping, SQL.
- ✓ **EventSentry**. Es una herramienta de gestión de eventos e información de seguridad SIEM, por sus siglas en inglés Security Information and Event Management). Este tipo de herramientas son de gran ayuda en los departamentos de TI, ya que no solo permiten monitorear sino también están apoyadas en herramientas de analítica y reportes de gran utilidad. EventSentry se enfoca a monitorear cualquier dispositivo SNMP, tales como los servidores de Linux, enrutadores e interruptores que usan SNMP. EventSentry v3.4, es a la fecha la última versión de este conjunto de monitoreo SIEM híbrido. EventSentry v3.4 ofrece varias funciones nuevas para Protéjase contra los ataques de ransomware
    - Detecta movimiento lateral en una red con umbrales de colector
    - Identificar software obsoleto en su red
    - Ver la utilización detallada del ancho de banda (requiere NetFlow)
    - Controle los dispositivos UPS conectados
    - Integre con soluciones de código abierto (Graylog, ELK, Nagios Log Server y otros) 23.
- ✓ **OpManager**. Se trata de una de las grandes plataformas dedicadas a la gestión de redes la cual permite a se podría decir que, a todo tipo de empresa, sin importar su tamaño, administrar y supervisar eficazmente su infraestructura de TI. OpManager proporciona una gran cantidad de herramientas para monitorear redes, servidores y centros de datos para la

[23] EVENT SENTRY. SIEM. [En línea]. Sistema de monitoreo. Disponible en https://www.eventsentry.com

identificación de problemas de desempeño o uso de las tecnologías en tiempo real.

- ✓ Funciones principales:
- ✓ monitoreo y análisis de ancho de banda
- ✓ monitoreo de servidores
- ✓ monitoreo de uso de Internet
- ✓ monitoreo de desempeño.
- ✓ OpManager[24] es utilizado por clientes conocidos como DHL, Siemens y NASA.

4.2.5 Sistemas de monitoreo comparativa. A continuación, encontramos una tabla en la cual se ha realizado una comparativa entre los diferentes sistemas de monitoreo, se pretende resaltar los siguientes criterios: requerimientos, arquitectura, el número de nodos o dispositivos a que soporta para efectos de monitoreo, el rendimiento, su usabilidad y el costo.

Tabla 1. Comparativa sistemas de monitoreo de redes

APP	Requerimientos	Plataforma	Nodos	Rendimiento	Usabilidad	Costos
Prtg Network Monitor	Arquitectura para 32 y 64 bits. Memoria RAM desde 3G has 128 Gb, Procesadores entre 2 y 16. Disco duro mínimo 250 GB, recomendado 2TB	x64 de PC/Server, Windows Server 2012 R2 que tenga instalado .NET Framework 4.5 o posterior	De 1000 a más de 10mil sensores y desde 100 dispositivos hasta más de 1000	El rendimiento varía de acuerdo con las configuraciones del hardware y también el número de nodos comprometidos a mayor número de nodo mayor consumo de recurso y menos rendimiento.	Muy fácil de usar, aunque con conceptos técnicos, interfaz gráfica, funciona bajo cualquier navegador en versiones no muy antiguas.	El costo varía dependiendo el número de nodos, tiene una modalidad de pago anual o mensual.

[24] OPMANAGER. Software para la gestión integrada de redes. [En línea]. Alineando TI con el negocio. Disponible en https://www.manageengine.com

Tabla 1. (continuación).

APP	Requerimientos	Plataforma	Nodos	Rendimiento	Usabilidad	Costos
Event sentry	La instalación mínima puede ocupar unos 350 megas, pero se debe tener en cuenta el almacenamiento de los diferentes logs que genera la aplicación los requerimientos de memoria si es recomendable que esté por encima de 1 GB	Se puede instalar en cualquier plataforma, sea Windows, Linux y OS. 32 y 64 bits	cualquier tipo: Misma máquina Misma red física (hubs). Mismo switch con puerto espejo. En ambas maquinas (origen y destino).	Mejora de productividad ● Antelación de problemas ● Reporte y aviso de incidentes ● Agilidad en su tratamiento ● Mejor y mayor relación e integración de sectores adjuntos	Fácil de usar, muy buen sistema de reportes y graficas	Tiene 3 modalidades de licenciamiento que van desde una a mil licencias bajo Windows y Linux, Licencia para máquinas virtuales y también licencia para trabajar directamente sobre la nube

Tabla 1. (continuación).

APP	Requerimientos	Plataforma	Nodos	Rendimiento	Usabilidad	Costos
OpManager	Se puede instalar en un disco duro de 500Gb con memoria RAM de 2 GB todo depende del número de nodos, su configuración recomendada para unos 1000 nodos es de 4 procesadores con 8GB de RAM	Windows: 2008, 2003 Server, Vista, 2000profes sional +SP4, XP Professiona l Linux: RedHat 7.x and above, Debian 3.0, Suse, Fedora & Mandrake, cualquier navegador de las últimas versiones	Desde 100 a más de 10000 nodos	A pesar de su poco requerimiento de hardware es se considera una aplicación de alto rendimiento. Aun así, es bueno dejar en claro que todo esto depende de la cantidad de nodos a monitorear.	A pesar de su interfaz gráfica se dice que es un poco difícil de configurar y su curva de aprendizaje es lenta.	Al ser una aplicaci ón modula r el precio varía de la cantida d de módulo s a adquiri da i, tambié n incluye algunos plugins.

4.3 MARCO CONCEPTUAL

A continuación, encontramos la definición de terminología usada en el documento, con el fin de que su comprensión sea más sencilla. Siempre que se habla de información implica hablar de algunos términos inherentes sin los cuales no sería posible una buena explicación y /o comprensión.

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000)[25]. Esta es la definición técnica, pero bien sabido es por cada institución que la información empresarial es uno de los principales activos a administrar, cuidar y proteger. Del mayor número de cada tipo de amenazas.

[25] ISO 2700. El portal de ISO 27001 en Español Obtenido de: http://www.iso27000.es/download/doc_iso27000_all.pdf

Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)[26].

Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)[27].

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000)[28]

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema. (ISO/IEC 27000)[29].

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados.

Desastre o Contingencia: Interrupción de la capacidad de acceso a la información o procesamiento de ésta, impidiendo así el flujo normal de trabajo o disposición. (ISO/IEC 27000)[30].

Computador: También se le denomina computador personal u ordenador, dependiendo del lugar geográfico, pero hace referencia a una máquina electrónica la

[26] Ibíd
[27] Ibíd
[28] Ibíd
[29] Ibíd
[30] Ibíd

cual está diseñada para procesar datos de forma automática, almacenarlos, efectuar operaciones y presentarlos cuando se le requiera.

Servidor: es en esencia un computador con mayores características (configuraciones) que un computador personal, al cual se le han asignado unas tareas específicas, su uso más cotidiano es el de gestionar y administrar la información de una o más empresas en su roll de servidor de aplicaciones por ejemplo o servidor web o servidor de correo.

4.4 MARCO LEGAL

4.4.1 Ley no 1273 del 5 de enero de 2009[31]. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Ley N° 1273, 2009).

CAPITULO PRIMERO De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un

[31] COLOMBIA. CONGRESO DE LA REPÚBLICA. 2009. Ley 1273. Bogotá, D.C.: s.n., 2009. pág. p. 15. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

ARTÍCULO 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que

la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

ARTÍCULO 269H:[32] CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: las penas imponibles de acuerdo con los artículos descritos en este título se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

- ✓ Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- ✓ Por servidor público en ejercicio de sus funciones
- ✓ Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- ✓ Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- ✓ Obteniendo provecho para sí o para un tercero.
- ✓ Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- ✓ Utilizando como instrumento a un tercero de buena fe.
- ✓ Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales

CAPITULO SEGUNDO De los atentados informáticos y otras infracciones **ARTÍCULO 2691:** HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

---

[32] Ibíd

ARTÍCULO 269J:[33] TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. la misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

ARTICULO 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así: Articulo 58 CIRCUSTANCIAS DE MAYOR PUNIBILIDAD. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera[34].

4.4.2 Gobierno TI. Gobierno de TI (Tecnologías de Información) Es la forma en que el gobierno de cada país intenta estructurar y ayudar a cada una de las empresas en su mejora en cuanto a los servicios que estas presten a la comunidad haciendo uso de las tecnologías

En Colombia esta norma la regula el ministerio de las TIC, y desde su implantación por parte de las empresas cada usuario puede hacer un sin número de consultas en línea, como, por ejemplo, consultar el estado del pase, de un trámite, de un crédito entre muchos otros[35].

---

[33] Ibíd.

[34] CONGRESO DE LA REPUBLICA DECOLOMBIA [En línea]. Colombia, 2009 Ley 1273 de 2009. Disponible en http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

[35] GOBIERNO TI. “Arquitectura TI”. Disponible en: http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8078.html

4.4.3 Documento conpes 3701. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación Se trata de una serie procesos y procedimientos y lineamientos de política en ciberseguridad y ciber defensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema[36].

4.4.4 Norma Técnica Colombiana NTC 5254.

"GESTIÓN DE RIESGO" En este documento encontramos una guía para le implementación del proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos[37].

[36] CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL [En línea]. REPUBLICA DE COLOMBIA. 2011. Documento CONPES 3701. Disponible en http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[37] ICONTEC. (Instituto Colombiano de Normas Técnicas y Certificación). 2006. Documento Norma Técnica Colombiana NTC 5254. Disponible en: https://docgo.org/ntc-5254-pdf

5 DISEÑO METODOLÓGICO

5.1 METODOLOGÍA DE INVESTIGACIÓN

Para el desarrollo de este proyecto se hará uso de la metodología de investigación **CUANTITATIVA**, ya que se pretende medir mediante escalas la seguridad informática y de la información.

5.2 METODOLOGÍA DE DESARROLLO

"La investigación es un esfuerzo que se emprende para resolver un problema, claro está, un problema de conocimiento" (p. 47). "Sabino"[38]. Una metodología de desarrollo se refiere al entorno que se usa para estructurar; manifiesto que pretende mediar y controlar el desarrollo de un proceso. Existe una gran variedad de metodologías desarrolladas a lo largo de los años, cada una de ellas con sus fortalezas y debilidades. Una determinada metodología no es necesariamente aplicable a todo tipo de proyectos, cada tipo de proyecto tiene una metodología a la que se adapta mejor.

[38] Carlos Sabino. (Buenos Aires, Argentina, 24 de julio de 1944) Sociólogo e historiador

A continuación, encontramos en la tabla número 2, el diseño metodológico, en la cual se pretende discriminar cada uno de los objetivos, partiendo del objetivo general y a cada uno de los objetivos específicos, numerando las actividades, técnicas, instrumentos población y el producto a entregar.

Tabla 2. Diseño metodológico.

OBJETIVO GENERAL: analizar y diagnosticar estado actual de la seguridad de la red de datos de la empresa Sunshine Bouquet zona norte Bogotá, Colombia.					
Objetivos Específicos	**Actividades**	**Técnicas**	**Instrumentos**	**Población**	**Producto esperado**
Identificar el estado actual de la seguridad de la seguridad física y lógica de la red de datos de la empresa Sunshine Bouquet Zona Norte Bogotá Colombia.	Reunión con Gerencia y departamento de IT	Reunión	Formatos de registro. Formato de preguntas	Gerencias de Sunshine y director de IT	Documento de requerimientos Análisis de los documentos
Definir la metodología y herramientas informáticas enfocadas al análisis de riesgos y pruebas de penetración.	Visitar cada una de las instalaciones (fincas) donde Sunshine Bouquet tiene usuarios de computador	Entrevistas	Formatos de registro. Formato de preguntas	Líder del proyecto Cada uno de los usuarios a quienes se les haya entregado una computadora o teléfono (Smartphone)	Matriz de riesgos y amenazas

Tabla 2. (continuación).

Objetivos Específicos	**Actividades**	**Técnicas**	**Instrumentos**	**Población**	**Producto esperado**
Realizar pruebas de penetración en la red de datos para definir el estado actual de su seguridad	Realizar pruebas de Pen test	Capacitación, socialización	Auditoria interna	Líder del proyecto Cada uno de los usuarios a quienes se les haya entregado una computadora o teléfono (Smartphone)	Pruebas Pen Test Informe de gerencia
Presentar un informe y proponer recomendaciones a partir de los de resultados obtenidos en el análisis y diagnóstico del estado actual de la red de datos	Documentar las acciones preventivas y correctivas	Auditorías internas	Implantar en el SGSI las mejoras identificadas	Población involucrada	Propuesta a gerencia

5.3 ALCANCE Y DELIMITACIÓN DEL PROYECTO

5.3.1 Alcance. El proyecto pretende realizar un análisis y diagnóstico de seguridad informática en las redes de datos y de la empresa Sunshine Bouquet Bogotá Colombia, Zona norte.

Involucra todos los usuarios de sistemas en las áreas de: Gestión Humana, Nomina, Almacén y Producción que para su efecto usen computadoras Smartphone, tabletas y cualquier otra persona que tenga relación o acceso a alguna forma de información de la entidad, que para el efecto denominamos, clientes, proveedores y terceros. Se aplicará en las fincas de Zona norte.

5.3.2 Delimitaciones. El proyecto no cubre las tres zonas restantes de la empresa Sunshine Bouquet, como tampoco cubre las sedes en Estados Unidos,

El proyecto está sujeto a normativas de ley, se basa en ISO 2700 y gobierno es línea, esto significa que esta sensible a cambios.

6 ACTIVIDADES

6.1 RECOPILACIÓN DE LA INFORMACIÓN,

El primer paso para la recopilación de la información se visitó la finca Betania, propiedad de Sunshine Bouquet y de esa manera presenciar su infraestructura física y lógica a nivel de rede de datos, como también su topología.

Sunshine Bouquet es en esencia una empresa productora y exportadora de flores, esto ha hecho que el departamento de TI encuentre algunas limitaciones en infraestructura y presupuesto a esto se puede adicionar que su actividad se desarrolla en el campo en fincas lejos de la ciudad.

Los procesos activos que demandan de un servicio permanente de internet para el efecto de este trabajo se han sectorizado de la siguiente manera:

Administrativos: hacemos referencia a todo usuario que haga parte de las áreas de recursos humanos, nómina y almacenes.

Producción: para Sunshine Bouquet producción es el área más sensible y de mayor interés, puesto en ella se basa su economía.

Producción consta de los siguientes procesos los cuales se han ido implementando en una aplicación que recibe el nombre de *Sisflor*.

Siembras: Aplicación tipo cliente servidor a la fecha en procesos de implementación.

Recepción: Aplicación tipo cliente servidor que a la fecha es el inicio de la lógica del negocio. Es la encargada del registro e inventario - corte de cada uno de los tallos que son cortados y enviados desde cultivo.

Clasificación: Aplicación cliente servidor la cual permite el proceso permite registrar el proceso de separar cada uno de los tallos en aptos y no aptos de acuerdo con criterios como: color, variedad, grado (largo del tallo) y a su vez armar ramos de 20, 24 ó 25 unidades según variedad, los cuales son etiquetados con un código de barras

y luego enviados a inventario de flor disponible para el armado de los arreglos florales que para el proceso se denominan Bouquets.

Inventario de flor disponible: Aplicación tipo cliente servidor la cual permite el ingreso de la flor clasificada, tanto de la finca como de terceros y su posterior entrega a los diferentes sitios de producción los cuales son los en cargados de armar Bouquets y luego enviarlos al siguiente proceso que se denomina despachos.

Despachos: Aplicación tipo cliente servidor que permite disponer de los Bouquet y armar el despacho de acuerdo con el requerimiento del cliente.

Sistema Financiero: Aplicación tipo cliente servidor que para Sunshine Bouquet se denomina *Sisfin* el cual costa de los siguientes módulos: Financiero, comercial y almacén.

Aspersiones: Aplicación tipo cliente servidor la cual permite administrar cada una de las aplicaciones de químicos al cultivo.

Sistema de Gestión: (*sigestión*) aplicación web la cual administra el contenido de cada uno de los procesos y procedimientos que se manejan en la empresa.

6.1.1 Entorno físico. Sunshine Bouquet adecua de sus fincas siguiendo los siguientes requerimientos en cuanto a instalaciones físicas: Una construcción a la cual se denomina oficinas administrativas, una construcción denominada comedores, una construcción denominada Vestier y una construcción denominada postcosecha dentro de la cual se dispone de un cuarto de datos asignado al área de TI.

6.1.2 Topología. Sunshine Bouquet en su zona norte consta de 1 servidor, 36 portátiles, 70 computadoras de escritorio 35 dispositivos móviles los cuales se denominan clientes concurrentes.
A manera de visita se encuentran unos 12 portátiles y unos 17 teléfonos inteligentes los cuales requieres de conexión a la red inalámbrica de la empresa,

6.1.3 Infraestructura. La organización cuenta con una conexión permanente de Internet a través de dos enlaces vía radio frecuencia con dos proveedores diferentes y una red estrella en cableado UTP Cat 5e y Cat 6e que conecta a las distintas áreas de la finca, también cuenta con 5 enlaces internos los cuales interconectan las fincas aledañas y que hacen parte del grupo zona norte.

6.1.4 Puntos que observar. Número de personas involucradas en el departamento de TI de Sunshine Bouquet Finca Betania.

- ✓ Actividad que desarrolla cada involucrado en el departamento de TI
- ✓ Interacción entre los involucrados
- ✓ Tiempo transcurrido
- ✓ Formatos que cada involucrado maneja

6.1.5 Entrevista. se entrevistó a personal del departamento de ti y a personal administrativo con acceso a medios y/o dispositivos informáticos, cambiando el tipo de preguntas para cada caso ver anexo no. 2.

6.1.6 Tablas Formato de preguntas (Auxiliares y Ayudantes). En las tablas no. 3 y no. 4 se hace referencia al formato que contiene las preguntas con las cuales se ha hecho la entrevista al personal con cargos de auxiliares y ayudantes involucrados en el proceso.

Tabla 3. Formato Entrevistas Auxiliares y Ayudantes.

Formato entrevista a Personal TI y administrativos con acceso a la información y dispositivos informáticos				
	Fecha			
Responsable	Pregunta		☑ Sí	☒ No
Auxiliar Soporte	¿Sabe usted que es Seguridad Informática?			
Auxiliar Soporte	¿Sabe usted si existe una Aplicación o dispositivo físico de esta índole en la empresa?			
Auxiliar Soporte	¿Ha recibido capacitación a respecto?			
Auxiliar Soporte	¿Es eficiente el manejo de la información actual?			
Auxiliar Soporte	¿Qué beneficios le aporta?			
Auxiliar Soporte	¿Le ahorra tiempo?			
Auxiliar Soporte	¿Le haría cambios las tecnologías que su empresa usa en la actualidad?			
Auxiliar Soporte	¿Sabe usted que es riesgo informático?			
Auxiliar Soporte	¿Sabe usted que es Ransomware?			
Auxiliar Soporte	¿Sabe usted qué es un ataque de día cero?			
Auxiliar Soporte	¿Sabe usted qué es ingeniería social?			

Tabla 4. Formato Entrevistas Administrador.

Formato entrevista a director TI			
	Fecha		
Responsable	Pregunta	☑ Sí	☒ No
Director TI	¿Su empresa tiene implementado SGSI?		
Director TI	¿Su empresa usa algún sistema de cifrado?		
Director TI	¿Su empresa usa algún sistema DPI?		
Director TI	¿Su empresa Firewall?		
Director TI	¿Su empresa usa mecanismos de seguridad perimetral?		
Director TI	¿Su empresa se ha sometido a algún test de hacking ético (pen test)?		
Director TI	¿Su empresa ha sido víctima de Ransomware?		
Director TI	¿Su empresa cuenta con un programa de capacitación en seguridad Informática?		

6.1.7 Análisis de requerimientos. Para el análisis de implementación de un Sistemas de Monitoreo en Redes de Datos Y Estadística de Ataques en la empresa Sunshine Bouquet Zona norte se apoyará en la metodología MAGERIT[39]

[39] MAGERIT. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

7 APLICANDO LA METODOLOGÍA MAGERIT V3.

7.1 ANÁLISIS Y TRATAMIENTO DE RIESGOS

El análisis de riesgos se define como un proceso mediante el cual y en primera medida se hace una identificación de cada uno de los activos informáticos es decir permite determinar cuál es el activo, el costo y que tan protegido o desprotegido puede estar.

7.1.1 Gestión del riesgo.

7.1.2 Actividades.

- ✓ **Impacto y riesgo residual:** Hace referencia al conjunto de medidas que la entidad toma o planifica en pro de disminuir o los riesgos que pueden presentar cada uno de sus activos.
- ✓ **Selección de Salvaguardas:** esta sección es la encargada de presentar una guía con la cual las entidades pueden tomar la mejor decisión hacia el mejor método de selección de las salvaguardas.
    - *Técnicas:* aplicaciones, equipos y comunicaciones
    - *Físicas:* Protegen el entorno de trabajo de las personas y los equipos

- ✓ **Política de la Organización:** Hace referencia a las políticas y directrices las cuales delegan cada una de las responsabilidades a cada una de las entidades o personas.
- ✓ **Normas:** unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada. (MAGERIT versión 3)
- ✓ **Procedimientos:** manuales paso a paso de qué y cómo proceder al desarrollo de una acción. (MAGERIT versión 3).

- ✓ **Controles**: permiten saber que todo lo anterior está funcionando según lo programado. (MAGERIT versión 3) [40].

7.1.3 Identificando los activos. Con identificación de los activos se refiere a un levantamiento de la información de cada activo informático que haga parte de la red o la estructura a evaluar. Es decir, se levanta un inventario de cada uno de los activos informáticos comprometidos.

7.1.4 Tabla Activos de Hardware (HW). Hacen parte de este todo el equipo de cómputo que formen par del sistema informático.

Tabla 5. Activos de Hardware.

Equipos (HW)						
Id	Nombre	Descripción	Ubicación	Responsable	Tipo	Nivel
Sp016-HW001	Srv_0001	Servidor firewall	Centro-Sistemas	Dpto-Sistemas	Servidor (físico)	Crítico
Sp016-HW002	Srv_0002	Servidor nómina	Centro-Sistemas	Dpto-Sistemas	Servidor (físico)	Crítico
Sp016-HW003	Srv_0003	Servidor sigestión	Centro-Sistemas	Dpto-Sistemas	Servidor (físico)	Crítico

[40] MAGERIT. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 5. (continuación).

Equipos (HW)						
Sp016-HW004	Srv_0004	Servidor APP	Centro-Sistemas	Dpto-Sistemas	Servidor (físico)	Crítico
Sp016-HW005	Srv_0005	Servidor Correo	Centro-Sistemas	Externo	Servidor (físico)	Crítico
Sp016-HW006	Srv_0006	Servidor web	Centro-Sistemas	Externo	Servidor (físico)	Crítico
Sp016-HW007	Srv_0007	Servidor Backups	Centro-Sistemas	Dpto. Sistemas	Servidor (físico)	Crítico
Sp016-HW008	Router Wifi	Wifi nomina	Off. Nomina	Dpto-Sistemas	Router (físico)	No-crítico
Sp016-HW009	Router Wifi	Wifi Sigestión	Off. Sigestión	Dpto-Sistemas	Router (físico)	No-crítico
Sp016-HW0010	Router Wifi	Wifi producción	Off. Producción	Dpto-Sistemas	Router (físico)	No-crítico
Sp016-HW0011	Router Wifi	Wifi sala de juntas	Off. Sala de juntas	Dpto-Sistemas	Router (físico)	No-crítico
Sp016-HW0012	Router Wifi	Wifi Almacén	Off. Almacén	Dpto-Sistemas	Router (físico)	No-crítico
Sp016-HW0013	AP_001	Enlace interno	Centro-Sistemas	Dpto-Sistemas	AP (físico)	Crítico
Sp016-HW0014	AP_002	Enlace interno	Centro-Sistemas	Dpto-Sistemas	Router (físico)	Crítico
Sp016-HW0015	AP_003	Enlace interno	Centro-Sistemas	Dpto-Sistemas	Router (físico)	Crítico
Sp016-HW0016	AP_004	Enlace Interno	Centro-Sistemas	Dpto-Sistemas	Router (físico)	Crítico

7.1.5 Tabla Activos de Servicios Internos (SI). Hacen parte de este ítem los servicios que la empresa dispone para sus colaboradores y visitantes.

Tabla 6. Activos de servicio Internos.

Servicios internos (SI)						
Id	Nombre	Descripción	Ubicación	Responsable	Tipo	Nivel
Sp016-SI-0001	Internet	Servicio de internet sectorizado	Todas las áreas	Dpto-Sistemas	Internet (lógico)	Crítico
Sp016-SI-0002	Skype	Video llamadas – Chat	Todas las áreas	Dpto-Sistemas	Skype (lógico)	Crítico
Sp016-SI-0003	Telefonía – Celular	Telefonía Celular	Todas las áreas	Dpto-Sistemas	Celular (físico)	Crítico

7.1.6 Tabla Activos de Aplicaciones (SW). Hacen parte de este ítem todas las aplicaciones nativas o de terceros que la empresa dispone para su funcionamiento.

Tabla 7. Activos de Aplicaciones

Servicios Aplicaciones (SW)						
Id	Nombre	Descripción	Ubicación	Responsable	Tipo	Nivel
Sp016-SW-0001	Ofimática	Office 365	Todas las áreas	Dpto-Sistemas	Ofimática (lógico)	Crítico
Sp016-SW-0002	McAfee	Antivirus	Todas las áreas	Dpto-Sistemas	McAfee (lógico)	Crítico
Sp016-SW-0003	Sigestión	Sistemas de gestión	Todas las áreas	Recursos humanos	Celular (físico)	Crítico
Sp016-SW-0003	Sisflor	Software de producción	Producción	Dpto-producción	Celular (físico)	Crítico
Sp016-SW-0003	Sisfin	Soft. Financiero y nomina	Financiera y nomina	Dpto-Financiero	Celular (físico)	Crítico

7.1.7 Tabla Activos De Soporte De La Información (BKPS). Hacen parte de este ítem todos dispositivos y/o periféricos que la empresa dispone para el respaldo de la información.

Tabla 8. Activos de BAKUPS

Soporte de la información (BKPS)						
id	nombre	Descripción	Ubicación	Responsable	tipo	nivel
Sp016-BK-001	Srv_0007	Servidor Backups	Centro-Sistemas	Dpto. Sistemas	Servidor (físico)	Crítico
Sp016-BK-002	CD	Documentación digital	Centro-Sistemas	Dpto-Sistemas	CD (físico)	Crítico
Sp016-BK-0002	DVD	Documentación digital	Centro-Sistemas	Dpto-Sistemas	DVD (físico)	Crítico
Sp016-BK_0003	USB	Documentación digital	Centro-Sistemas	Dpto. Sistemas	USB (físico)	Crítico
Sp016-SI_0003	Disco duro	Documentación digital	Centro-Sistemas	Dpto-producción	DD (físico)	Crítico

7.1.8 Tabla Activo de Equipamiento Auxiliar (EAUX). Hacen parte de este ítem todos dispositivos auxiliares que apoyen o HAGAN parte del sistema informático de la compañía.

Tabla 9. Activos Equipamiento Auxiliar

Equipamiento Auxiliar (EAUX)						
Id	Nombre	Descripción	Ubicación	Responsable	Tipo	Nivel
Sp016-EAUX-0001	Planta E._01	Plata Eléctrica	Producción	Dpto. Mantenimiento	Planta (físico)	Crítico
Sp016-EAUX-0002	Cableado	Cableado estr . cat. 6e	Todas las áreas	Dpto-Sistemas	Cableado (físico)	Crítico
Sp016-EAUX-0002	Canaleta	Canaleta metálica 10x4	Todas las áreas	Dpto-Sistemas	Canaleta (físico)	Crítico
Sp016-EAUX-0003	UPS	UPS 12kva	Centro-Sistemas	Dpto. Sistemas	UPS (físico)	Crítico

Tabla 9. (continuación).

Equipamiento Auxiliar (EAUX)						
Sp016-EAUX-0004	CCTV	Circuito cerrado de TV	Todas las áreas	Dpto-Sistemas	CCTV (físico)	No-Crítico
Sp016-EAUX-0005	Antenas	Antenas de comunicación	Producción	Dpto-producción	Antenas (físico)	Crítico
Sp016-EAUX-0006	Torre_01	Torre de comunicaciones	Producción	Dpto-producción	Torre (físico)	Crítico

7.1.9 Tabla Activo de Personal (P). Hacen parte de este ítem todas las personas que involucradas en cada uno de los procesos y procedimientos de la compañía.

Tabla 10. Activos de Personal

Personal (P)						
Id	Nombre	Descripción	Ubicación	Responsable	Tipo	Nivel
Sp016-P-0001	Director TI	Director área de sistemas	Dpto-Sistemas	Dpto. Mantenimiento	Planta (físico)	Crítico
Sp016-P-0002	Jefe Sistemas	Jefe Sistemas	Dpto-Sistemas	Dpto-Sistemas	Cableado(físico)	Crítico
Sp016-P-0002	Programadores	Programador sistemas	Dpto-Sistemas	Dpto-Sistemas	Canaleta (físico)	Crítico
Sp016-P-0003	Ing. Soporte	Ing. Soporte	Dpto-Sistemas	Dpto. Sistemas	UPS (físico)	No-Crítico
Sp016-P-0004	Diseñadores	Diseñadores web	Dpto-Sistemas	Dpto-Sistemas	CCTV (físico)	No-Crítico
Sp016-P-0005	Auxiliares	Auxiliar de sistemas	Dpto-Sistemas	Dpto-producción	Antenas (físico)	No-Crítico

7.2 VALORANDO LOS ACTIVOS

7.2.1 Tabla Criterios de valoración. Para tal efecto MAGEIRT tiene una tabla, la cual presento a continuación.

Tabla 11. Criterios de valoración.

NIVEL	CRITERIO
10	NIVEL 10
9	NIVEL 9
8	NIVEL 8 (+)
7	ALTO
6	ALTO (-)
5	MEDIO (+)
4	MEDIO
3	MEDIO (-)
2	BAJO (+)
1	BAJO
0	DEPRECIABLE

7.2.2 Tabla Dimensiones. Consiste en presentar la información de los activos en acuerdo a una convención de dimensiones que sugiere **MAGERET.**

Tabla 12. Dimensiones (convenciones).

Letra	Descripción
D	Disponibilidad
I	Integridad de los datos
C	Confiabilidad de los datos
A	Autenticidad (usuarios e información)
T	Trazabilidad (Servicio y datos)

Tabla 13. (Continuación).

Tipos de Activos	Dimensiones				
Activos	**D**	**I**	**C**	**A**	**T**
Servicios internos					
Internet	(10)			(7)	(7)
Aplicaciones					
Ofimática	(10)				(7)
Antivirus	(10)				(7)
Sistema Operativo	(10)				(7)
Sistema de Información	(9)	(9)	(10)	(9)	(9)
Equipos					
Servidor de la base de datos	(10)	(10)	(10)	(9)	(9)
Medios de Impresión	(10)				(6)
Computadoras de escritorio	(10)				(8)
Routers	(10)				(8)
Cámaras de seguridad		(8)	(8)		(8)
Telefonía	(10)	(7)			(7)
Red WIFI	(10)				(7)
Red LAN	(10)				(7)
INTERNET	(10)	(7)	(7)		
Soportes de Información					
CD		(7)	(7)		
Documentación digital de procesos		(8)	(8)		
Documentación digital del Sistema de Información		(8)	(8)		
Informes en digital y físico		(8)	(8)		
Equipamiento Auxiliar					
Generador eléctrico	(8)				
Cableado	(8))				
Telefonía	(10)	(7)			(7)
Red WIFI	(10)				(7)
Red LAN	(10)				(7)
Telefonía	(10)	(7)			(7)
Red WIFI	(10)				(7)
Red LAN	(10)				(7)
INTERNET	(10)	(7)	(7)		
Soportes de Información					

Tabla 13. (continuación).

Dimensiones					
CD		(7)	(7)		
Documentación digital de procesos		(8)	(8)		
Documentación digital del Sistema de Información		(8)	(8)		
Informes en digital y físico		(8)	(8)		
Equipamiento Auxiliar					
Generador eléctrico	(8)				
Cableado	(8))				
Mobiliario	((8)				
Sistemas de Vigilancia	((8)				
Antenas	(8))				
Radios	(8))				
Instalaciones					
Edificio			(8)		
Personal					
Jefe de Oficina de Capital Humano			(8)		
Profesionales universitarios			(8)		
Secretarias			(7)		
Administrador de la base de datos			(9)		

7.2.3 Tabla Caracterización de las amenazas. Consiste en presentar la información de los activos de acuerdo con una tabla de convenciones que sugiere MAGERET.

Tabla 14. Características de las amenazas (convenciones)

Letra	Descripción
N	Desastre Natural
I	De origen industrial
E	Errores y fallos no intencionados
A	Ataque intencionado

Tabla 15. Características de las amenazas.

Activos	Amenazas
Internet	Uso no autorizado
Ofimática	(A1) Errores de usuarios (A2) Vulnerabilidades del software (E1) Errores de mantenimiento (A3) Propagación de programas maliciosos
Antivirus	(A1) Propagación de programas maliciosos (E1) Vulnerabilidades de los programas
Sistema Operativo	(E.1) Errores de los usuarios (E.4) Propagación de software dañino (E.2) Vulnerabilidades de los programas (software) (A.1) Uso no autorizado
Sistema de Información	(E.1) Errores de los usuarios (E.4) Propagación de software dañino (E.2) Vulnerabilidades del programa (software) (A.1) Uso no autorizado (A.2) Denegación de servicios (A.3) Acceso no autorizado (A.4) Abuso de privilegios de acceso
Servidor de base de datos	(N.1) Fuego (N.2) Daños por agua (I.2) Contaminación medioambiental (I.1) Avería de origen físico o lógico (I.3) Condiciones inadecuadas de temperaturas o humedad (E.5) Errores del administrador del sistema, de la seguridad (E.6) Errores de mantenimiento, actualización de equipos hardware (A.3) Acceso no autorizado (A.4) Manipulación del hardware
Medios de impresión	(I.1) Avería de origen físico o lógico (I.3) Condiciones inadecuadas de temperaturas o humedad (E.6) Errores de mantenimiento, actualización de equipos hardware (A.3) Acceso no autorizado

Tabla 15. (continuación).

Activos	Amenazas
Computadoras de escritorio	(N.2) Daños por agua (I.1) Avería de origen físico o lógico (I.3) Condiciones inadecuadas de temperaturas o humedad (E.6) Errores de mantenimiento, actualización de equipos hardware (E.7) Caída del sistema por agotamiento de recursos (A.4) Abuso de privilegios de acceso (A.1) Uso no autorizado
Routers	(N.1) Fuego (N.2) Daños por agua (I.2) Contaminación medioambiental (I.1) Avería de origen físico o lógico (I.3) Condiciones inadecuadas de temperaturas o humedad (A.3) Acceso no autorizado
Cámaras de seguridad	(A.3) Acceso no autorizado (N.2) Daños por agua (I.2) Contaminación medioambiental (I.1) Avería de origen físico o lógico (A.1) Uso no autorizado
Telefonía	(A.3) Acceso no autorizado
Red WIFI	(I.4) Fallo de servicios de comunicaciones (E.8) Errores de re-encaminamiento
Red LAN	(E.8) Errores de re-encaminamiento (E.9) Errores de secuencia (A.5) Suplantación de la identidad del usuario (A.6) Alteración de secuencia (A.3) Acceso no autorizado
INTERNET	(I.4) Fallo de servicios de comunicaciones (E.10) Alteración de la información

Tabla 15. (continuación).

Activos	Amenazas
CD /DVD	(E.10) Alteración de la información (E.13) Fuga de información (A.10) Modificación de la información (A.12) Revelación de la información
Documentación digital de procesos. (USB/DD)	(A.3) Acceso no autorizado (E.10) Alteración de la información (A.10) Modificación de la información (A.11) Robo de la información
Documentación digital del Sistema de Información. (USB/DD)	(A.3) Acceso no autorizado (E.10) Alteración de la información (A.10) Modificación de la información (A.11) Robo de la información
Informes en digital y físico	(A.3) Acceso no autorizado (E.10) Alteración de la información (A.10) Modificación de la información (A.11) Robo de la información
Planta eléctrica	(I.2) Contaminación medioambiental (I.3) Condiciones inadecuadas de temperaturas o humedad
Cableado voz y datos	(I.2) Contaminación medioambiental (I.3) Condiciones inadecuadas de temperaturas o humedad
Mobiliario	(I.2) Contaminación medioambiental
Sistema de Vigilancia	(I.2) Contaminación medioambiental (I.3) Condiciones inadecuadas de temperaturas o humedad
Antenas	(I.2) Contaminación medioambiental
Radios	(I.2) Contaminación medioambiental
Oficinas	(N.1) Fuego (N.2) Daños por agua (N.3) Tormentas (N.4) Terremotos (A.7) Ocupación enemiga

Tabla 15. (continuación).

Activos	Amenazas
Director TI	(E.11) Enfermedad (E.12) Huelga (A.8) Extorsión (A.9) Ingeniería Social
Ingenieros	(E.11) Enfermedad (E.12) Huelga (A.8) Extorsión (A.9) Ingeniería Social
Programadores	(E.12) Huelga (A.8) Extorsión (A.9) Ingeniería Social
Administrador de la base de datos	(E.11) Enfermedad (E.12) Huelga (A.8) Extorsión (A.9) Ingeniería Social (A.4) Abuso de privilegios de acceso
Vigilantes	(A.8) Extorsión (A.9) Ingeniería Social

7.2.4 Tabla Valorando las amenazas. Consiste en presentar la información del valor de la amenaza de acuerdo con una tabla de convenciones que sugiere MAGERET.

Tabla 16. Valorando las amenazas (convenciones).

ABREVIATURA	DESCRIPCIÓN
MA	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA
CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO POSIBLE
MB	SIGLOS
MR	MUY RARA

Tabla 17. Valorando las amenazas.

Activos	Amenazas	P	[D]	[I]	[C]	[A]	[T]
Internet	[A.1] Uso no autorizado	MA	M	M	M		
Ofimática	[E.1] Errores de los usuarios	P	M	M	M		
	[E.2] Vulnerabilidades de los programas (software)	P	M	M	M		
	[E.3] Errores de mantenimiento / actualizaciones de programas (software)	P	M	B			
	[A.2] Propagación de software dañino	PP	B	B	B		
Antivirus	[A.2] Propagación de software dañino	PP	B	B	B		
	[E.2] Vulnerabilidades de los programas (software)	P	M	M	M		
	[E.3] Errores de mantenimiento / actualizaciones de programas (software)	P	M	M			
Sistema Operativo	[I.1] Avería de origen físico o lógico	P	M				
	[E.1] Errores de los usuarios	PP	M	M	M		
	[E.4] Propagación de software dañino	PP	B	B	B		
	[E.2] Vulnerabilidades de los programas (software)	P	B	M	M		
	[E.3] Errores de mantenimiento / actualizaciones de programas (software)	P	M	B			
	[A.1] Uso no autorizado	P	B	B	B		
Sistema de Información	[E.1] Errores de los usuarios	PP	B	B	B		
	[E.4] Propagación de software dañino	PP	B	B	B		
	[E.2] Vulnerabilidades del programa (software)	PP	B	B	B		
	[E.3] Errores de mantenimiento / actualizaciones de programas (software)	PP	M	M			
	[A.1] Uso no autorizado	P	B	B	B		
	[A.2] Denegación de servicios	P	A	A	A	A	
	[A.3] Acceso no autorizado	P	A	A	A	A	
	[A.4] Abuso de privilegios de acceso	P	M	M	M	M	
Servidor de base de datos	[N.1] Fuego	P	A				
	[N.2] Daños por agua	P	A				
	[I.2] Contaminación medioambiental	P	A				
	[I.1] Avería de origen físico o lógico	P	A				
	[I.3] Condiciones inadecuadas de temperaturas o humedad	MA	MA				

Tabla 17. (continuación).

Activos	Amenazas	P	[D]	[I]	[C]	[A]	[T]
	[E.5] Errores del administrador del sistema, de la seguridad	P	M	M	M		
	[E.6] Errores de mantenimiento, actualización de equipos hardware	P	M				
	[A.3] Acceso no autorizado	PP		M	M		
	[A.4] Manipulación del hardware	P	M				
Medios de impresión (impresoras - fotocopiadoras)	[I.1] Avería de origen físico o lógico	P	M				
	[I.3] Condiciones inadecuadas de temperaturas o humedad	P	M				
	[E.6] Errores de mantenimiento, actualización de equipos hardware	P	M				
	[A.3] Acceso no autorizado	PP		M	M		
Computadoras de escritorio	[N.2] Daños por agua	PP	M				
	[I.1] Avería de origen físico o lógico	P	M				
	[I.3] Condiciones inadecuadas de temperaturas o humedad	PP	M				
	[E.6] Errores de mantenimiento, actualización de equipos hardware	P	M				
	[E.7] Caída del sistema por agotamiento de recursos	P	M				
	[A.4] Abuso de privilegios de acceso	PP	M	M	M		
	[A.1] Uso no autorizado	P	M	M	M		
Routers	[N.1] Fuego	PP	M				
	[N.2] Daños por agua	PP	M				
	[I.2] Contaminación medioambiental	PP	M				
	[I.1] Avería de origen físico o lógico	P	M				
	[I.3] Condiciones inadecuadas de temperaturas o humedad	P	M				
	[A.3] Acceso no autorizado	P	M	M	M		
Cámaras de seguridad	[A.3] Acceso no autorizado	P	M	M	M		
	[N.2] Daños por agua	P	M	M	M		
	[I.2] Contaminación medioambiental	PP	M	M	M		
	[I.1] Avería de origen físico o lógico	PP	M				
	[A.1] Uso no autorizado	P	M				
Telefonía	[A.3] Acceso no autorizado	P	M	M	M		
Red WIFI	[I.4] Fallo de servicios de comunicaciones	P	M				
	[E.8] Errores de re-encaminamiento	P			B		

Tabla 17. (continuación).

Activos	Amenazas	P	[D]	[I]	[C]	[A]	[T]
Red LAN	[E.8] Errores de re-encaminamiento	PP	B				
	[E.9] Errores de secuencia	P		M			
	[A.5] Suplantación de la identidad del usuario	P		M	M	M	
	[A.6] Alteración de secuencia	P		M			
	[A.3] Acceso no autorizado	PP		M			
INTERNET	[I.4] Fallo de servicios de comunicaciones	P	A				
	[E.10] Alteración de la información	P		B			
CD/DVD	[E.10] Alteración de la información	PP		B			
	[E.13] Fuga de información	PP			B		
	[A.10] Modificación de la información	PP		B			
	[A.12] Revelación de la información	P	A				
Documentación digital de procesos. (USB/DD)	[A.3] Acceso no autorizado	PP		B	B		
	[E.10] Alteración de la información	PP		B	B		
	[A.10] Modificación de la información	P		M	M		
	[A.11] Robo de la información	PP		B	B		
Documentación digital del Sistema de Información. (USB/DVD)	[A.3] Acceso no autorizado	PP		B	B		
	[E.10] Alteración de la información	PP		B	B		
	[A.10] Modificación de la información	P		B	B		
	[A.11] Robo de la información	PP		B	B		
Informes en digital y físico	[A.3] Acceso no autorizado	PP		B	B		
	[E.10] Alteración de la información	P		B	B		
	[A.10] Modificación de la información	PP		B	B		
	[A.11] Robo de la información	PP		B	B		
Planta eléctrica	[I.2] Contaminación medioambiental	P	M				
	[I.3] Condiciones inadecuadas de temperaturas o humedad	P	A				
Cableado	[I.2] Contaminación medioambiental	PP	A				
	[I.3] Condiciones inadecuadas de temperaturas o humedad	MR	B				
Muebles	[I.2] Contaminación medioambiental	PP	M				
Sistema de Vigilancia	[I.2] Contaminación medioambiental	PP	M				
	[I.3] Condiciones inadecuadas de temperaturas o humedad	MA	A				
Antenas	[I.2] Contaminación medioambiental	PP	A				
Radios	[I.2] Contaminación medioambiental	PP	M				
Edificio	[N.1] Fuego	P	A				

Tabla 17. (continuación).

Activos	Amenazas	P	[D]	[I]	[C]	[A]	[T]
	[N.2] Daños por agua	P	A				
	[N.3] Tormentas	P	M				
	[N.4] Terremotos	P	M				
	[A.7] Ocupación enemiga	P	MA		A		
Director TI	[E.11] Enfermedad	P	M	M	M		
	[E.12] Huelga	PP	B				
	[A.8] Extorsión	PP	M	M	M		
	[A.9] Ingeniería Social	MA	A	A	B		
Ingenieros	[E.11] Enfermedad	P	M	M	M		
	[E.12] Huelga	PP	B				
	[A.8] Extorsión	P	M	M	M		
	[A.9] Ingeniería Social	MA	A	A	B		
Programadores	[E.12] Huelga	PP	B				
	[A.8] Extorsión	P	M	M	M		
	[A.9] Ingeniería Social	MA	A	A	M		
Administrador de la base de datos	[E.11] Enfermedad	P	M	M	M		
	[E.12] Huelga	P	A	M	A		
	[A.8] Extorsión	PP	M	M	M		
	[A.9] Ingeniería Social	MA	A	A	A		
	[A.4] Abuso de privilegios de acceso	P	M	M	M		
Vigilantes	[A.8] Extorsión	PP	M	M	M		
	[A.9] Ingeniería Social	MA	M	M	M		

7.2.5 Tabla Valoración de las salvaguardas. Consiste en presentar la información de las salvaguardas de acuerdo con una tabla de convenciones que sugiere MAGERET.

Tabla 18. Valoración salvaguardas.

Eficacia	Nivel	Madurez	Estado
0%	L1	Inexistente	Inexistente
10%	L2	Inicial	Iniciado
50%	L3	Reproducible	Parcialmente realizado
90%	L4	Proceso definido	En funcionamiento
95%	L5	Gestionado y mediable	Monitorizado
100%	L6	Optimizado	Mejora continua

8 METODOLOGÍAS DE MONITOREO DE REDES

8.1 OSSTMM[41]

Open Source Security Testing Methodology Manual (OSSTMM) (Manual de la Metodología Abierta de Testeo de Seguridad) El OSSTMM es un trabajo realizado por el Instituto para la Seguridad y Metodologías Abiertas (ISECOM[42]).

Se dedica a la investigación, certificación, entrenamiento e integridad de los negocios, en el campo de la seguridad informática de forma práctica. OSSTMM es una metodología diseñada para realizar pruebas de seguridad, que se encuentra dividida por secciones, módulos y tareas. En cada sección se trata un área que conforma el sistema de información de una organización. El OSSTMM propone en cada sección la ejecución de unas tareas con el fin de encontrar la existencia de problemas que afecten en gran medida la seguridad de una organización.

Consta de las siguientes fases.

Sección A (Seguridad de la Información)

- ✓ Revisión de la Inteligencia Competitiva
- ✓ Revisión de Privacidad
- ✓ Recolección de Documentos

Sección B (Seguridad de los Procesos)

- ✓ Testeo de Solicitud
- ✓ Testeo de Sugerencia Dirigida
- ✓ Testeo de las Personas Confiables

Sección C (Seguridad en las tecnologías de Internet)

- ✓ Logística y Controles

---

[41] ISECOM, Institute for Security and Open Methodologies. OSSTMM 2.1. [en línea], 18 de febrero de 2017. Disponible en Internet: http://fcbi.unillanos.edu.co/segurinfo.unillanos/archivos/materialApoyo/OSSTMM.es.2.1.pdf.
[42] Ibid.

- ✓ Exploración de Red
- ✓ Identificación de los Servicios del Sistema
- ✓ Búsqueda de Información Competitiva
- ✓ Revisión de Privacidad
- ✓ Obtención de Documentos
- ✓ Búsqueda y Verificación de Vulnerabilidades
- ✓ Testeo de Aplicaciones de Internet
- ✓ Enrutamiento
- ✓ Testeo de Sistemas Confiados
- ✓ Testeo de Control de Acceso
- ✓ Testeo de Sistema de Detección de Intrusos
- ✓ Testeo de Medidas de Contingencia
- ✓ Descifrado de Contraseñas
- ✓ Testeo de Denegación de Servicios
- ✓ Evaluación de Políticas de Seguridad

Sección D (Seguridad en las Comunicaciones)

- ✓ Testeo de PBX
- ✓ Testeo del Correo de Voz
- ✓ Revisión del FAX
- ✓ Testeo del Modem

Sección E (Seguridad Inalámbrica)

- ✓ Verificación de Radiación Electromagnética (EMR)
- ✓ Verificación de Redes Inalámbricas [802.11]
- ✓ Verificación de Redes Bluetooth
- ✓ Verificación de Dispositivos de Entrada Inalámbricos
- ✓ Verificación de Dispositivos de Mano Inalámbricos
- ✓ Verificación de Comunicaciones sin Cable
- ✓ Verificación de Dispositivos de Vigilancia Inalámbricos
- ✓ Verificación de Dispositivos de Transacción Inalámbricos
- ✓ Verificación de RFID

- ✓ Verificación de Sistemas Infrarrojos
- ✓ Revisión de Privacidad
- ✓ Sección F – Seguridad Física
- ✓ Revisión de Perímetro
- ✓ Revisión de monitoreo
- ✓ Evaluación de Controles de Acceso
- ✓ Revisión de Respuesta de Alarmas
- ✓ Revisión de Ubicación
- ✓ Revisión de Entorno

8.2 ISSAF

ISSAF[43], del acrónimo en inglés OISSG (Open Information System Security Group) Es considerado un framework dedicado a la metodología de testeo en seguridad informática. Su función consiste es realizar pruebas de vulnerabilidad las cuales obedecen algunos criterios de evaluación. Que son los estándares en los que se basa ISSAF. Cada uno de éstos ha sido escrito y revisado por expertos en cada una de las áreas de seguridad informática. Estos criterios de evaluación se componen de los siguientes ítems:

- ✓ Una descripción del criterio de evaluación.
- ✓ Puntos y objetivos que cubrir.
- ✓ Los prerrequisitos para conducir la evaluación.
- ✓ El proceso mismo de evaluación.
- ✓ El informe de los resultados esperados.
- ✓ Las contramedidas y recomendaciones.
- ✓ Referencias y Documentación Externa.

8.3 OTP[44]

Del acrónimo en inglés “OWASP Testing Project” (OTP), de ha orientado a realizar pruebas sobre aplicaciones Web y hoy por hoy en una de las grandes referencias

[43] ISSAF. Disponible en http://www.oissg.org/issaf
[44] OTP. Disponible en https://www.owasp.org/index.php/OWASP_Testing_Project

al momento de establecer las buenas prácticas en cuanto a seguridad y programación de aplicaciones web. OTP intenta dar respuestas a las siguientes preguntas:

- ✓ ¿que?
- ✓ ¿por qué?
- ✓ ¿cuándo?
- ✓ ¿donde?
- ✓ ¿como?

E intenta cubrir los siguientes puntos al momento de hacer un Testing:

- ✓ El alcance
- ✓ Principios
- ✓ Explicación de las técnicas.

Su metodología de testeo incorpora aspectos muy importantes relacionados con el "Ciclo de Vida del Desarrollo de Software" con esto asegura las buenas prácticas incluso antes de que la aplicación esté en producción.

OTP invita a seguir los siguientes pasos:

Paso 1 Antes de comenzar el desarrollo

- ✓ Paso 1A Revisión de Políticas y Estándares
- ✓ Paso 1B Desarrollo de un Criterio de Medidas y Métricas (Aseguramiento de la Trazabilidad)

Paso 2 Durante la definición y el diseño

- ✓ Paso 2A Revisión de los Requerimientos de Seguridad
- ✓ Paso 2B Diseño de Revisión de Arquitectura
- ✓ Paso 2C Creación y Revisión de modelos UML
- ✓ Paso 2D Creación y Revisión de modelos de Amenazas

Paso 3 Durante el desarrollo

- ✓ Paso 3A Code Walkthroughs

- ✓ Paso 3B Revisión de Código

Paso 4 Durante el deployment

- ✓ Paso 4A Testeo de Penetración sobre la Aplicación
- ✓ Paso 4B Testeo sobre la Administración y Configuración

Paso 5 Operación y mantenimiento

- ✓ Paso 5A Revisión Operacional
- ✓ Paso 5B Conducción de Chequeos Periódicos
- ✓ Paso 5C Verificación del Control de Cambio

8.4 PTES

PTES[45] (Penetration Testing Execution Standart), es un estándar de ejecución de pruebas de penetración (Pentesting), consta de siete secciones principales. Con ellos pretende servir de guía en la realización de una prueba penetración,

Cubre desde el inicio que incluye todas las preguntas y respuestas antes del pentesting, pasando por la recopilación de información y las fases de modelado de amenazas donde los evaluadores trabajan detrás de escena para obtener una mejor comprensión de la organización, haciendo investigaciones de vulnerabilidad. explotación y post-explotación, donde la experiencia técnica de seguridad de los evaluadores viene a jugar un papel muy importante, finalmente va a la presentación de informes, que captura todo el proceso, de manera que tenga que el cliente pueda tener en sus manos una clara y completa descripción de cada una de las vulnerabilidades y falencias de su red de datos y componentes que al conforman.

Las siguientes son las secciones principales definidas por el estándar como base para la ejecución de pruebas de penetración:

- ✓ Interacciones previas al compromiso

[45] PTES. High Level Organization of the Standard. [En Línea]. Sitio oficial, Disponible en www.pentest-standard.org

- ✓ La recogida de información
- ✓ Modelado de amenazas
- ✓ Análisis de vulnerabilidad
- ✓ Explotación
- ✓ Explotación posterior
- ✓ Informes

.

9 PROPUESTA

Sunshine Bouquet, en su zona Norte requiere la implementación de políticas de seguridad que permitan proteger y salvaguardar cada uno de los recursos informáticos que hacen parte de la infraestructura TIC.

Estas políticas deben ser muy claras tanto en su permisión como en su prohibición desde y hacia cada uno de los recursos, usuarios y equipos informáticos.

Posterior a la recolección y el análisis de la información se ha hecho uso de algunos instrumentos como la observación en primera medida y la entrevista de los principales usuarios involucrados en el mayor flujo de movimiento de información como se ha identificado como cargos medios; los cuales serán abordadas con el apoyo de tecnologías como OSSTMM 2.1[46], la cual recopila un manual de metodologías abiertas para el testeo de la seguridad. Este proyecto se fundamente en la sección C, la cual trata de la seguridad en las tecnologías de internet, esto envista de que el las 5 aplicaciones más usada en la empresa y las cuales han sido desarrolladas por la propia compañía, es decir es software a la medida, son aplicaciones tipo web.

9.1 ¿POR QUÉ OSSTMM?

En referencia al capítulo 8 Metodologías de monitoreo de redes, se evidencia que OSSTMM junto con PTES[47] no solo son las más completas, sino que son las que más características tiene en común con el tipo de trabajo que tenemos en desarrollo. Pero OSSTMM es la única que abarca todos los ámbitos, con lo que se convierte en una metodología que sirve para evaluar la seguridad de localizaciones físicas, lógicas y cualquier tipo de interacción y/o comunicación en una infraestructura de red. (Wireless, Cableadas, Analógicas y Digitales). Uno de sus principales objetivos

[46] ISECOM, Institute for Security and Open Methodologies. OSSTMM 2.1. [en linea], 18 de febrero de 2017. Disponible en Internet: http://fcbi.unillanos.edu.co/segurinfo.unillanos/archivos/materialApoyo/OSSTMM.es.2.1.pdf.
[47] PTES. High Level Organization of the Standard. [En Línea]. Sitio oficial, Disponible en www.pentest-standard.org

de esta metodología es de poder responder las preguntas del STAR[48]; las cuales obedecen a un tipo de preguntas enfocadas en la ayuda tanto al auditor como al cliente a entender mejor el estado actual de la seguridad de su infraestructura de red.

Tabla comparativa metodologías: la tabla número 19, muestra una comparativa de las diferentes metodologías frente al ámbito en el que cada una de ellas hace más hincapié

Tabla 19. Comparativas metodologías.

Ámbito	NIST 800-115	PTES	OWASAP	OSSTMM
Ámbito Fisco				✓
Ámbito Social	✓			✓
Ámbito digital	✓	✓	✓	✓
Guía técnica		✓	✓	
Métricas				✓
Gestión de proyecto		✓		
Informes	✓	✓		✓

9.1.1 Ventajas y Desventajas. Algunas de sus ventajas que se han encontrado en la metodología son las siguientes:

- ✓ **Las métricas**. El principal requisito de una investigación son las formas en que se mide ya sea los hallazgos como también los resultados, y en el caso de un estudio de seguridad de la información, las métricas son imprescindibles.
- ✓ **Usabilidad**. Ampliamente difundida y valorada ya se en albito experimental como laboral por un gran número de entidades.
- ✓ **Multipropósito**. Su fuerte radica en que esta metodología es aplicable tanto el ámbito digital, el ámbito físico y humano.
- ✓ **Desventajas.** Esta metodología requiere gran cantidad de información para poder efecto de métricas, este mismo requisito hace que los resultados sean mucho más exactos, aunque es bien sabido que las métricas requieren de tiempo y experiencia si lo que se requiere es información fiable.

[48] STAR, Security Test Audit Report. [en línea], 8 mayo 2017. Disponible en Internet: https://dreamlab.net

- ✓ Esto mismo hace que su implementación sea más lenta y en casos tediosa al momento de su implementación.

9.1.2 Ámbitos de actuación. OSSTMM propone los siguientes ámbitos:

- ✓ Seguridad física (PHYSSEC):
  - *Humano*. Elemento humano sometido a pruebas de ingeniería social.
  - *Físico*. Evaluar los medios de seguridad física.
- ✓ Seguridad en el espectro *(ESPECSEC)*:
  - *Wireless. Evaluar las comunicaciones a nivel de espectro.*
- ✓ Seguridad en las comunicaciones (COMSEC):
  - *Telecomunicaciones*. Seguridad en las redes telefónicas analógicas y digitales.
  - *Redes de datos.* Seguridad en los sistemas informáticos y redes de datos.

9.1.3 Tipos de auditoría. Esta metodología propone distintos tipos de auditoría en función de las necesidades del cliente:

- ✓ Hacking Ético
- ✓ Caja Negra
- ✓ Caja Gris
- ✓ Caja Blanca
- ✓ Tándem
- ✓ Inversión

9.1.4 Fases de la metodología. La metodología está dividida en 17 fases agrupadas según su topología.

1. **Posture Review (Revisión Previa):** Identificar las reglas, normas, regulaciones, leyes y políticas aplicables al objetivo.
2. **Logistics (Logística):** La preparación del canal de pruebas (COMSEC) para evitar falsos positivos y falsos negativos.

3. **Active Detection Verification (Detección Activa):** Identificar los controles de seguridad activos y pasivos, de esta manera es más fácil la elección de las pruebas a realizar.
4. **Visibility Audit (Visibilidad):** Enumerar los objetivos del alcance mediante interacción con los sistemas vivos.
5. **Access Verification (Verificación Acceso):** Requiere enumerar los puntos de acceso del objetivo.
6. **Trust Verification (Verificación de Confianza):** Acceso a información sin la necesidad de estar identificado o autenticado.
7. **Controls Verification (Verificación de Controles**): Enumerar y verificar medidas de seguridad de los servicios y activos.
8. **Process Verification (Verificación de Procesos):** Evaluar los procesos encargados de las tareas de seguridad, para ver si se estén realizando de forma correcta. Esto corresponde al tipo de auditorías en donde el objetivo es evaluar la capacidad del equipo de seguridad de la organización.
9. **Configuration Verification (Verificación de Configuración):** Busca toda la información, básica o técnica, sobre cómo los activos funcionan en busca de configuraciones malas, inseguras o inexistentes.
10. **Property Validation (Validación):** Verificar la existencia de datos o información que pueda ser ilegal o poco ética.
11. **Segregation Review (Revisión de Segregación):** Se revisa la correcta separación de información privada y personal, de la información propiedad de la organización.
12. **Exposure Verification (Exposición):** Localiza y revisa información que pueda ser utilizada para acceder a múltiples sitios con la misma autenticación.
13. **Competitive Intelligence Scouting (Inteligencia):** Buscar información que pueda ser considerada para la inteligencia de negocios relacionada con la parte económica y de espionaje industrial.
14. **Quarantine Verification (Cuarentena):** Las medidas de contención son las encargadas de manejar la entrada de amenazas en la red de la organización.

15. **Privileges Audit (Escalado de Privilegios):** Pruebas en las que el analista ha recibido algún tipo de credencial.

16. **Survivability Validation (Validación de Supervivencia):** Determina la resistencia del objetivo ante pruebas de stress.

17. **Alert and Log Review (Revisión de Logs y Alertas):** Analizar la correcta gestión de alertas y logs que ha generado el proceso de análisis.

A continuación, se encuentra una descripción detallada de cada uno de los puntos para tener en cuenta como parte del mejoramiento en el tanto es el uso como en el resguardo de su infraestructura TIC

9.1.5 Tabla Seguridad perimetral. Hace referencias a todos los sistemas destinados a proteger de intrusos tu perímetro, debe cumplir cuatro funciones básicas: resistir a los ataques externos. Identificar los ataques sufridos y alertar de ellos. Aislar y segmentar los distintos servicios y sistemas en función de su exposición a ataques. Filtrar y bloquear el tráfico, permitiendo únicamente aquel que sea absolutamente necesario.

Tabla 20. Controles en redes de datos Sunshine Bouquet Zona Norte.

Titulo	Descripción
Políticas de seguridad	» Sunshine Bouquet debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada al personal involucrado y a las partes externas pertinentes.

Tabla 20. (continuación).

Titulo	Descripción
Controles	» Estos deben implementarse a Equipos, usuarios, roles, sistemas de información. Bases de datos, red de datos LAN y Wifi. » El departamento de TI de Sunshine Boquet a través de su personal de soporte en el área de sistemas deberá garantizar y asegurar que cada usuario tenga asignado unos derechos de acceso a los sistemas de información y recursos informáticos, de acuerdo con sus funciones, que permanezcan actualizados con el nivel de autorización sin que estas políticas interfieran en el adecuado desarrollo de sus labores y/o funciones. » Es responsabilidad del departamento de sistemas monitorear cada una de las políticas y garantizar su correcto funcionamiento como también su respectivo registro. » Es responsabilidad del departamento de sistemas validar que un usuario no pueda tener múltiples sesiones abiertas en cada uno de los sistemas a los cuales tenga acceso. » El departamento de sistemas debe garantizar que los usuarios no puedan instalar ningún tipo de software en los equipos asignados. » El departamento de sistemas debe garantizar un filtro el cual impida el acceso mediante internet a redes sociales, juegos, emisoras en línea, pornografía y todo tipo de contenido que no sea de carácter laboral. » El departamento de sistemas debe garantizar el bloqueo de puertos USB a memorias o dispositivos no autorizados. » El departamento de sistemas debe garantizar el cifrado de la información de cada usuario y de esa manera impedir la fuga de información confidencial.

Tabla 20. (continuación).

Titulo	Descripción
Roles	» Se deben definir y asignar a todas las responsabilidades de la seguridad de la información. » Los accesos a cada uno de los sistemas de información deben ser autorizados por la dirección de cada uno de estos sistemas de información.
Contraseñas	» Cada usuario debe contar con una autenticación y contraseña los cuales deben ser de uso personal e intransferible. » Las contraseñas deben tener un nivel de complejidad alto, es decir debe involucrar números, letras, mayúsculas y caracteres especiales; deben tener un periodo de caducidad y no deben permitir ser repetidas de periodos anteriores. » Las contraseñas no deben revelarse en ninguna circunstancia, en caso de fuerza mayos estas deben ser cambiadas inmediatamente, el nombre de usuario y la contraseña no puede ser iguales. No se debe usar contraseñas cíclicas. » La contraseña que se asigna por primera vez debe ser cambiada al inicio de la primera sesión. » Los usuarios deben poder cambiar la contraseña sin intervención del personal de sistemas. » Se debe configurar un número máximo de intentos fallidos, de haber cumplido la cuota, el usuario deberá reportar el incidente al departamento de sistema » Los computadores y aplicaciones deben cerrar sesión y auto bloquearse cuando no se detecte presencia del usuario pasado un tiempo determinado. » Es responsabilidad del área de sistemas mantener una cuenta de usuario con privilegios de administrador para efectos de contingencia en cada uno de los sistemas de información y servidores. Este usuario también debe tener un tiempo máximo para ser actualizado y cambiado de contraseña.

Tabla 20. (continuación).

Titulo	Descripción
Carta de responsabilidad	» Los equipos informáticos deberán ser entregados mediante una carta de responsabilidad, la cual explique las debidas sanciones en caso de daño, uso indebido o mal intencionado de los recursos. Cada usuario debe ser responsable de las actividades y transacciones realizadas en el equipo informático u roll asignado.
Retiros o cambios de cargo o roll	» Es responsabilidad de cada uno de los directivos informar al departamento de sistemas cada vez que haya un retiro, cambio de cargo, vacaciones o trasferencia de algún usuario para su respectiva actualización de privilegios o implementación de políticas o la respectiva desactivación del usuario.
Inventario de activos	» Es responsabilidad del departamento de sistemas mantener un inventario actualizado de cada uno de los equipos informáticos que hacen parte de la red de datos de Sunshine Bouquet Zona Norte. » Es responsabilidad del departamento de sistemas contar con documentación actualizada sobre los componentes y organización de la red y los recursos asociados como son: Políticas, enlaces, dispositivos de conexión física y protocolos de comunicaciones direcciones IP, segmentaciones, VPN´S y canales de comunicación.
Compras y actualizaciones	» Es responsabilidad el departamento de sistemas la adquisición de nuevos equipos informáticos y/o de comunicaciones. » Es responsabilidad del departamento de sistemas mantener actualizado y licenciado cada una de las aplicaciones de uso corporativo como son: Sistemas operativos, paquetes de ofimática, gestores de correo, antivirus, antimalware, antispyware,

Tabla 20. (continuación).

Titulo	Descripción
Backups	» Es responsabilidad del departamento de sistemas velar por el cuidado de la información de cada uno de los usuarios mediante un programa de copias de seguridad y su respectivo registro y control.
Formación y socialización	» Es responsabilidad del departamento de sistemas contar con un programa de capacitación e información continua a los usuarios.
Dispositivos Móviles	» El departamento de TI debe adoptar políticas y medidas de seguridad de soporte, para gestionar los riesgos que suponen estos dispositivos.
Teletrabajo	» Esta es una actividad que día a día es más común en las empresas, de tal manera que deben estar regidas y protegidas por políticas de seguridad de la información
Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa
Redes inalámbricas	» La administración de las redes inalámbricas debe ser responsabilidad del departamento de sistemas. » El departamento de sistemas debe garantizar una zona desmilitarizada (DMZ). » El departamento de sistemas debe garantizar una segmentación en las redes inalámbricas. » Las redes inalámbricas deben tener contraseña y filtrado MAC » El departamento de sistemas debe contar con Sistema de detección de intrusos y programas de monitoreo del comportamiento de cada uno de los dispositivos
Descargas	» El departamento de sistemas debe restringir las descargas sin importar el tipo de dispositivo conectado a la red. » Sólo funcionarios con previa autorización podrán “descargar” información desde Internet, esto se hará bajo la supervisión y monitoreo del departamento de sistemas.
Firewall	» Es responsabilidad del departamento de sistemas contar bien sea con dispositivos o software de firewall.
Internet	» Es responsabilidad del departamento de sistemas segmentar el acceso a internet por niveles y categorizarlos en restringido, menos restringido y sin restricción.

Tabla 20. (continuación).

Titulo	Descripción
Control de accesos físicos	» ES responsabilidad de las directivas definir y usar perímetros de seguridad, y a su vez asignarlos a las áreas que contengan información confidencial o critica, e instalaciones de manejo de información. » Las áreas seguras deben estar protegidas con controles de acceso apropiados para garantizar el acceso solo a personal autorizado.
Propiedad Intelectual	» Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
Cumplimiento con las políticas y normas de seguridad	» Es responsabilidad de las directivas revisar con regularidad el cumplimiento, procesamientos y procedimientos en cada una de las áreas de su alcance.

10 CONCLUSIONES

Se realizó una visita de campo a las instalaciones de la zona Norte de la empresa Sunshine Boquet ubicada en Tabio, Cundinamarca. Se pudo corroborar que las Tecnologías de la Información tienen limitaciones de conectividad en el lugar, por ser alejadas del área urbana. La empresa en esta zona tiene 1 servidor, 36 portátiles, 70 computadores y 35 dispositivos móviles.

Se aplicó una entrevista al personal de cada área de la sede para identificar las actividades de Tecnologías de la Información (TI) que desarrollan, la interacción, tiempos de respuesta y los formatos digitales que manejan.

La metodología empleada para el análisis es MAGERIT[49]. En la cual se establecen unos criterios de valoración de los activos con una escala descendente (10-0) y cinco dimensiones (disponibilidad, integridad de los datos, confiabilidad de los datos, autenticidad y trazabilidad). Los mejor puntuados en todas las dimensiones son sistema de información y servidor de la base de datos. También se aplicó el manual de la metodología abierta de testeo de seguridad (OSSTMM).

En cuanto al análisis de riesgos este permitió determinar los activos informáticos de la empresa. La mayoría de los activos encontrados se encuentran en nivel crítico (activos de hardware, activos de servicios internos, activos de aplicaciones, activos de soporte, activos de equipo auxiliar y activos de personal).

Al comparar las diferentes metodologías, se escogió la OSSTMM para delimitar la propuesta para la empresa Sunshine Bouquet. Se presentó una descripción detallada de los puntos propuestos de seguridad perimetral para el mejoramiento y monitoreo de TI en Sunshine Bouquet.

[49] MAGERIT. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

El uso adecuado de técnicas y metodologías del PenTesting permiten evaluar y encontrar riesgos existentes en los sistemas informáticos que, de otra manera, serían casi imperceptibles. De este modo no deben considerarse como un ejercicio aislado y poco rutinario, sino por el contrario deben ser implementados en las empresas como parte de sus procesos y procedimientos. Casi siempre resulta más eficaz y económico implantar una política que enmendar un desastre.

Se dice que la seguridad en cualquier organización es un aspecto frecuentemente cambiante, Una empresa puede alcanzar un nivel de es decir puede pasar de su momento óptimo a uno totalmente vulnerable, en un pequeño lapso, estamos rodeados de bugs, actualizaciones y cambios de versiones por doquier. No se debe olvidar que cualquier firmware puede no solo comprometer a un equipo sino, con este a la infraestructura entera.

Teniendo presente lo expuesto en las conclusiones del análisis y diagnóstico al estado actual de la seguridad de la red de datos de la empresa Sunshine Bouquet zona norte Bogotá, Colombia, se cumple con el objetivo propuesto, dando como resultado la siguiente lista de recomendaciones.

11 RECOMENDACIONES

Día tras día se escucha hablar sobre los riesgos de la información, para donde quiera que se mire hay algo o alguien que intenta llegar a ella, se ha vuelto como un reto personal. “todos trabajando en pro o en contra de ella”, esto no solo es una buena alarma la cual invita a actuar y que mejor hacerlo con procedimientos y procesos ya certificados, como lo son los sistemas de monitoreo en redes de datos y estadística de ataques, este tipo de tecnologías y prácticas estructuradas no solo muestra de forma gráfica y estadística los diferentes riesgos potenciales que son el pan de cada día, sino que prepara para la acción pronta y continua en el cuidado tanto de la información como de la infraestructura.

Es de vital importancia para Sunshine Bouquet, la adquisición e implementación de una arquitectura de seguridad informática, que esté en la capacidad de detectar, frenar, minimizar y/o prevenir tanto ataques como la fuga de la información. Esta debe cubrir la seguridad perimetral como red lógica de la empresa.

En la mayoría de las aplicaciones las cuales fueron cusa de la auditoría se requiere de un esquema que constate como mínimo la identidad del usuario, es decir que administre y audite sus credenciales de acceso, el uso de las aplicaciones, como también el encriptamiento del tráfico de datos en la red.

Hacer espacial hincapié en el seguimiento del tratado de los datos, es decir se debe monitorear y registrar: quien, cuando, con qué dispositivo, y a qué tipo de información hubo y tuvo acceso.

En cuanto a las aplicaciones, deben pretender y tratar de estar siempre disponibles, sin sacrificar la seguridad de estas. Deben contar con la mayor seguridad disponible y contar siempre con la experiencia del usuario.

Implementar políticas de capacitación y socialización de las políticas de la empresa en cuando a buenas prácticas y seguridad de la información a los colabores de la empresa, clientes proveedores y visitantes.

Unas de los principales beneficios de analizar y diagnosticar estado actual de la seguridad de la red de datos de la empresa Sunshine Bouquet zona norte Bogotá, Colombia:

Ayuda a estructurar y establecer una metodología con la cual podremos lograr una mejor administración de la gestión de la seguridad de la información.

Implanta medidas de seguridad para que los usuarios y clientes puedan acceder a la información segura.

Fomenta la mejora continua en la organización.

Es de vital importancia que las empresas no solo tomen conciencia sobre los riesgos y la seguridad informática, sino que también este esfuerzo se vea materializado en la asignación de presupuestos y disponga los recursos necesarios para la ejecución de este tipo de estrategia.

En cuanto a los servidores se recomienda implementar un buen plan de virtualización, esto no solo ayuda a implementar políticas de seguridad centralizadas, sino que en muchos casos resulta en ahorro de dinero, hardware y tiempo para la compañía.

Se propone la posibilidad de implementación de Machine learning, ya que pudimos detectar una gran cantidad de datos y tareas que soy muy repetitivas.

12 BILBIOGRAFÍA

ZORRILLA ARENA, Santiago (2000), Introducción a la metodología de la investigación, México: McGraw Hill

Benavides M.C. y Solarte F. (2012). Módulo de Riesgos y Control Informático

ISO2700. ¿Qué es un SGSI? [en línea]. <http://www.iso27000.es/sgsi.html> [citado en 15 de octubre de 2016]

Dirección de Estándares y Arquitectura de TI del Ministerio de las Tecnologías de Información y las Comunicaciones de la República de Colombia. (2014). Generalidades del Marco de Referencia – versión 1.0. [en línea]. <http://www.mintic.gov.co/portal/604/w3-propertyvalue-558.html >

ISO27000.es. Sistema de Gestión de la Seguridad de la Información. [en línea]. <http://www.iso27000.es/doc_sgsi_all.htm> [citado en 15 de octubre de 2015]

RISTI - Revista Ibérica de Sistemas y Tecnologías de Informação [en línea]. <http://www.scielo.gpeari.mctes.pt/scielo.php?pid=S1646-98952014000100004&script=sci_arttext> [citado en 11 de enero de 2016]

ISO 27001: La Seguridad de la Información en la Gestión de la Continuidad de Negocio. [en línea]. <http://www.pmg-ssi.com/2014/11/iso-27001-la-seguridad-de-la-informacion-en-la-gestion-de-la-continuidad-de-negocio/> [citado en 15 de octubre de 2015]

MENDEZ, C. Metodología, Diseño y Desarrollo del proceso de Investigación. Tercera Edición, McGraw Hill, Colombia, 2001.

JIMÉNEZ, L. Guía de desarrollo de un plan de continuidad de negocio. [en línea]. <http://www.criptored.upm.es/guiateoria/gt_m001r.htm> [citado en 30 de octubre de 2015]

LERMA, Héctor Daniel. Metodología de la investigación. Bogotá: Ecoe Ediciones, 2004.

NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos

Gómez R., Pérez D., Donoso Y. y Herrera A. (2010) Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Artículo. Revista de Ingeniería. Universidad de los Andes.

NTC-ISO/IEC 27005, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información

Ministerio de las Tecnologías de la información y las Comunicaciones. (2014). Decreto 2573 de 2014[en línea]. <http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf> [citado en 23 de enero de 2016]

Introducción al Sistema de Gestión de Seguridad de la Información – SGSI [en línea] <http://www.iso27000.es/sgsi.html> [citado en 01 de marzo de 2017]

ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS.

2012. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de

los Sistemas de Información. Madrid: s.n., 2012. p.1-127. Obtenido de:

https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-imetodo/file.html.

Todo sobre MAGERIT [en línea] <http://administracionelectronica.gob.es/ctt/magerit> [citado en 29de octubre de 2016]

Metodología MAGERIT [en línea] <http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/index.html> [citado en 11 de mayo de 2016]

Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT

[en línea]. <https://books.google.com.co/books?id=L-htLwEACAAJ&dq=magerit&hl=es-419&sa=X&redir_esc=y> [citado en 05 de junio de 2015].

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. 2015. Manual Estrategia de Gobierno en Línea. Bogotá, D.C.: s.n., 2015. p. 1-37. Obtenido de: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf.

Pentesting [en línea]. https://books.google.com.co/books?id=sua0BAAAQBAJ&pg=PA560&dq=que+es+pentesting&hl=es-419&sa=X&redir_esc=y#v=onepage&q=que%20es%20pentesting&f=false

Sitio oficial de Kali Linux [en línea] <http://tools.kali.org/ > [citado en 13 de febrero de 2016]

Mejores prácticas en la seguridad e contenidos [en línea] < www.mpaa.org>

Hoja de ruta [en línea] <https://www.w3.org/2014/07/mobile-web-app-state/index.es.html>

Sitio oficial de OWSAP [en línea] <https://www.owasp.org/index.php/Main_Page> [citado en 25 de enero de 2017]

10 consejos para prevenir ataques de Phishing [en línea] <http://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/> [citado en 07 de febrero de 2017].

Área de informática y sistemas, 2018. Empresa SUNSHINE BOUQUET. Bogotá, D.C.

SERNA, Leonardo; MORANTES, Luis; DELGADO, Edilson, 2015. Transferencia óptima de datos para el monitoreo y control remoto de sistemas en Tiempo real. Editorial Instituto Tecnológico Metropolitano, pág. 3. Primera Edición.

13 ANEXOS

13.1 CARTA DE AVAL POR PARTE DE SUNSHINE BOUQUET

CARTA DE ACEPTACIÓN

(Octubre 15 DE 2016)

DATOS DEL COLABORADOR

Nombre del colaborador:	**Silvio Humberto López Enríquez C.C: 98.384.388**
Cargo:	**Programador sistemas**
Tipo de contrato:	**Indefinido**
Horario:	**Lunes a sábado**
Departamento o área:	**Sistemas**

ACTIVIDADES A REALIZAR:

"SISTEMA DE MONITOREO EN REDES DE DEDATOS Y ESTADÍSTICA DE ATAQUES EN LA EMPRESA SUNSHINE BOUQUET ZONA NORTE BOGOTÁ COLOMBIA"

ATENTAMENTE

Jefe Área de Sistemas
mtavera@sunshinebouquet.com

http://www.sunshinebouquetcompany.com

14 VERIFICACIÓN FÍSICA Y LÓGICA SISTEMAS DE INFORMACIÓN

La tabla 21 presenta un resumen de cada una de las verificaciones y hallazgos locativos dentro de las red física y lógica de la finca Betania

Tabla 21. Planilla de validación.

SUNSHINE BOUQUET COMPANY		**PLANILLA DE VALIDACIÓN**	
AUDITOR: Silvio Humberto Lopez Enríquez.			
FECHA DE VISITA: Mayo De 2017.			
ALCANCE: Licenciamiento Software			
SERVIDOR	**PROPIETARIO**	**SEDE**	**S. O. INSTALADO**
NOMINA	ASISTEC	BQT	Windows Microsoft Office Enterprise Edition 2007 - B48G
SISFIN	SUNSHINE	BQT	Microsoft Office Professional Edition 2003- GWH28
SISFIN1/BACK UP	ASISTEC	BQT	Windows Microsoft Office Enterprise Edition 2007 - B48G
1. Una vez finalizada la revisión física de la totalidad de los servidores registrados en los documentos de control se evidencio que los siguientes software office instalados no presentan sus licencias respectivas: Una vez realizada la inspección física de los equipos a 39 de los 146 computadores, que se encuentran registrados en el documento de control para los componentes tecnológicos de la compañía Sunshine Bouquet como de propiedad de esta, se identificaron las siguientes situaciones:			

Tabla 21. (continuación).

PLANILLA DE VALIDACIÓN
LICENCIAMIENTO
✓ En 5 computadores se logró evidenciar que el código de la etiqueta no corresponde al sistema operativo que actualmente se encuentra instalado en las maquinas. Estas fueron: o PC-Nomina o PC-Nomina-Aux o PC-Aux- Sena o PC- Contratación o PC-Enfermería-Cultivo ✓ En revisión física realizada a la muestra de computadores licenciados en modalidad CAJA, se identificó que los siguientes códigos de licencia del sistema operativo Windows 7 que actualmente se encuentra instalado en las maquinas, no presentan un soporte legal. o MB8VG-KB3VC-D236C-H82YB-KYRY6 o YQYVG-FR8DB-29J6H-3KBF7-BX286 o 4FXW8-97KD9-QFKDJ-FV3QC-CY34B o DX4MW-PB7F4-YR4WT-BV3MM-4YV79 o BTH8T-MTYCP-4GKX7-3QQQT-86CB6 ✓ Una vez realizada la inspección física del software office en 39 de los 87 computadores, que se encuentran registrados en el documento de control para los componentes tecnológicos de la compañía, se identificó que 3 no presentan licencias de office esto fueron: o PC- Enfermería o PC- Aux-Sena o PC-Aux-Contratación

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN
posible evidenciar que el documento de inventario de software se encuentra desactualizado y en entrevista con el jefe del área de TI se concluyó que, aunque exista una política para la instalación de software no autorizado los usuarios pueden realizar esta actividad. **SEGURIDAD** 2. Una vez realizada la validación del modelo de seguridad para la información de la compañía, se evidencio que en los computadores pertenecientes a: MARIBLE ACUÑA en el cargo de JEFEGH y ESTEBAN HERNANDEZ en el cargo de NOMINA no existe un software de protección antivirus instalado. 3. Una vez revisadas las políticas y en entrevista con el director del área MARIA ESTELA TAVERA y la ingeniera de soporte NIDIA ROMERO, se logró evidenciar una violación a la administración de los equipos, al evidenciarse instalaciones en los usuarios: ANDRÉS MARTÍNEZ y PAOLA MURILLO, de aplicativos como: Facebook Video Calling y Plants vs. Zombies. Los cuales no están autorizados. 4. Una vez realizadas las pruebas desde la red local de la compañía se logró evidenciar el acceso a los siguientes sitios: ✓ Redes sociales: ✓ YouTube ✓ Lovoo ✓ Gotinder ✓ Adoptaunman. ✓ Acceso a correo personal: ✓ Gmail ✓ Contenido Adulto: ✓ Descarga imágenes xxx

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN
5. En revisión física realizada al equipo en el cargo de PLANEACIÓN en la sede BOUQUETERA, se logró evidenciar un acceso al correo personal en la cuenta de Hotmail por parte del funcionario encargado del área. **DATOS** 6. En revisión al desarrollo de las actividades de respaldo para la información de la organización, mediante el uso de la aplicación COBIAN, se logró evidenciar que no existe un proceso documentado para realizar los Backups en la sede principal de la compañía. 7. En verificación a la metodología implementada en los Backups y la disponibilidad de la información salvaguardada, se evidencio que esta solo cubre un periodo no mayor a 1 mes. **ADMINISTRACIÓN Y GESTIÓN** 8. No se maneja una bitácora o mecanismo automatizado que registren las soluciones a los fallos, en los equipos informáticos de la compañía. **9.** Mediante la verificación de los documentos de mantenimientos de los equipos críticos se logró evidenciar que la compañía no maneja mantenimientos de tipo predictivos. **HARDWARE** 10. Una vez realizada la inspección física de los equipos a 80 de los 298 computadores, que se encuentran registrados en el documento de control para los componentes tecnológicos de la compañía, en estos se identificó 1 computador con performance bajos para el desarrollo de sus actividades:

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN
Mediante la inspección física realizada a los puntos de voz y datos del sistema de cableado estructurado de la compañía en las sedes Bouquetera, Betania, Cerezo y Sarama se evidenciaron las siguientes situaciones: 11. No se realiza la marcación para el cableado estructurado en el patch panel de la sede Betania.  12. Falta la marcación para los puntos de voz y datos en todos los puntos en las sedes de Bouquetera, Betania. 

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN
13. Los puntos de vos y datos ubicados en la oficina de ALMACEN a nombre de DANIEL SIEMPIRA en la sede de BETANIA, se encuentran instalados **de forma** inadecuada para su utilización, puesto que ocasionaría en cualquier momento interrupción del servicio al no estar instalado como la norma lo indica y expuesto al daño por el medio ambiente y accidentes.  14. En revisión realizada a algunas canaletas, se logró evidenciar que no se está segmentado los ductos para el cableado eléctrico y el de voz – datos para la Zona de Postcosecha en la sede Cerezo. 

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN
15. Los puntos de voz y datos ubicados en la oficina de SALUD OCUPACIONAL a nombre de ANGELA GUAMÁN en la sede de BBETANIA, se evidencio el mal estado del cable de red, tanto para el ponchado como su estado en la oficina.  **CICLO DE VIDA DEL SERVICIO** En inspección física a los procesos realizados bajo el área de TI y mediante entrevista realizada al director del área MARIA ESTELA TAVERA, se evidenciaron las siguientes situaciones: 16. En el área no existen identificados los servicios prestados dentro de la compañía, ni acuerdos de niveles de servicios tanto para clientes internos (otra área dentro la compañía) como para clientes externos (Proveedores) 17. El área de TI no cuenta con una biblioteca definitiva de medios (DML) donde se almacena las licencias, versiones definitivas y aprobadas de todo el software de los elementos de configuración. 18. No existe un plan de gestión del conocimiento, donde se documenten ideas,

Tabla 22. (continuación).

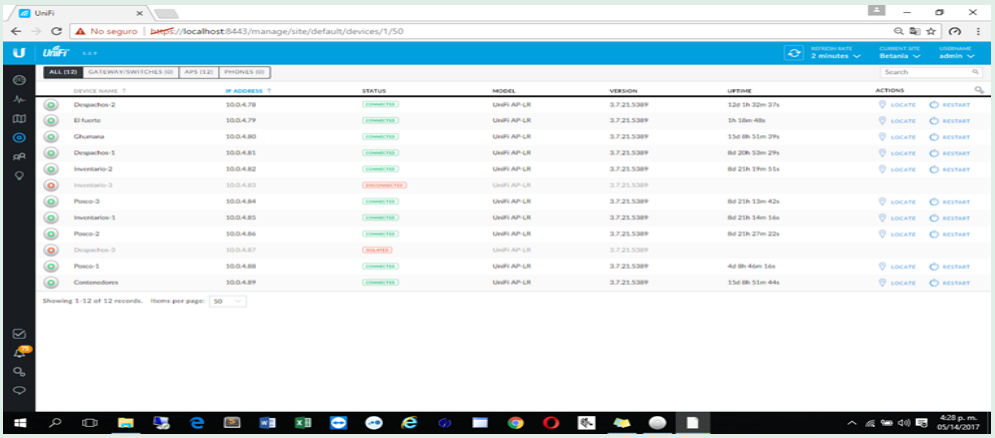
PLANILLA DE VALIDACIÓN
REDES INALAMBRICAS 19. La contraseña de la red inalámbrica cuyo SSID es Ghumana, se evidenció que tiene una contraseña muy débil, “admin3210.    20. La red inalámbrica Betania, esta red consta de 11 dispositivos inalámbricos ubiquiti de la serie UNIFI, se evidencia lo siguiente: Su firmware esta desactualizado, Dos de los dispositivos se encuentra no operativos, uno en estado de insolación y el otro en estado de desconectado. 

Tabla 22. (continuación).

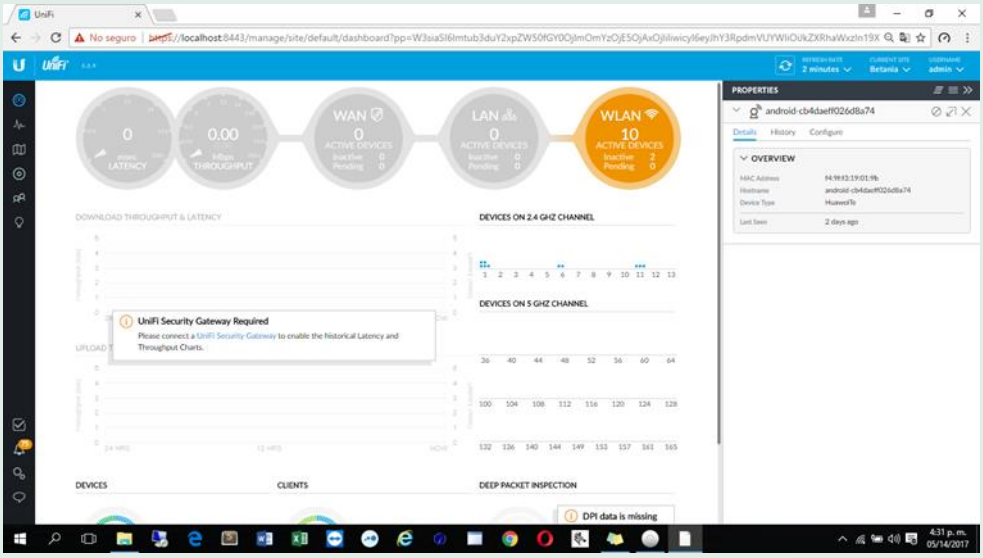
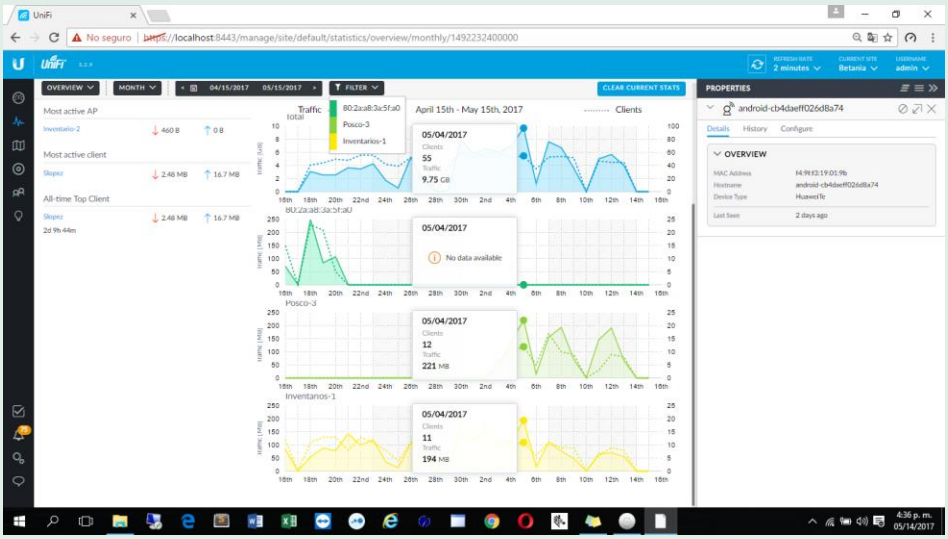
PLANILLA DE VALIDACIÓN
21. La red inalámbrica Betania, esta red consta de 11 dispositivos inalámbricos ubiquiti de la serie UNIFI, se evidencia lo siguiente: ✓ **La red no cuenta con un dispositivo DPI ni filtro de contenido**  22. La red inalámbrica Betania, esta red consta de 11 dispositivos inalámbricos ubiquiti de la serie UNIFI, se evidencia lo siguiente: ✓ **Saturación de la red en horas pico** 

Tabla 22. (continuación).

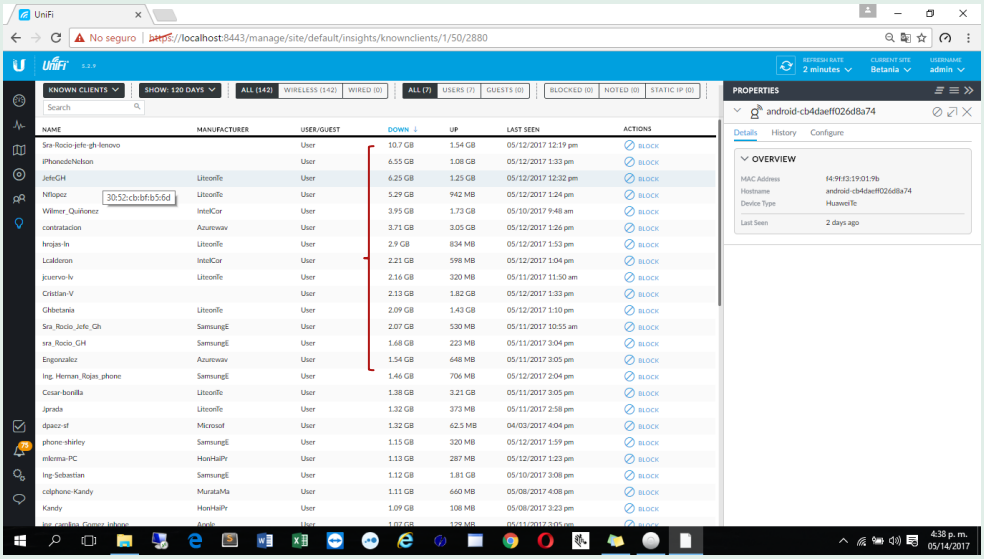
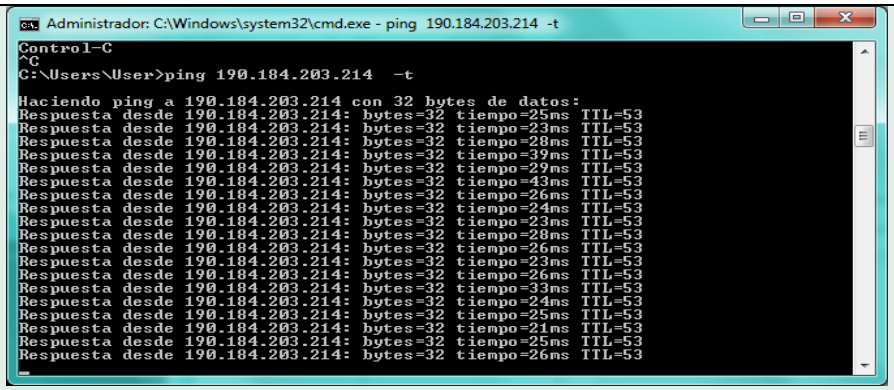
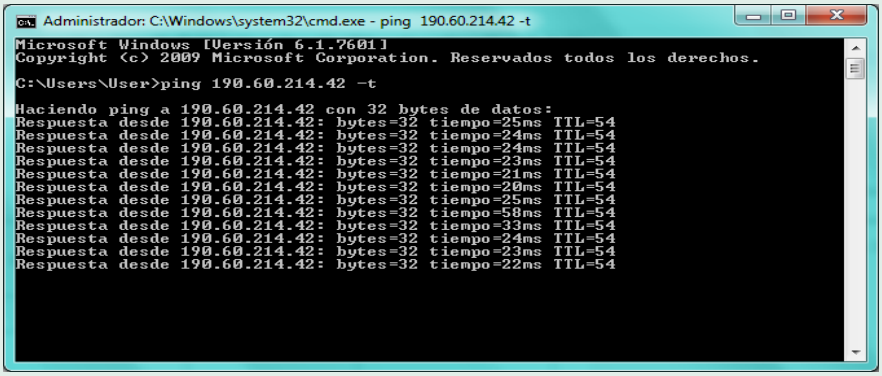
PLANILLA DE VALIDACIÓN
23. La red inalámbrica Betania, esta red consta de 11 dispositivos inalámbricos ubiquiti de la serie UNIFI, se evidencia lo siguiente: ✓ **Algunos usuarios con exceso de descarga, según la política de la compañía estos están restringidos.**  24. La finca Betania cuenta con dos ips públicas: ✓ **http://190.60.214.42/ ifx** ✓ **http://190.184.203.214 hit** las dos responde a ping externo, esto es una falencia ya que aumenta la posibilidad de ataques DDoS

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN





25. La finca Betania haciendo un listado de red, se evidencia carpetas compartidas si ningún tipo de restricción.

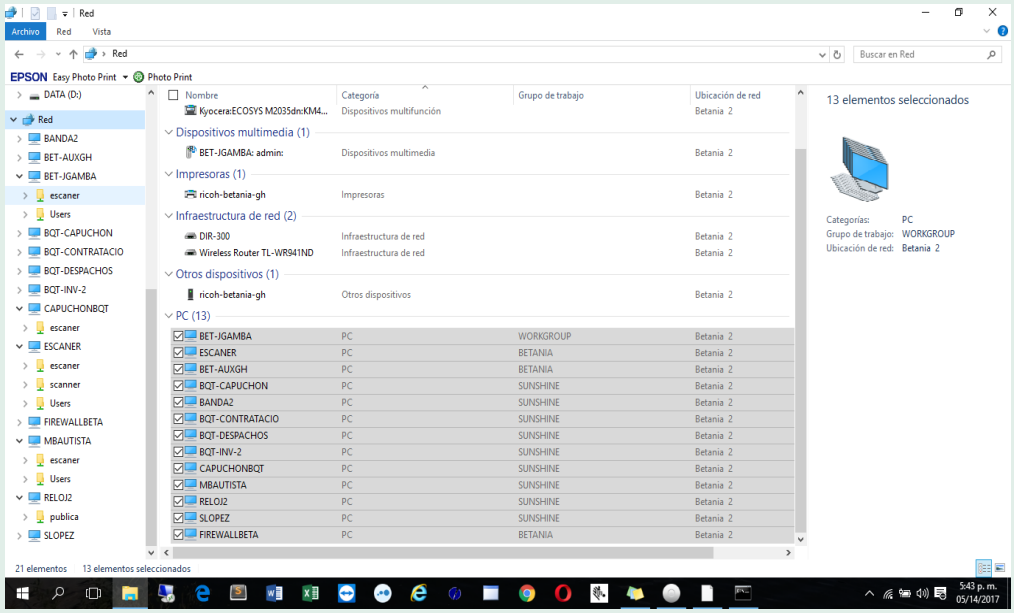


Tabla 22. (continuación).

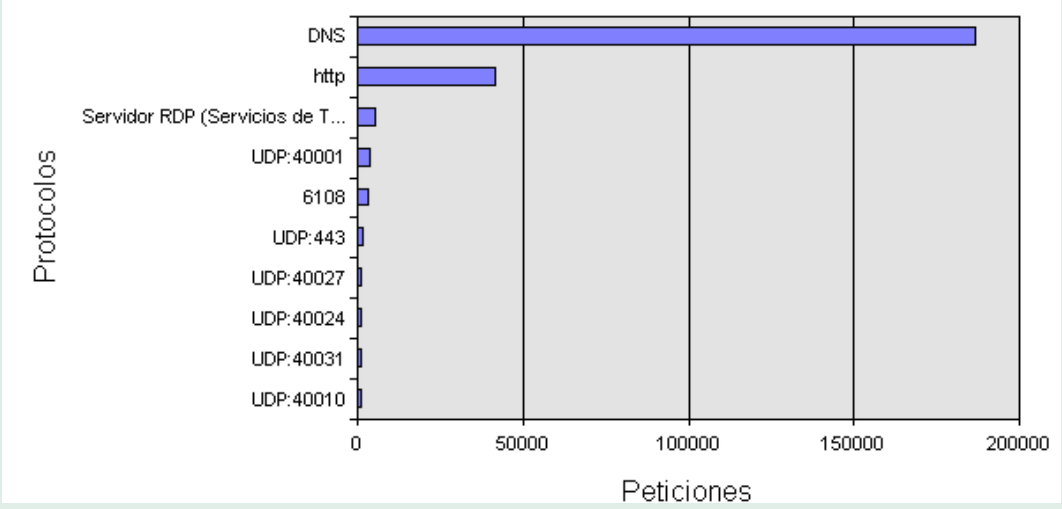
PLANILLA DE VALIDACIÓN

26. Reporte de navegación:

Protocolos

Los siguientes protocolos de comunicación se usaron para conducir tráfico de red a través del servidor. Periodo del informe. 15/05/2017

Los protocolos que se usaron con mayor frecuencia se muestran primero. Este reporte contiene el tráfico tanto de web como el que no es de web.



Núm.	Protocolo	Peticiones	% de número total de peticiones
1	DNS	186731	67,10 %
2	http	41720	15,00 %
3	Servidor RDP (Servicios de Terminal Server)	5190	1,90 %
4	UDP:40001	3534	1,30 %
5	6108	3119	1,10 %
6	UDP:443	1474	0,50 %
7	UDP:40027	1254	0,50 %
8	UDP:40024	1229	0,40 %
9	UDP:40031	1183	0,40 %
10	UDP:40010	1143	0,40 %
11	UDP:40032	1097	0,40 %
12	UDP:40022	1087	0,40 %
13	UDP:40011	1062	0,40 %
14	UDP:40029	1058	0,40 %
15	UDP:40014	1047	0,40 %
	Todo el resto	**26546**	**9,50 %**
	Total	**278474**	**100,00 %**

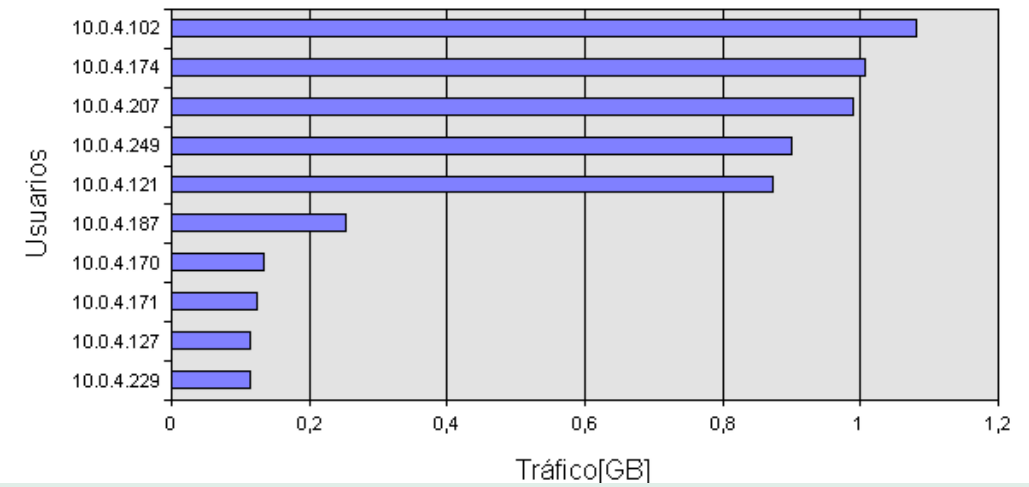
Resumen de protocolo

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN

27. Reporte de usuarios más recurrentes

Los siguientes usuarios generaron la mayor cantidad de tráfico de red, Los usuarios que generaron el mayor tráfico se muestran primero. Las direcciones.



Núm.	Usuario	Peticiones	% de número total de peticiones	Bytes de entrada	% de número total de bytes de entrada	Bytes de salida	% de número total de bytes de salida	Número total de bytes	% de número total de bytes
1	10.0.4.102	14090	5,10 %	1,08 GB	16,20 %	3,42 MB	1,70 %	1,08 GB	15,80 %
2	10.0.4.174	326	0,10 %	0,99 GB	14,90 %	18,10 MB	9,20 %	1,01 GB	14,70 %
3	10.0.4.207	621	0,20 %	993,55 MB	14,60 %	19,48 MB	9,90 %	0,99 GB	14,50 %
4	10.0.4.249	879	0,30 %	903,23 MB	13,30 %	17,81 MB	9,00 %	921,04 MB	13,20 %
5	10.0.4.121	6154	2,20 %	888,76 MB	13,10 %	4,24 MB	2,10 %	893,00 MB	12,80 %
6	10.0.4.187	3248	1,20 %	259,15 MB	3,80 %	639,16 KB	0,30 %	259,78 MB	3,70 %
7	10.0.4.170	2516	0,90 %	134,31 MB	2,00 %	2,76 MB	1,40 %	137,07 MB	2,00 %
8	10.0.4.171	717	0,30 %	122,78 MB	1,80 %	3,49 MB	1,80 %	126,27 MB	1,80 %
9	10.0.4.127	3841	1,40 %	114,02 MB	1,70 %	1,98 MB	1,00 %	116,01 MB	1,70 %
10	10.0.4.229	6532	2,30 %	106,78 MB	1,60 %	8,90 MB	4,50 %	115,68 MB	1,70 %
11	10.0.4.161	2787	1,00 %	109,87 MB	1,60 %	1,65 MB	0,80 %	111,53 MB	1,60 %
12	10.0.4.160	7246	2,60 %	108,88 MB	1,60 %	799,07 KB	0,40 %	109,66 MB	1,60 %
13	10.0.4.114	1222	0,40 %	94,85 MB	1,40 %	1,03 MB	0,50 %	95,88 MB	1,40 %
14	10.0.4.129	26135	9,40 %	83,95 MB	1,20 %	4,31 MB	2,20 %	88,25 MB	1,30 %
15	192.240.114.82	4368	1,60 %	69,76 MB	1,00 %	12,18 MB	6,20 %	81,94 MB	1,20 %
	Todo el resto	**197792**	**71,00 %**	**697,19 MB**	**10,20 %**	**96,48 MB**	**48,90 %**	**793,67 MB**	**11,30 %**
	Total	**278474**	**100,00 %**	**6,65 GB**	**100,00 %**	**197,24 MB**	**100,00 %**	**6,84 GB**	**100,00 %**

Resumen de usuarios más frecuentes

28. Sitios web más frecuentes

Los siguientes sitios web fueron los solicitados con mayor frecuencia por los clientes, durante el periodo del informe. Los sitios web más visitados se muestran primero.

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN

Núm.	Sitio	Usuarios únicos	Peticiones	% de número total de peticiones	Bytes de entrada	% de número total de bytes de entrada	Bytes de salida	% de número total de bytes de salida	Número total de bytes	% de número total de bytes
1	69.16.233.171	23	10831	26,00 %	531,34 MB	16,50 %	22,25 MB	42,70 %	553,59 MB	16,90 %
2	190.144.156.101	14	10720	25,70 %	123,05 MB	3,80 %	20,75 MB	39,80 %	143,79 MB	4,40 %
3	204.79.197.223	7	7876	18,90 %	1,18 GB	37,50 %	1,68 MB	3,20 %	1,18 GB	37,00 %
4	104.91.153.222	29	2775	6,70 %	849,96 KB	0,00 %	472,89 KB	0,90 %	1,29 MB	0,00 %
5	23.32.195.20	16	1313	3,10 %	408,90 KB	0,00 %	231,56 KB	0,40 %	640,46 KB	0,00 %
6	54.213.30.144	2	342	0,80 %	8,49 MB	0,30 %	184,17 KB	0,30 %	8,67 MB	0,30 %
7	104.91.150.3	23	250	0,60 %	66,50 KB	0,00 %	434,63 KB	0,80 %	501,12 KB	0,00 %
8	23.32.192.108	35	195	0,50 %	56,71 KB	0,00 %	293,29 KB	0,50 %	350,00 KB	0,00 %
9	35.165.107.206	2	182	0,40 %	4,72 MB	0,10 %	137,74 KB	0,30 %	4,85 MB	0,10 %
10	40.87.63.92	6	164	0,40 %	331,17 KB	0,00 %	306,01 KB	0,60 %	637,18 KB	0,00 %
11	23.67.17.91	23	163	0,40 %	501,15 KB	0,00 %	34,68 KB	0,10 %	535,83 KB	0,00 %
12	190.60.67.59	5	159	0,40 %	3,14 MB	0,10 %	345,22 KB	0,60 %	3,47 MB	0,10 %
13	104.91.145.83	14	156	0,40 %	47,88 KB	0,00 %	42,07 KB	0,10 %	89,95 KB	0,00 %
14	62.82.203.70	1	155	0,40 %	2,83 MB	0,10 %	83,40 KB	0,20 %	2,91 MB	0,10 %
15	23.32.206.20	14	154	0,40 %	46,31 KB	0,00 %	42,14 KB	0,10 %	88,45 KB	0,00 %
	Todo el resto		**6285**	**15,10 %**	**1,31 GB**	**41,60 %**	**4,85 MB**	**9,30 %**	**1,32 GB**	**41,00 %**
	Total	**65**	**41720**	**100,00 %**	**3,15 GB**	**100,00 %**	**52,09 MB**	**100,00 %**	**3,20 GB**	**100,00 %**

Resumen de sitios web más frecuentes

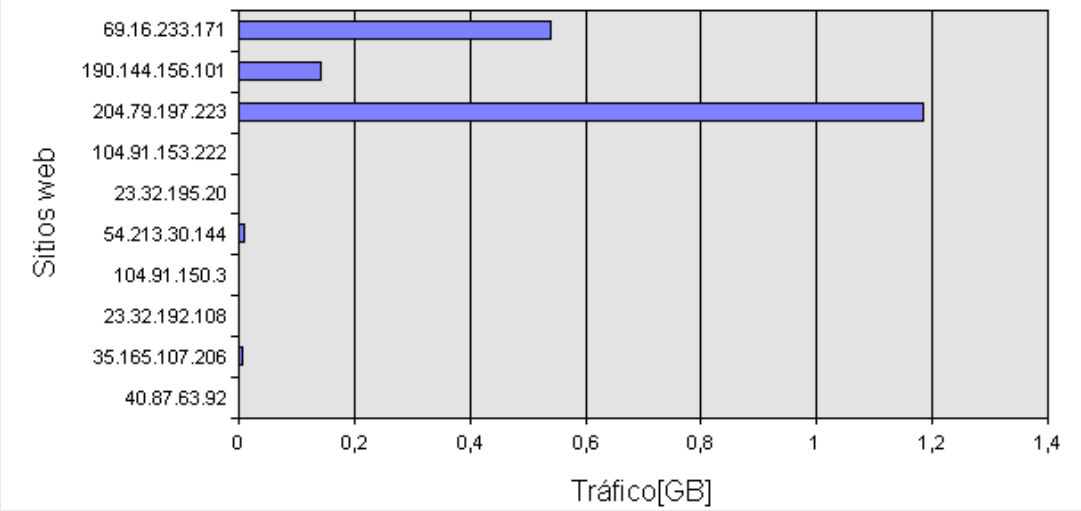


Tabla 22. (continuación).

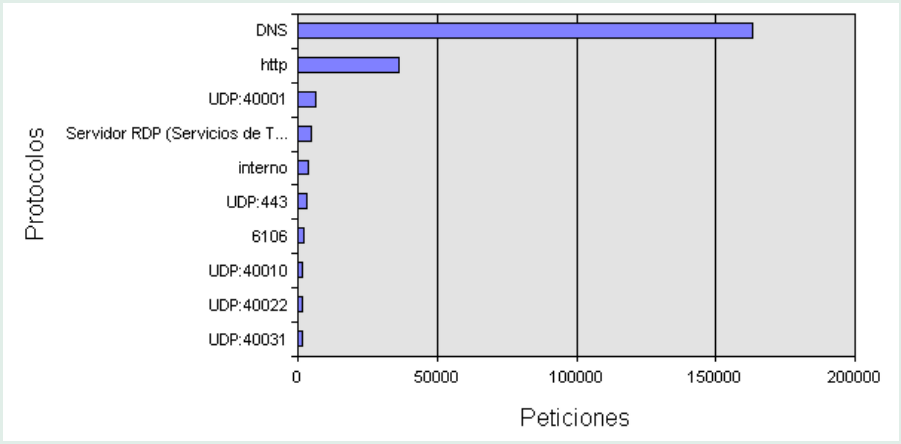
PLANILLA DE VALIDACIÓN

28. Reporte de navegación

Periodo del informe. 15/05/2017

Protocolos

Los siguientes protocolos de comunicación se usaron para conducir tráfico de red a través del servidor.



Núm.	Protocolo	Peticiones	% de número total de peticiones
1	DNS	163287	61,10 %
2	http	36523	13,70 %
3	UDP:40001	6259	2,30 %
4	Servidor RDP (Servicios de Terminal Server)	4902	1,80 %
5	interno	3829	1,40 %
6	UDP:443	3005	1,10 %
7	6106	1904	0,70 %
8	UDP:40010	1667	0,60 %
9	UDP:40022	1660	0,60 %
10	UDP:40031	1622	0,60 %
11	UDP:40024	1585	0,60 %
12	UDP:40012	1571	0,60 %
13	UDP:40002	1557	0,60 %
14	UDP:40034	1523	0,60 %
15	UDP:40013	1430	0,50 %
	Todo el resto	**34715**	**13,00 %**
	Total	**267039**	**100,00 %**

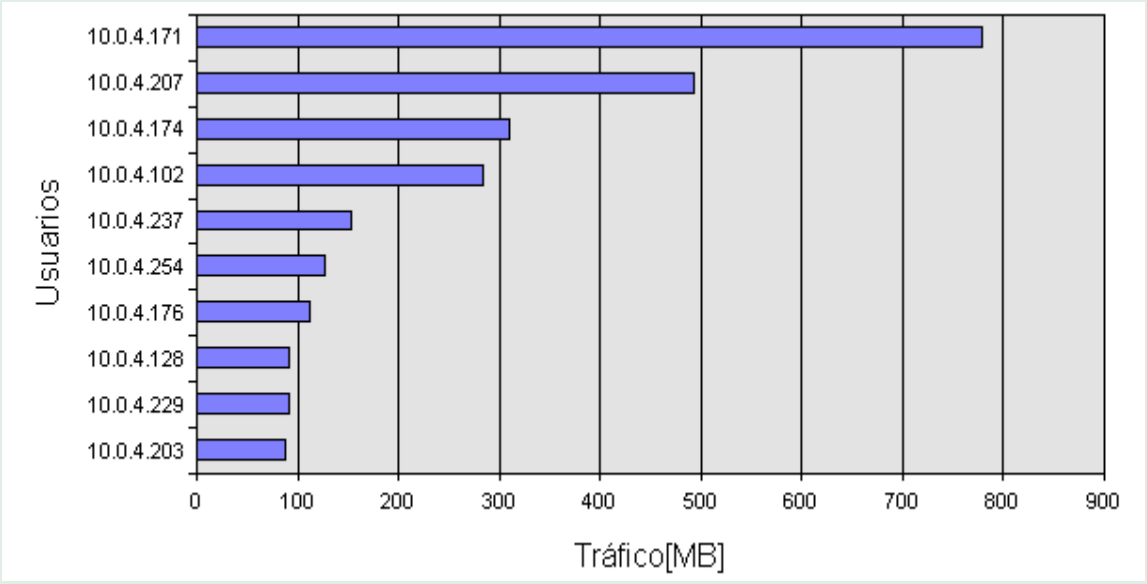
Resumen de protocolo

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN

28. Usuarios más frecuentes

Los siguientes usuarios generaron la mayor cantidad de tráfico de red a través del servidor, durante el periodo del informe.



Núm.	Usuario	Peticiones	% de número total de peticiones	Bytes de entrada	% de número total de bytes de entrada	Bytes de salida	% de número total de bytes de salida	Número total de bytes	% de número total de bytes
1	10.0.4.171	634	0,20 %	763,53 MB	22,80 %	15,75 MB	6,40 %	779,28 MB	21,60 %
2	10.0.4.207	853	0,30 %	481,30 MB	14,30 %	11,14 MB	4,50 %	492,44 MB	13,70 %
3	10.0.4.174	260	0,10 %	302,02 MB	9,00 %	8,04 MB	3,30 %	310,06 MB	8,60 %
4	10.0.4.102	25747	9,60 %	274,54 MB	8,20 %	8,56 MB	3,50 %	283,11 MB	7,90 %
5	10.0.4.237	2046	0,80 %	152,88 MB	4,60 %	403,71 KB	0,20 %	153,28 MB	4,30 %
6	10.0.4.254	11545	4,30 %	123,74 MB	3,70 %	2,75 MB	1,10 %	126,49 MB	3,50 %
7	10.0.4.176	2340	0,90 %	70,45 MB	2,10 %	41,30 MB	16,70 %	111,75 MB	3,10 %
8	10.0.4.128	5658	2,10 %	85,46 MB	2,50 %	5,90 MB	2,40 %	91,37 MB	2,50 %
9	10.0.4.229	5786	2,20 %	85,23 MB	2,50 %	5,67 MB	2,30 %	90,90 MB	2,50 %
10	10.0.4.203	5632	2,10 %	75,77 MB	2,30 %	12,84 MB	5,20 %	88,60 MB	2,50 %
11	10.0.4.240	2794	1,00 %	67,92 MB	2,00 %	15,25 MB	6,20 %	83,17 MB	2,30 %
12	10.0.4.127	2887	1,10 %	78,59 MB	2,30 %	2,90 MB	1,20 %	81,49 MB	2,30 %
13	10.0.4.120	531	0,20 %	79,01 MB	2,40 %	126,84 KB	0,10 %	79,14 MB	2,20 %
14	10.0.4.121	1282	0,50 %	61,42 MB	1,80 %	10,05 MB	4,10 %	71,47 MB	2,00 %
15	10.0.4.129	21869	8,20 %	60,68 MB	1,80 %	3,33 MB	1,30 %	64,01 MB	1,80 %
	Todo el resto	**177175**	**66,30 %**	**593,60 MB**	**17,70 %**	**102,86 MB**	**41,70 %**	**696,46 MB**	**19,30 %**
	Total	**267039**	**100,00 %**	**3,28 GB**	**100,00 %**	**246,86 MB**	**100,00 %**	**3,52 GB**	**100,00 %**

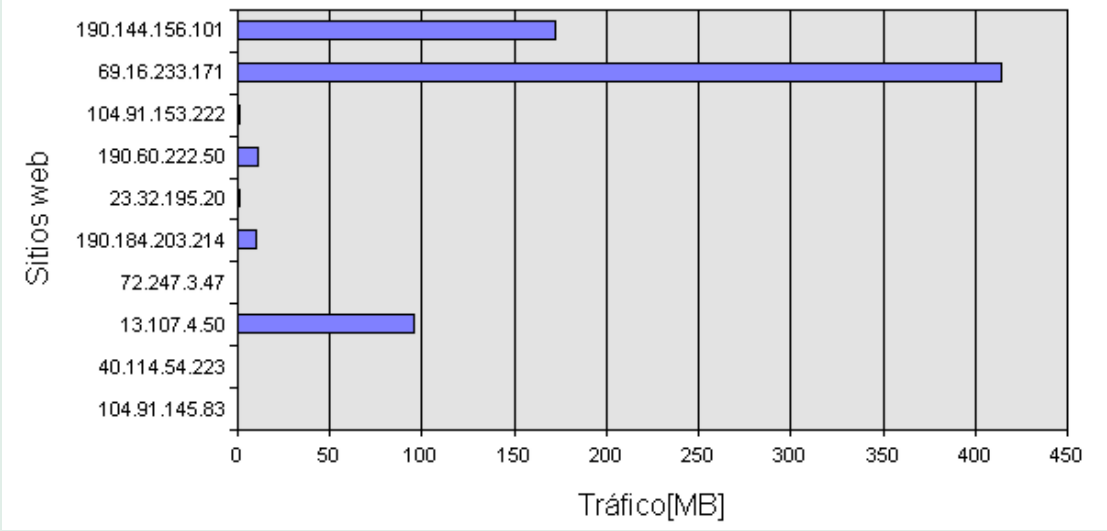
Resumen de usuarios más frecuentes

Tabla 22. (continuación).

PLANILLA DE VALIDACIÓN

29. Sitios web más frecuentes

Los siguientes sitios web fueron los solicitados con mayor frecuencia por los usuarios, durante el periodo del informe.



Núm.	Sitio	Usuarios únicos	Peticiones	% de número total de peticiones	Bytes de entrada	% de número total de bytes de entrada	Bytes de salida	% de número total de bytes de salida	Número total de bytes	% de número total de bytes
1	69.16.233.171	22	8368	22,90 %	394,56 MB	31,80 %	20,08 MB	35,10 %	414,64 MB	31,90 %
2	190.144.156.101	11	16236	44,50 %	145,87 MB	11,80 %	26,80 MB	46,90 %	172,67 MB	13,30 %
3	190.25.210.90	4	31	0,10 %	142,75 MB	11,50 %	4,77 KB	0,00 %	142,76 MB	11,00 %
4	200.25.54.146	2	7	0,00 %	111,16 MB	9,00 %	1,30 KB	0,00 %	111,16 MB	8,60 %
5	13.107.4.50	4	236	0,60 %	95,30 MB	7,70 %	80,77 KB	0,10 %	95,38 MB	7,30 %
6	190.25.210.75	10	99	0,30 %	43,11 MB	3,50 %	25,29 KB	0,00 %	43,14 MB	3,30 %
7	8.253.165.248	1	37	0,10 %	33,01 MB	2,70 %	13,55 KB	0,00 %	33,02 MB	2,50 %
8	8.253.183.248	1	34	0,10 %	32,03 MB	2,60 %	12,63 KB	0,00 %	32,04 MB	2,50 %
9	8.254.248.110	1	33	0,10 %	30,94 MB	2,50 %	12,26 KB	0,00 %	30,95 MB	2,40 %
10	8.253.149.120	1	27	0,10 %	27,02 MB	2,20 %	10,08 KB	0,00 %	27,03 MB	2,10 %
11	200.25.54.24	1	47	0,10 %	26,52 MB	2,10 %	16,61 KB	0,00 %	26,54 MB	2,00 %
12	200.25.54.155	1	34	0,10 %	21,42 MB	1,70 %	10,21 KB	0,00 %	21,43 MB	1,70 %
13	200.69.125.178	3	13	0,00 %	13,39 MB	1,10 %	2,75 KB	0,00 %	13,39 MB	1,00 %
14	72.247.240.99	1	3	0,00 %	11,16 MB	0,90 %	661,00 N	0,00 %	11,16 MB	0,90 %
15	190.60.222.50	6	1308	3,60 %	9,62 MB	0,80 %	1,11 MB	1,90 %	10,73 MB	0,80 %
	Todo el resto		**10010**	**27,40 %**	**102,76 MB**	**8,30 %**	**9,02 MB**	**15,80 %**	**111,78 MB**	**8,60 %**
	Total	**69**	**36523**	**100,00 %**	**1,21 GB**	**100,00 %**	**57,20 MB**	**100,00 %**	**1,27 GB**	**100,00 %**

Resumen de sitios web más frecuentes

La tabla 23 presenta un resumen de una prueba de Etical Haccking la cual fue realizada en las instalaciones de la finca Betania.

Tabla 223 Pen Testing

Pen Testing
Objetivo: Presentar los servicios de Ethical Hacking, con el fin de revisar los niveles de seguridad actuales en la red de datos de Sunshine Bouquet Zona Norte". Realizar el análisis de vulnerabilidades y Ethical Hacking, interno y externo para los servidores de Isa Server y Sisfin, los cuales se encuentran alojados en la Finca Betania (esta finca hace parte de la Zona norte), en busca de posibles fallos de seguridad. **Alcance:** La Propuesta que se presenta el servicio integral de Hacking Ético a los sistemas Operativos de Ubuntu, y Windows server 2008 para realizar pruebas y verificaciones de seguridad correspondientes. Incluye la identificación de vulnerabilidades, usando la ayuda de Kali Linux, Nessus, Nmap, Nping, Ncrack **Recolección de Información.** Los ataques se llevaron a cabo con el nivel de acceso de usuario que la compañía tiene definido como estándar, es decir sin privilegios, y con restricciones de navegación en internet, la evaluación se llevó a cabo de acuerdo con las recomendaciones formuladas en el NIST SP 800-1151. Se utilizaron dos formas: ✓ El uso de aplicaciones ✓ Ingeniería social: es decir usando recurso humano implicado Así que el primer paso es hacer un escaneo de las redes, cableado e inalámbricas **Identificación de objetivos.** Sunshine Bouquet Zona Norte, has dispuesto para la realización de las de Pen Test, los siguientes servidores. **Técnicas y herramientas.** Se contará con la aplicación de metodologías de OWASP e ISSAF y las recomendaciones formuladas en el NIST SP 800-1151. La información obtenida de esta exploración de vulnerabilidades sirve para implementar correcciones y controles a los sistemas permitiéndoles ser más seguros**.**

Tabla 233 Pen Testing (Continuación)

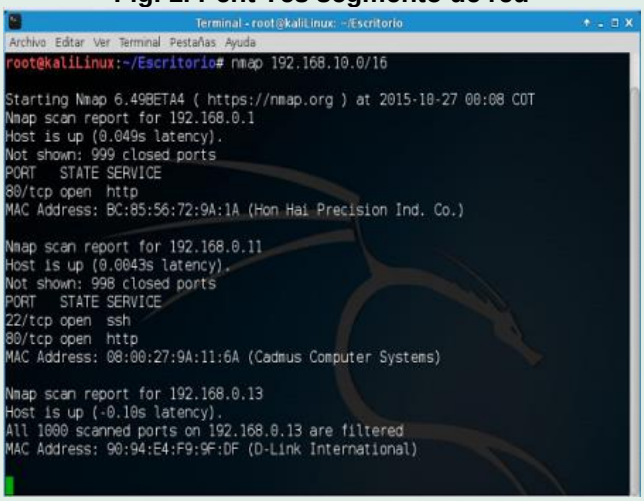
Pen Testing
Análisis de Vulnerabilidades. Análisis básico automatizado de las vulnerabilidades externas sobre IP 192.168.0.11basados en las siguientes herramientas: **Test de vulnerabilidades** *NMAP* ("Network Mapper"): Herramienta para exploración de redes y puertos y de sondeo de seguridad e inventario de la red. *NESSUS:* Aplicación de escaneo de vulnerabilidades para sistemas operativos, y exploits, el cual intenta realizar varios ataques de manera automática. **Ataque.** **Detección de Red.** Reconocimiento. Se recolectó información por medio del escaneo del segmento de red con el comando: nmap 192.168.0.0/16. También se puede realizar el escaneo de equipo de manera individual. Cabe resaltar que en esta fase no se busca encontrar ninguna vulnerabilidad en absoluto, lo que se pretende es obtener la mayor cantidad posible de equipos que la red objetivo tiene con presencia en internet. **Fig. 1. Pent Tes segmento de red**  **Fuente: El Autor**

Tabla 243 Pen Testing (Continuación)

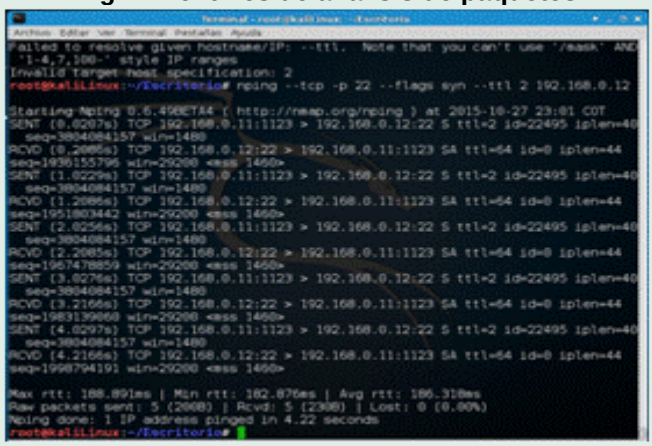
Pen Testing
Detección de servicios. Escanear modo TCP (-tcp) para sondear el puerto 22 (p 22) utilizando el flag SYN (-flags sin) con un TTL de 2 (-ttl 2) en el host remoto (192.168.0.12) comando: “nping --tcp -p 22 --flags syn --ttl 2 192.168.0.11” **Fig. 2. Pent Tes de análisis de paquetes**  **Fuente: El Autor** **Barridos de puertos TCP y UDP** Se examinaron los puertos y servicios de cada uno de estos equipos y con base en el tipo de servicios que ofrecen, se realizará inferencia sobre el papel que cada uno juega dentro de la red objetivo. Se Escaneo en modo detallado (-v), permitir la detección del sistema operativo, la detección de versiones, la exploración de la escritura, y traceroute (-A), con detección de versiones (sV) contra la IP de destino (192.168.0.12) comando: “nmap -v -A -sV 192.168.0.12”

Tabla 253 Pen Testing (Continuación)

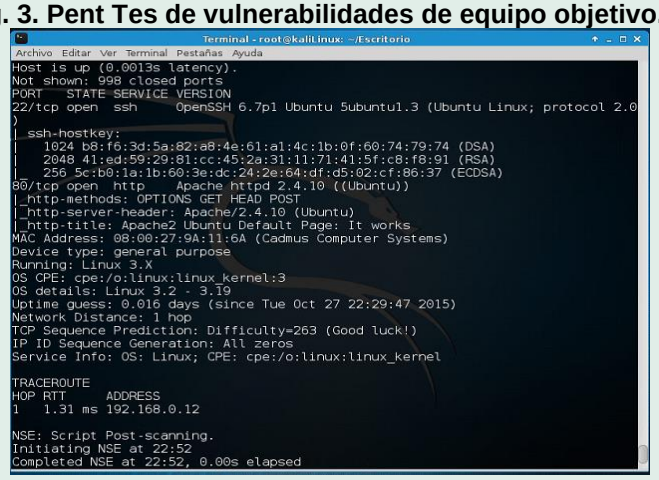
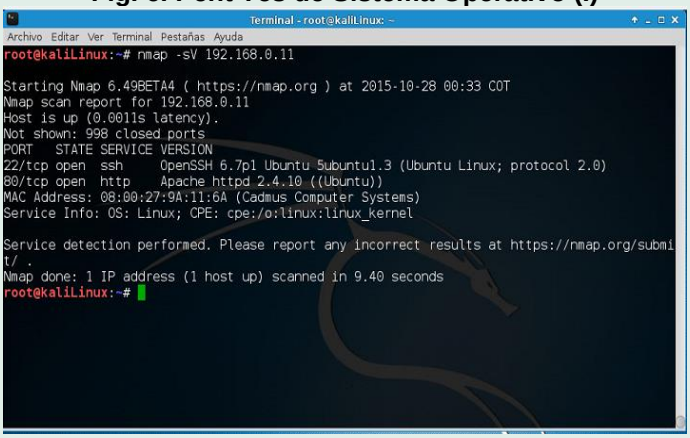
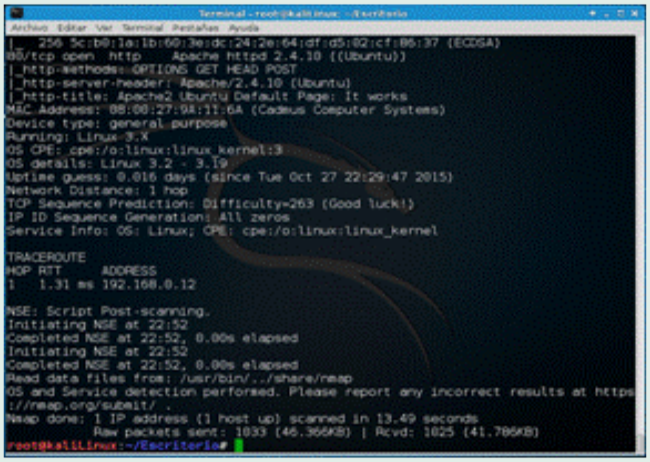
Pen Testing
Fig. 3. Pent Tes de vulnerabilidades de equipo objetivo. (I)    **Fuente: El Autor** Se escaneo con opción “-sV” de nmap habilita la detección de versión. Después de descubrir los puertos TCP y UDP utilizando algunos de los escaneos proporcionados por nmap, la detección de versión interroga estos puertos para determinar más sobre lo que está actualmente en funcionamiento con el comando: # “nmap -sV 192.168.0.11” **Fig. 6. Pent Tes de Sistema Operativo (I)**    **Fuente: El Autor** **Detección de Sistema Operativo.** Se determino los equipos críticos de la red objetivo a los cuales se les aplicará el procedimiento que se describe en la fase de la siguiente sección.

Tabla 263 Pen Testing (Continuación)

Pen Testing

Fig. 5. Pent Tes de vulnerabilidades de equipo objetivo. (II)

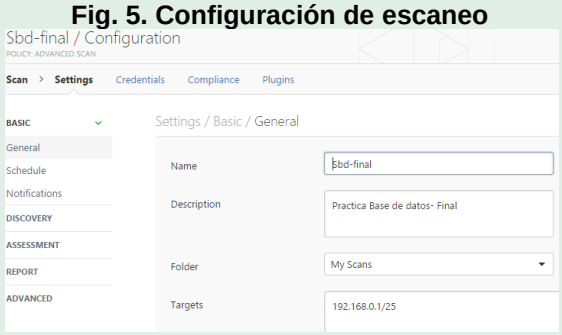


Fuente: El Autor

Escaneo de la Red

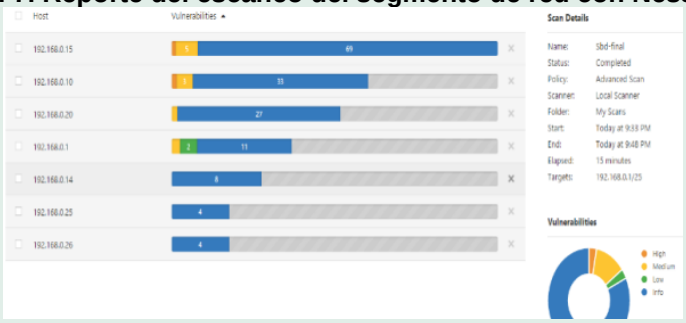
Se realizó escaneo de la red con Nessus Sacan en la siguiente segmentación: 192.168.0.1/25

Fig. 5. Configuración de escaneo



Fuente: El Autor

Fig. 7. Reporte del escaneo del segmento de red con Nessus



Fuente: El Autor

Tabla 273 Pen Testing (Continuación)

Pen Testing
Ataque de Hombre en el medio, más conocido como MiTM ‘’Man In The Middle Mobile’’ El ataque hombre en la mitad del inglés (“man-in-the-middle sigla MiTM) es considerado como uno del os ataques tipo básico. Su fuerte radica en que las víctimas no suelen darse cuenta de su presencia, ya que se trata de una forma de ataque silencioso. **MiTM** tiene algunas variantes: Rogue APs, conexiones wifi que falsifican los accesos legítimos para que el usuario se conecte y se puedan interceptar sus comunicaciones. Heartbleed, un bug en OpenSSL que hace que los ataques de man-in-the-middle puedan prolongar su alcance. SSL, utilizan autenticaciones end-to-end, creadas específicamente para prevenir ataques MiTM. El Heartbleed, al comprometer esta función del SSL, deja la puerta abierta para el man-in-the-middle. Ejecutando el websploit, se escribe en la consola el siguiente comando y “websploit” luego se pulsa la tecla enter, como se indica en la figura- **Fig. 8. Configuración de Websploit**  **Fuente: El Autor**

Tabla 283 Pen Testing (Continuación)

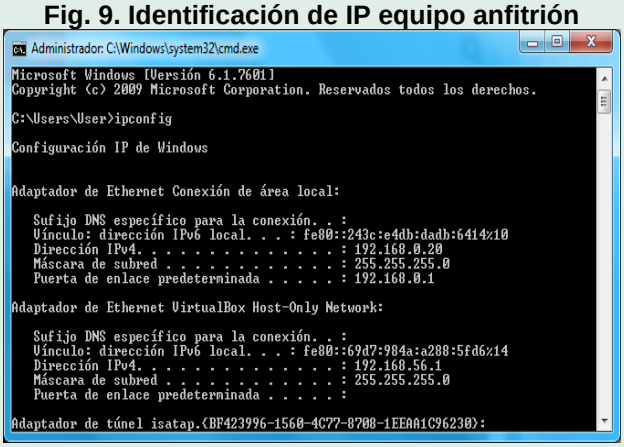
Pen Testing
Iniciamos el ataque MiTM, se hace con el comando “use network/mitm” Averiguando la ip de nuestro Router: para averiguarlo sigue estos pasos: inicio/ejecutar… allí escriba cmd y pulse la tecla enter, ya en la consola de Windows digite “ipconfig” y pulse la tecla enter. **Fig. 9. Identificación de IP equipo anfitrión**  **Fuente: El Autor** Indicamos la ip de nuestro Router con el siguiente comando: “set Router 192.xxx.xxx.xxx” Indicamos la dirección ip de la víctima con el siguiente comendo: “set público 192.168.0.20” Activamos el esniffer con el siguiente comando: “set sniffer dsniff”, ver imagen siguiente **Fig. 10. Configuración de Websploit**  **Fuente: El Autor**

Tabla 293 Pen Testing (Continuación)

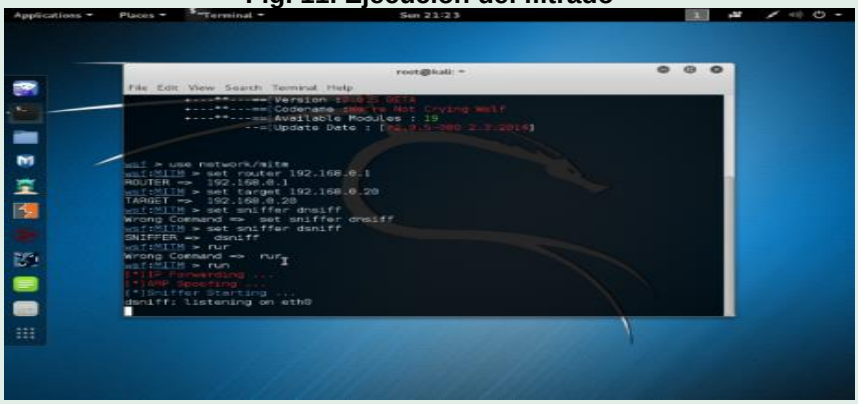
Pen Testing
Ejecutamos la aplicación para comenzar el filtrado de contenido: se hace con el comando “run” **Fig. 11. Ejecución del filtrado**  **Fuente: El Autor** De aquí en adelante toda actividad que haga el usuario del equipo atacado y que implique usar la tarjeta de red, pasará por nuestro esniffer y será guardado en un log con el nombre de “sslstrip.log” (Abriendo el archivo sslstrip. lo) **Fig. 12. Procesos de sniffer**  **Fuente: El Autor**

Tabla 303 Pen Testing (Continuación)

Pen Testing
Para el ejercicio abro Hotmail e ingresé a mi cuenta. **Fig. 13 Ingreso a cuenta**  **Fuente: El Autor** **Haciendo test a la bd MYSQL con SQLmap** Ingresando a SQLmap, por inicio y ejecutar, se pude combinar la tecla de Windows más la r, allí escribimos “cmd” luego enter, salimos del directorio por defecto con el comando “cd..” cuantas veces sean necesarias, hasta llegar al prom “c:|\>” una vez allí ingresaremos al directorio en el que se ha descomprimido SQLmap, en mi caso le llame “sqlmap”, así que ingresare de la siguiente forma: “cd sqlmap” “SQLmap, sqlmap.py –u ip víctima –ddbs” La herramienta auditara el sitio y comprobara si es vulnerable, de serlo mostrara el nombre de las bases de datos. Una vez con esta información procedemos a ver las tablas de esa base de datos “sqlmap.py -u 192.168.56.101 –dbs” Este comando muestra un listado can cada una de las tablas disponibles en la BD. sqlmap.py -u 192.168.56.101 -D usuarios --tables Ahora se requiere saber la estructura de la tabla usuarios, para ello usaremos el siguiente comando: “sqlmap.py -u 192.168.56.101/registro.php -D usuarios --table -T fonep_usuarios –columns”

Tabla 313 Pen Testing (Continuación)

Pen Testing
Fig. 14. Identificación de tablas de bd  **Fuente: El Autor** Hemos avanzado al punto en que ya solo queda ver el contenido de la tabla usuarios, lo haremos con el siguiente comando: "sqlmap.py -u 192.168.56.101/registro.php -D usuarios -T usuarios_usuarios –dump" Uniscan es un escáner de vulnerabilidades que puede explorar sitios web y aplicaciones web para diversos problemas de seguridad como LFI, RFI, inyección SQL, XSS etc. Para este caso se usó el programa que esta predeterminado en la Kali Linux **Fig. 15. Identificación de tablas de bd**  **Fuente: El Autor**

Tabla 323 Pen Testing (Continuación)

Pen Testing
Fig. 16. Identificación y serialización de la web  **Fuente: El Autor** **Resumen Ejecutivo** Se tuvo en cuenta la Metodología para la gestión de Riesgos MAGERIT. Se determinan 3 modelos derivados que son: *Elementos:* contempla los activos de la empresa, las amenazas que se pueden presentar, las vulnerabilidades que están presentes, el impacto que puede tener una vulnerabilidad, los riesgos a los cuales se expone la compañía y los controles que se deben ejercer. *Eventos:* contempla la interrelación de cada uno de los elementos y de la misma manera el modo en el que se relacionan. *Procesos*: contempla cada paso en la planificación y gestión en donde vemos en primer lugar la planificación, seguidamente tenemos el análisis de riesgos y la gestión de riesgos, finalizando con las medidas de control estipuladas para cada riesgo. Para la presentación de los resultados del siguiente análisis, se establecen el siguiente nivel de riesgo en la evaluación de vulnerabilidades encontradas: *Nivel de riesgo Alto:* Fallas de Seguridad que proporcionan información clara para acceder al sistema, o permite el acceso directo al mismo.

Tabla 333 Pen Testing (Continuación)

Pen Testing

Nivel de riesgo medio: Fallas de seguridad que proporcionan información del sistema que podrían facilitar el acceso al mismo, utilizando técnicas de exploración y convirtiendo la falla en una de nivel más alto.

Nivel de riesgo bajo: Fallas de seguridad que de por sí solas no comprometen la seguridad del sistema analizado, pero combinando con otras fallas y utilizando técnicas de explotación podría aumentar el nivel de Riesgo a medio o alto.

Las Vulnerabilidades identificadas corresponden a:

Nivel de riesgo	Total
Alto	4
Medio	4
Bajo	3

Hallazgos

A continuación, se relacionan los hallazgos los cuales serán presentados según la importancia del nivel del riesgo.

ID	**001**	**Nivel**	**Alto**
Descripción del Hallazgo	Contraseñas débiles: Permite la creación de usuarios con contraseñas débiles, esto podría ocasionar que un atacante realice un ataque de fuerza bruta con muchas posibilidades de éxito.		
Recomendaciones	Se recomienda el uso de contraseñas con una longitud mínima de ocho caracteres para usuarios y para administradores de 16. Además, debe estar compuesta por números, letras y símbolos. Esto con el fin de incrementar la dificultar de un ataque.		

ID	**002**	**Nivel**	**Alto**
Descripción del Hallazgo	DoS en la versión de Apache. La versión actual de apache que se encuentra instalada en el servidor contiene múltiples vulnerabilidades que pueden llegar a comprometer la seguridad del servidor causando denegación del servicio.		
Recomendaciones	Actualizar a la última versión de Apache		

Tabla 343 Pen Testing (Continuación)

Pen Testing			
ID	**003**	**Nivel**	**Alto**
Descripción del hallazgo	Finca Betania, dispone de un servidor firewall, isa Server 2008, se trata de una tecnología obsoleta, tanto el sistema operativo como isa server		
Recomendaciones	la recomendación es hacer cambio, por un firewall administrable de última generación		
ID	**004**	**Nivel**	**Alto**
Descripción del hallazgo	La base de datos de Oracle muestra claramente que no está encriptada y actualizaciones obsoletas		
Recomendaciones	Como primera medida usar algoritmo de encriptación y configurar el update automático		
ID	**005**	**Nivel**	**Alto**
Descripción del hallazgo	En cuanto a la base de datos MYSQL, está totalmente desprotegida, no solo la base de datos, también se evidencia la tabla de usuarios el campo de la contraseña hay algunas que no están encriptadas		
Recomendaciones	Encriptar tano la base como loas contraseñas de la tabla usuarios,		
ID	**006**	**Nivel**	**Medio**
Descripción del Hallazgo	Implementación de Métodos no seguros. El servidor tiene activos los métodos de TRACER,		
Recomendaciones	Implementar métodos de petición seguros y deshabilitar los no seguros.		
ID	**007**	**Nivel**	**Medio**
Descripción del Hallazgo	Fuga de información en versión es de aplicación. Mediante la herramienta nmap se obtuvo información exacta de la versión de Apache 2.4.10, facilitando la búsqueda de vulnerabilidades publicadas asociadas que permitan tener acceso al sistema.		
Recomendaciones	Actualizar Ubuntu		
ID	**008**	**Nivel**	**Medio**
Descripción del Hallazgo	Fuga de información en versión es de aplicación. Mediante la herramienta nmap se obtuvo información exacta de la versión de Ubuntu 5.0, facilitando la búsqueda de vulnerabilidades publicadas asociadas que permitan tener acceso al sistema.		
Recomendaciones	Actualizar Apache.		

Tabla 353 Pen Testing (Continuación)

Pen Testing			
ID	**009**	**Nivel**	**Medio**
Descripción del hallazgo	Varios computadores los cuales hacen parte de la red, tienen sistemas operativos Windows XP, se sabe que Windows XP, ya no tiene actualizaciones por parte de Microsoft		
Recomendaciones	Actualizar sistemas Operativos		

ID	**010**	**Nivel**	**Bajo**
Descripción del Hallazgo	Biblioteca OpenSSL. Existen vulnerabilidades en la biblioteca OpenSSL que afectan Apache. Es importante verificar que se está utilizando la versión más reciente de OpenSSL y todos los productos que utilizan OpenSSL para el cifrado de la información utilicen esta versión más moderna.		
Recomendaciones	Actualización de OpenSSL		

ID	**012**	**Nivel**	**Bajo**
Descripción del hallazgo	La red inalámbrica de gestión humana está configurada con seguridad spk,		
Recomendaciones	Configurarla por filtrado MAC		

ID	**013**	**Nivel**	**Bajo**
Descripción del hallazgo	Se identificaron vulnerabilidades en el servidor web Apache ya que implemente por defecto funciones php Obsoletas		
Recomendaciones	Deshabilitar la directiva magic_quotes_gpc ya que ha sido eliminada a desde la versión 5.4.0.		

ID	**IP**	**Descripción**
Isa Server	192.168.0.11	Exploración de vulnerabilidades sin implementación de reglas de acceso interno. Pruebas de Caja Negra.
Ubuntu Server 14.04.3 LTS	192.168.0.10	Exploración de vulnerabilidades con implementación de reglas de acceso interno. Pruebas de Caja Blanca.

Tabla 364. Resumen Analítico en Educación RAE.

30. RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
SISTEMAS DE MONITOREO EN REDES DE DATOS Y ESTADÍSTICA DE ATAQUES EN LA EMPRESA SUNSHINE BOUQUET ZONA NORTE BOGOTÁ COLOMBIA
Autores
SILVIO HUMBERTO LÓPEZ ENRÍQUEZ
Palabras Claves
Sistemas de información, Firewall, Red perimetral, Kali Linux, Sniffer, Servidor, Unifi, Isa server.
Descripción del problema
Sunshine Bouquet es una empresa certificada y líder en producción limpia y elaboración de productos florales de excelente calidad, buscando la satisfacción total del cliente en la cadena, con costos competitivos a través de la efectividad de sus procesos y un equipo humano satisfecho. Sunshine Bouquet en la actualidad tiene una sede en Colombia y una sede en EE. UU., su planta operativa es de un poco más de cuatro mil quinientos empelados. El departamento de TI (Tecnologías de la información) que es uno solo para los dos países cuenta con una planta operativa de veintidós colaboradores, aproximadamente 450 cuentas de correo corporativo, y unos 600 usuarios de computadoras, estos están divididos en Computadoras de Escritorio, Portátiles, Tabletas y Smartphones. Un centro de datos de 11 servidores centralizados y unos seis servidores que se instalan en algunas de las fincas en las cuáles hacen de firewall. Es importante dejar en claro que la empresa Sunshine Bouquet está conformada por zonas y fincas en Colombia; el mayor porcentaje de estas fincas se encuentra en el departamento de Cundinamarca y dos fincas en Antioquia. En Cundinamarca se han sectorizado por zonas, siendo estas zona norte, zona sur y zona occidente. Uno de los problemas más graves que presenta la compañía es la falta de un sistema de Monitoreo en sus redes de Datos y una carencia completa de la estadística de estos, esto incide en constantes ataques de virus, perdida de información y un completo descontrol de las acciones por parte de los usuarios en las máquinas y en la información sensible que cada uno de ellos tiene bajo su responsabilidad.

Tabla 374. Resumen Analítico en Educación RAE. (Continuación)

Objetivo General
Proponer la implementación de un sistema de monitoreo de seguridad en la red de datos y estadísticas de ataques en la empresa Sunshine Bouquet Zona Norte Bogotá, Colombia.
Objetivos Específicos
✓ Realizar levantamiento de la información de metodologías de monitoreo del estado actual de seguridad informática de la empresa. ✓ Determinar las metodologías y herramientas informáticas de riesgos a usar en el diagnóstico de la red de datos de Sunshine Bouquet. ✓ Definir metodologías de análisis de riesgo y técnicas de pen test que se aplicaran para el diagnóstico de la red de datos de Sunshine Bouquet Zona Norte. ✓ Realizar la propuesta de implementación del sistema de monitoreo de seguridad en la red de datos de la empresa Sunshine Bouquet Zona norte
Justificación
La empresa Sunshine Bouquet, dedicada a la producción y comercialización de arreglos florales (Bouquets), durante sus más de 20 años ha aumentado su producción, lo que conlleva a que la información en la entidad tienda a crecer exponencialmente causando inconvenientes en la sistematización de datos. Por tanto, se necesita protección tanto a nivel lógico como físico, por ello es conveniente formular un sistema monitoreo en las redes de datos y estadísticas de ataques En el transcurso del tiempo la pérdida de información y todo el problema que esto conlleva se ha vuelto un tema cotidiano en la empresa Sunshine Bouquet, la información en la entidad acumula un banco de información que data de unos 17 años de existencia, almacena información confidencial tanto de clientes como de proveedores. Adicional maneja cinco aplicaciones cliente servidor que necesitan monitoreo y acceso restringido. El propósito es garantizar la seguridad de la información sea gestionada correctamente, identificando inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C.I.D: ✓ *Confidencialidad:* la información no está a disposición de individuos, entidades o procesos no autorizados. ✓ *Integridad*: La información está completa y fiable. ✓ *Disponibilidad*: la información está disponible y oportuna a personas, entidades o procesos autorizados cuando lo requieran.

Tabla 384. Resumen Analítico en Educación RAE. (Continuación)

Producto final que entregar
Al final de este proyecto se entregara un manual que indicará los procesos, procedimientos para la implementación y puesta en marcha de un sistema de monitoreo de datos y estadística de ataques en las redes de la empresa Sunshine Bouquet zona Norte, Bogotá Colombia, allí aparecerá la documentación de: cada uno de los puntos identificados como riesgos informáticos dentro de la compañía estrictamente en la Zona norte, las políticas de seguridad informática por cada uno de los procesos (actividades electrónicas) que se realizan en Sunshine Bouquet, las recomendaciones y sugerencias a cada proceso y procedimiento que haya sido objeto de estudio para la implementación del sistema de monitoreo y la información detallada sobre las estadísticas de ataque. También se pretende mostrar de forma gráfica cada uno de estos sucesos.
Fuentes bibliográficas
Gómez R., Pérez D., Donoso Y. y Herrera A. (2010) Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Artículo. Revista de Ingeniería. Universidad de los Andes. NTC-ISO/IEC 27005, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información Ministerio de las Tecnologías de la información y las Comunicaciones. (2014). Decreto 2573 de 2014[en línea]. <http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf> [citado en 23 de enero de 2016] Introducción al Sistema de Gestión de Seguridad de la Información – SGSI [en línea] <http://www.iso27000.es/sgsi.html> [citado en 01 de marzo de 2017] Todo sobre MAGERIT [en línea] <http://administracionelectronica.gob.es/ctt/magerit> [citado en 29de octubre de 2016] Metodología MAGERIT [en línea] <http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/index.html> [citado en 11 de mayo de 2016] Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT [en línea]. <https://books.google.com.co/books?id=L-htLwEACAAJ&dq=magerit&hl=es-419&sa=X&redir_esc=y> [citado en 05 de junio de 2015] Pentesting [en línea]. https://books.google.com.co/books?id=sua0BAAAQBAJ&pg=PA560&dq=que+es+pentesting&hl=es-419&sa=X&redir_esc=y#v=onepage&q=que%20es%20pentesting&f=false Sitio oficial de Kali Linux [en línea] <http://tools.kali.org/ > [citado en 13 de febrero de 2016] Mejores prácticas en la seguridad y contenidos [en línea] < www.mpaa.org> Hoja de ruta [en línea] <https://www.w3.org/2014/07/mobile-web-app-state/index.es.html>

Tabla 394. Resumen Analítico en Educación RAE. (Continuación)

Fuentes bibliográficas
Sitio oficial de OWSAP [en línea] <https://www.owasp.org/index.php/Main_Page> [citado en 25 de enero de 2017] 10 consejos para prevenir ataques de Phishing [en línea] <http://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/> [citado en 07 de febrero de 2017] ZORRILLA ARENA, Santiago (2000), Introducción a la metodología de la investigación, México: McGraw Hill Benavides M.C. y Solarte F. (2012). Módulo de Riesgos y Control Informático ISO2700. ¿Qué es un SGSI? [en línea]. <http://www.iso27000.es/sgsi.html> [citado en 15 de octubre de 2016] Dirección de Estándares y Arquitectura de TI del Ministerio de las Tecnologías de Información y las Comunicaciones de la República de Colombia. (2014). Generalidades del Marco de Referencia – versión 1.0. [en línea]. <http://www.mintic.gov.co/portal/604/w3-propertyvalue-558.html > ISO27000.es. Sistema de Gestión de la Seguridad de la Información. [en línea]. <http://www.iso27000.es/doc_sgsi_all.htm> [citado en 15 de octubre de 2015] RISTI - Revista Ibérica de Sistemas y Tecnologías de Informação [en línea]. <http://www.scielo.gpeari.mctes.pt/scielo.php?pid=S1646-98952014000100004&script=sci_arttext> [citado en 11 de enero de 2016] ISO 27001: La Seguridad de la Información en la Gestión de la Continuidad de Negocio. [en línea]. <http://www.pmg-ssi.com/2014/11/iso-27001-la-seguridad-de-la-informacion-en-la-gestion-de-la-continuidad-de-negocio/> [citado en 15 de octubre de 2015] MENDEZ, C. Metodología, Diseño y Desarrollo del proceso de Investigación. Tercera Edición, McGraw Hill, Colombia, 2001. JIMÉNEZ, L. Guía de desarrollo de un plan de continuidad de negocio. [en línea]. <http://www.criptored.upm.es/guiateoria/gt_m001r.htm> [citado en 30 de octubre de 2015] LERMA, Héctor Daniel. Metodología de la investigación. Bogotá: Ecoe Ediciones, 2004. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos

Tabla 404. Resumen Analítico en Educación RAE. (Continuación)

Metodología
“La investigación es un esfuerzo que se emprende para resolver un problema, claro está, un problema de conocimiento” (p. 47). “Sabino" Una metodología de desarrollo se refiere al entorno que se usa para estructurar, manifiesto que pretende mediar y controlar el proceso de desarrollo de un proceso, existen una gran variedad de metodologías desarrolladas a lo largo de los años, cada una de ellas con sus fortalezas y debilidades. Una determinada metodología no es necesariamente aplicable a todo tipo de proyectos, más bien cada tipo de proyecto tiene una metodología a la que se adapta mejor. Situación actual de la zona Norte, en cuanto a procesos y procedimientos relacionados con sistemas de cómputo, usuarios involucrados, disposición y manejo de la información empresarial. Definición de roles, identificación de riesgos informáticos, en cuanto a software, hardware, infraestructura, procesos y procedimientos.
Conclusiones
Uno de los primeros y principales paso antes de dar inicio a un proyecto es el denominado levantamiento de la información, de esto depende en gran medida el éxito o el fracaso de este, así es de vital importancia no solo estima una buena porción de tiempo y conocimiento a esta etapa de un proyecto. El levantamiento de la información no solo se refiere a la documentación técnica involucrada, sino también debemos incluir a todas aquellas experiencias por parte de la mayor cantidad de personal involucrado en dicho proceso caso de estudio. Una vez que hayamos recopilado, analizado, debatido y concluido el tipo de solución que desplegaremos a la mayor cantidad de información de parte del proceso caso de estudio, es el momento de dedicar también muy buen tiempo y conocimiento a las herramientas que usaremos para dar la mejor solución posible, y aquí es muy importante tomar en cuenta a todas esas personas o entidades que gozan de buena experiencia en casos similares a lo que se pretende abordar. Con esto requisitos listos es momento de hacer el despliegue de cada una de las pruebas propuestas, sin olvidar en ningún momento el registro de cada uno de los eventos en su respectivo formato.

Tabla 414. Resumen Analítico en Educación RAE. (Continuación)

Recomendaciones
El activo de la información es uno de los de mayor índice de riesgo hoy en día, para donde quiera que se mire hay algo o alguien que intenta llegar a ella, se ha vuelto como u reto personal. “todos trabajando en pos o en contra de ella”, así que una vez avisado solo queda actuar, y que mejor hacerlo con procedimientos y procesos ya certificados, como lo son los sistemas de monitoreo en redes de datos y estadística de ataques, esto no solo mostrará de forma gráfica y estadística de los diferentes rasgos potenciales que son el pan de cada día, sino que prepara a la entidad para la acción pronta y continua en el cuidado no solo en nuestros datos, sino de nuestra infraestructura. Unas de los principales beneficios de un sistema de monitoreo en redes de datos y estadística de ataques son los siguientes: Establecer una metodología precisa y concisa con la cual gestionar la seguridad de la información. Garantizar que los usuarios y clientes puedan acceder a la información segura. Fomentar la mejora continua en la organización. Detectar fortalezas y debilidades de los sistemas actuales. Usar las estadísticas para la creación de planes de contingencia. Simular técnicas de defensa.
Fecha de realización
Mayo 28 de 2017