IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN EMPRESARIAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA JARDINES CRISTO REY LTDA.

ÁNGELA LIZETH SANTILLÁN MOSQUERA

Trabajo presentado en la modalidad de Proyecto Aplicado como alternativa de trabajo de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PASTO

2019

IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN EMPRESARIAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA JARDINES CRISTO REY LTDA.

ÁNGELA LIZETH SANTILLÁN MOSQUERA

Trabajo de tesis, para optar el título de especialista en Seguridad en Informática

Asesor

ING. YENNY STELLA NÚÑEZ ÁLVAREZ.

Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PASTO

2019

San Juan de Pasto, 19 de junio de 2019

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado (En caso de ser solo uno, borrar este o agregar de ser necesario).

DEDICATORIA

La presente investigación la dedico a mi familia, a mi esposo que me ha acompañado durante todo este proceso y a mi hijo quien es la principal fuente de motivación para continuar con mi preparación personal, además a mi familia quienes con su esfuerzo y dedicación colaboraron de manera desinteresada a la realización de esta meta

ÁNGELA LIZETH SANTILLÁN MOSQUERA

AGRADECIMIENTOS

Agradezco inicialmente y sobre todo a Dios por permitirme llevar a feliz término la presente investigación, a mi familia por brindarme la confianza y el apoyo incondicional en todos los momentos de la especialización, a los Tutores por sus orientaciones, a mi asesor por su valioso aporte al desarrollo del documento final, a la empresa Jardines Cristo Rey, por permitir la interacción con sus sistemas informáticos, al personal encargado del control y la administración de la red de datos de Jardines Cristo Rey, por la colaboración prestada para la recolección de la información requerida, además a la Universidad Nacional Abierta y a Distancia por ser la Institución que brinda la posibilidad de formarme como Especialista en Seguridad en Informática y en general a todas aquellas personas que de una u otra manera se encuentran relacionadas la culminación satisfactoria de esta meta.

TABLA DE CONTENIDO

LISTAS DE TABLAS

LISTA DE CAPTURAS DE PANTALLA

LISTA DE FOTOS

LISTA DE ILUSTRACIONES

LISTA DE ANEXOS

LISTA DE EVIDENCIAS

GLOSARIO

ALGORITMO: Palabra que viene del nombre del matemático árabe Al-Khwarizmi (780 - 850 aprox.). Define el conjunto de instrucciones que sirven para ejecutar una tarea o resolver un problema. Los motores de búsqueda usan algoritmos para mostrar los resultados de búsquedas.

ANCHO DE BANDA: Bandwidth en inglés. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información.

ANTIVIRUS: Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

ARCHIVO: Archivo es el equivalente a "file", en inglés. Es data que ha sido codificada para ser manipulada por una computadora.

BPS: Bits por Segundo. Velocidad a la que se transmiten los bits en un medio de comunicación.

CABLEADO: Columna vertebral de una red la cual utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), de forma que la información se transmite de un nodo a otro.

CARPETA: Espacio del disco duro de una computadora cuya estructura jerárquica en forma de árbol contiene la información almacenada en una computadora, habitualmente en archivos y es identificado mediante un nombre.

CLIENTE: Aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red. Sistema o proceso el cual le solicita a otro sistema o proceso la prestación de un servicio.

COMPUTACIÓN: Es la ciencia que estudia el procesamiento automático de datos o información por medio de las computadoras.

CONMUTACIÓN DE PAQUETES: Un portador separa los datos en paquetes. Cada paquete contiene la dirección de origen, la dirección de su destino, e información acerca de cómo volver a unirse con otros paquetes emparentados.

CONTRASEÑA: PASSWORD. Código utilizado para dar acceso a un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

COOKIE: Un cookie es un pequeño pedazo de data enviado desde un servidor web al navegador del cliente que se guarda localmente en la máquina del usuario.

CRIPTOGRAFÍA: Se dice que cualquier procedimiento es criptográfico si permite a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, luego de haberlo descifrado.

DHCP: Siglas del inglés "Dynamic Host Configuration Protocol." Protocolo Dinámico de Configuración del Host. Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP a las diferentes computadoras de la red.

ENCRIPTACIÓN: Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

ETHERNET: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10 Mbps, por lo tanto tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

EXTRANET: Cuando una intranet tiene partes públicas, en donde posiblemente usuarios externos al intranet pueden llenar formularios que forman parte de procesos internos del intranet.

FIREWALL: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

GATEWAY: Un gateway es un punto de red que actúa como entrada a otra red. En el internet, un nodo o "parada" puede ser un "nodo gateway" o un "nodo host".

HACKER: Persona que tiene un conocimiento profundo acerca del funcionamiento de redes de forma que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

HACKING ÉTICO: Hacking ético es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

HOST: Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas (ssh, FTP, www, email, entre otros.). Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

IP: Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única.

ISO: International Standards Organization es una red de institutos nacionales de estándares constituido por 157 países, un miembro por país, con un secretariado central en Geneva, Suiza, en donde se coordina todo el sistema. Es el desarrollador y publicador de Estándares Internacionales más grande del mundo.

ISP: Internet Service Provider. Proveedor de Servicio Internet. Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.

KALI: Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad. Kali es una completa re-construcción de BackTrack Linux desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de Debian.

LAN: Local Area Network. Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones.

MAC ADDRESS: Siglas del inglés Media Access Control. Es una dirección que usualmente está compuesta por números y letras asignado a los equipos que forman parte de una red, que es único e identifica su lugar dentro de la red.

MÁQUINA VIRTUAL: Software que emula un los componentes de un hardware, permitiendo instalar en estos componentes virtuales un sistema operativo distinto del anfitrión y abrirlo como si fuera "un programa más".

MODELO CLIENTE-SERVIDOR: Sistema que se apoya en terminales (clientes) conectadas a una computadora que los provee de un recurso (servidor).

MODEM: Equipo que permite conectar computadoras por medio de una llamada telefónica, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información).

NETWORKING: Término utilizado para referirse a las redes de telecomunicaciones en general.

PING: Packet Internet Groper. Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa. El PING envia paquetes al IP o host que se le indique, y nos dice cuanto tiempo demoró el paquete en ir y regresar, entre otras pocas informaciones.

PROTOCOLO: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

PROXY: Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red.

PUERTO: Número que aparece tras un nombre de dominio en una URL. Dicho número va precedido del signo dos puntos. Canal de entrada/salida de una computadora.

RED: Sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes. En inglés se le conoce como Network. El internet está compuesto de miles de redes, por lo tanto al internet también se le conoce como "la red".

RED INALÁMBRICA: Red que no utiliza como medio físico el cableado sino el aire y generalmente utiliza microondas o rayos infrarrojos.

SERVIDOR: Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

SERVIDOR DE CORREO: Un servidor de correo (mail server) es la computadora donde se ejecuta un programa de gestión de emails.

SERVIDOR WEB: Un servidor web es el programa, y la computadora que lo corre, que maneja los dominios y páginas web, interpretando lenguajes como html y php, entre otros.

SISTEMA OPERATIVO: Operating System (OS) en inglés. Programa especial el cual se carga en una computadora al prenderla, y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán, como por ejemplo, un procesador de palabras o una hoja de cálculo, un juego o una conexión a Internet. Windows, Linux, Unix, Android, MacOS son todos sistemas operativos.

SSH SECURE SHELL (SSH): es un protocolo de red seguro para la comunicación de data, que permite la conexión de dos computadoras, usualmente una de ellas es un servidor Unix o Linux.

TCP/IP: El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). En español es Protocolo de Control de Transmisión y Protocolo de Internet.

TOPOLOGÍA DE RED: Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red.

UPS: Siglas en ingles de Uninterruptible Power Suply, es un aparato que incluye una batería que en caso que se vaya la electricidad, puede, por ejemplo, mantener una computadora funcionando lo suficiente para que el usuario pueda apagarla y guardar data importante.

USB: Universal Serial Bus. Estándar utilizado en las PCs con el fin de reconocer los dispositivos hardware (impresora, teclado, entre otros.) y ponerlos en funcionamiento de forma rápida y sencilla. Elimina la necesidad de instalar adaptadores en la PC.

USUARIO: Persona que tiene una cuenta en una determinada computadora por medio de la cual puede acceder a los recursos y servicios que ofrece una red. Puede ser tanto usuario de correo electrónico como de acceso al servidor en modo terminal. Un usuario que reside en una determinada computadora tiene una dirección única de correo electrónico.

VIRUS: Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas.

WiFi: Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz.

RESUMEN

El presente proyecto de aplicación busca mediante la identificación y la realización de pruebas de testeo a la red de datos de la compañía JARDINES CRISTO REY LTDA., ubicada en la ciudad de Pasto (Colombia), con las cuales se permita evidenciar y diagnosticar el conjunto de vulnerabilidades existentes en el control de acceso al Sistema de Gestión Empresarial, el cual soporta todos los procesos administrativos de la compañía, lo que lo convierte en un sistema primordial para la empresa y que exige a la administración el protegerlo, ya que en la actualidad no cuenta con medidas de seguridad empleadas para tal fin. El estudio obtenido se empleará posteriormente para realizar la evaluación de su impacto, de acuerdo al dictamen revelado, con lo anterior se busca identificar y plantear un conjunto de estrategias de mitigación de los riesgos encontrados que conlleve la prevención contra incidentes y por ende el fortalecimiento de la seguridad en el control de acceso del Sistema de Gestión Empresarial, lo que da como resultado la elaboración de un documento que contenga el desarrollo del proceso propuesto en este proyecto.

Para su desarrollo se aplicará la metodología propuesta por Serrato, en la cual se definen los pasos a ejecutarse en el rastreo y evaluación de vulnerabilidades en sistemas de gestión de información a nivel lógico, de igual manera que se hará uso del software libre OpenVAS (Sistema Abierto para Evaluación de Vulnerabilidades), con lo que se busca llevar a cabo el levantamiento de evidencias relacionadas con fallas y vulnerabilidades del sistemas de información de la compañía.

Palabras claves: Seguridad Informática, testeo de red, vulnerabilidades, control de acceso, medidas de seguridad.

ABSTRACT

This application project seeks through the identification and testing of the data network of the company JARDINES CRISTO REY LTDA., Located in the city of Pasto (Colombia), with which it is allowed to evidence and diagnose the whole of existing vulnerabilities in the control of access to the Business Management System, which supports all the administrative processes of the company, which makes it a fundamental system for the company and which requires the administration to protect it, since currently does not have security measures used for that purpose. The study obtained will be used later to carry out the evaluation of its impact, according to the revealed opinion, with the above it seeks to identify and propose a set of mitigation strategies of the risks found that entails the prevention against incidents and therefore the strengthening of security in the access control of the Business Management System, which results in the preparation of a document that contains the development of the process proposed in this project.

For its development the methodology proposed by Serrato will be applied, in which the steps to be executed in the tracking and evaluation of vulnerabilities in information management systems at the logical level are defined, in the same way that free software OpenVAS will be used. Open for Vulnerability Assessment), which seeks to carry out the collection of evidence related to failures and vulnerabilities of the company's information systems.

Keywords: Computer Security, network testing, vulnerabilities, access control, security measures.

INTRODUCCIÓN

Según Najar[1], desde hace algunos años, la información ha sido considerada como el activo más valioso al interior de las organizaciones, razón por la cual, la seguridad de los sistemas informáticos recae en el personal designado para tal fin y son ellos quienes deben establecer procedimientos y herramientas suficientes y necesarias para el manejo y la administración de la información empresarial de una manera segura.

Cabe anotar que la seguridad de la información debe ser considerada como una función transversal dentro de las compañías, lo que implica la concientización sobre la responsabilidad y el compromiso misional en el empleo de prácticas adecuadas en su procesamiento y manejo, lo anterior sin importar cuál sea la actividad económica a la que se dedique la compañía. Por lo tanto es menester de la compañía el apropiarse de los mecanismos esenciales que aseguren y protejan la información, de tal manera que no esté expuesta a ataques informáticos.

De igual manera y tomando en cuenta que la idea de riesgo se asocia al concepto de incertidumbre y que por el contrario la proyección de la seguridad crea certidumbre y viabilidad[2], una empresa que administra su información de dicha manera refleja estas condiciones hacia el exterior. Además, se debe considerar que el manejo inadecuado de la información o la insensibilidad en los controles existentes vuelven los sistemas de información vulnerables a ataques, por parte de personas mal intencionadas o delincuentes informáticos quienes se encuentran al acecho de empresas con este tipo de falencias[3].

Además y con la necesidad de mitigar os riesgos de seguridad existentes en una organización es imprescindible la ejecución y el levantamiento de evidencias que permitan diagnosticar y evidenciar de forma adecuada el conjunto de

[1] NAJAR, José Custodio. Information Security: A Valuable Asset of the Organization. En: Vínculos Vol. 12 Núm. 1. 2015

[2] WWW.CEUPE.COM. Análisis de viabilidad riesgo de proyecto. [en línea] www.ceupe.com. 2019. [Consultado: 19 de junio de 2019] Disponible en internet: https://www.ceupe.com/blog/analisis-de-viabilidad-riesgo-de-proyecto.html

[3] UDG.MX. Delincuentes informáticos ya no atacan empresas grandes, sino a usuarios de smartphone. [en línea] www.udg.mx. 2018. [Consultado: 29 de marzo de 2018] Disponible en internet: http://www.udg.mx/es/noticia/delincuentes-informaticos-ya-no-atacan-empresas-grandes-sino-usuarios-smartphone

vulnerabilidades presentes en los sistemas de información de la compañía, lo anterior mediante la evaluación de las mismas y buscando la reducción del impacto con el planteamiento de estrategias para la mitigación de los riesgos y es esta condición el punto de partida del presente proyecto buscando mejorar la seguridad en el control de acceso, con el uso de estándares relacionados con los conceptos de seguridad informática(ISO/IEC 27002).

1. ANTECEDENTES Y CONTEXTO

1.1. PLANTEAMIENTO DEL PROBLEMA

Cabe resaltar que la información es un recurso y que al poseer esta connotación adquiere valor, situación que se puede observar en la empresa JARDINES CRISTO REY LTDA., de la ciudad de Pasto, por consiguiente, se presenta la necesidad de protegerla debidamente, con lo que se garantice la continuidad de los servicios prestados por la empresa, en lo referente con su sistema de Gestión Empresarial, ya que este soporta todos los procesos administrativos de la compañía.

Además, con relación a la información registrada de los clientes que hacen uso de los servicios funerarios ofrecidos por la compañía y con base en lo enunciado en el decreto 1377 de 2013[4], es necesario clarificar que según las definiciones expuestas en el Artículo 3 del mismo y la información solicitada al momento de la firma del contrato en este se encuentra únicamente información considerada como dato público, como son el nombre del cliente, su dirección, numero de documento de identidad, entre otros. De igual manera y en relación a la libertad para la recolección de estos datos, la compañía JARDINES CRISTO REY LTDA., al momento de recolectarlos y mediante forma oral solicita la autorización para su tratamiento.

Una vez se firma el contrato entre el cliente y la compañía se procede al registro de la información en la base de datos, en la que permanece indefinidamente, debido a las características del servicio funerario, el cual será empleado al momento de fallecer el titular o un familiar del mismo y una vez se realicen las exequias, existen procesos de exhumación debidamente considerados, por lo anterior se puede definir que la información almacenada no es susceptible a ser suprimida. Por ende y para evitar filtraciones de informaciones sensibles es menester el mejorar la seguridad del sistema de Gestión Empresarial de la compañía JARDINES CRISTO REY LTDA., y es un aparte de esta seguridad el prevenir accesos no autorizados a la misma, situación en la que se fundamenta la presente investigación.

[4] PRESIDENCIA DE LA REPUBLICA. Decreto 1377 de 2013. [en línea] http://wsp.presidencia.gov.co. 2013. [Consultado: 19 de junio de 2019] Disponible en internet: http://http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

Cabe anotar que entre la información que se administra en el servidor de Gestión Empresarial, se encuentra financiera y contable, comercial, Kardex y asignación de lotes funerarios, la cual es de vital importancia, debido a que si se presenta pérdidas o se expone a terceros la empresa se verá afectada en el normal desarrollo de sus funciones, al igual que se afectaran los tres pilares de la seguridad de la información que son confidencialidad, integridad y disponibilidad.

En la actualidad JARDINES CRISTO REY LTDA., no cuenta con estrategias de mitigación de riesgos para su Sistema de Gestión de Seguridad de la Información, condición que ha permitido la ocurrencia de ataques por parte de personas inescrupulosas, agravado por errores en el manejo de protocolos de seguridad informática, según lo expone el ingeniero encargado del área de sistemas de la compañía. Para la verificación de las condiciones existentes, se espera realizar un análisis, de las condiciones de seguridad informática en el que se evidencie los procesos de control actuales, logrando en etapas posteriores del presente estudio la optimización de los mismos mediante la aplicación del estándar ISO/IEC 27002, buscando con esto atenuar los riesgos presentes en la seguridad informática; tomando en cuenta que existen diferentes tipos de amenazas presentes sobre el sistema de Gestión Empresarial que podrían conllevar a la interrupción de las funciones propias de la compañía, como es el caso de la administración, comercialización y venta de servicios funerarios, actividad central de JARDINES CRISTO REY LTDA.

Formulación del problema:

¿Es posible mejorar la seguridad para el control de acceso al sistema de Gestión Empresarial de la compañía Jardines Cristo Rey Ltda., mediante la definición de un plan de mitigación de riesgos el cual responda a una previa identificación de vulnerabilidades empleando pruebas de testeo de red?.

1.2. JUSTIFICACIÓN

Con la promulgación de la ley 1581 de 2012 y el Decreto 1377 de 2013, las entidades públicas al igual que las empresas privadas poseen la obligación de realizar un manejo adecuado y la revisión del uso que se brinda a los datos personales existentes en sus sistemas de información, lo que conlleva en muchos casos la necesidad de reformular las políticas de manejo de información al igual que el fortalecimiento de las herramientas informáticas de las que hacen uso. Es por ello que se considera necesario que el sistema de Gestión Empresarial de la empresa JARDINES CRISTO REY LTDA., ubicado en la ciudad de Pasto, cumpla entre otras

dichas regulaciones, dado que este contiene información financiera, comercial, información de Kardex e inventarios de lotes funerarios, elementos fundamentales para el normal desarrollo de su actividad económica, lo que requiere la necesidad de protegerla, buscando garantizar la continuidad de los servicios ofrecidos por la empresa.

El término a buen fin de este proyecto brinda la posibilidad de identificar las condiciones de seguridad existentes mediante la aplicación de pruebas de testeo empleadas en los sistemas y procesos informáticos realizados en los equipos de cómputo de la compañía, lo que permite la aplicación de los conocimientos adquiridos en el transcurso de la Especialización en Seguridad en Informática. De igual manera, el aplicar un reconocimiento de vulnerabilidades al sistema de Gestión Empresarial ayudara a evaluar las condiciones de seguridad que permita la elaboración de un plan encargado de la mitigación de las vulnerabilidades existentes o a presentarse en el sistema de gestión de la información logrando con ello un sistema de información más confiable, íntegro y disponible; cabe anotar además que el desarrollo del proyecto brindara al grupo de trabajo la posibilidad de culminar satisfactoriamente esta etapa académica.

1.3. OBJETIVOS

1.3.1. Objetivo General

Identificar las vulnerabilidades de seguridad en el control de acceso al sistema de Gestión Empresarial de la compañía Jardines Cristo Rey Ltda., mediante la aplicación de pruebas de testeo de red.

1.3.2. Objetivos Específicos

- Determinar la metodología de pruebas de penetración para la identificación de vulnerabilidades
- Realizar pruebas de testeo a la red de datos, que permitan diagnosticar las vulnerabilidades existentes en el control de acceso al sistema de Gestión Empresarial de la empresa Jardines Cristo Rey Ltda.
- Evaluar las vulnerabilidades encontradas con relación con los riesgos detectados en las pruebas de testeo de red y su impacto con el sistema de Gestión Empresarial.
- Identificar y definir estrategias de seguridad sobre el control del sistema empleadas en la mitigación de los riesgos encontrados encaminados hacia la prevención y el fortalecimiento de la seguridad en el control de acceso al sistema de Gestión Empresarial.

2. MARCO CONCEPTUAL Y TEÓRICO

2.1. MARCO LEGAL

Legislación de Seguridad Informática en Colombia

Ley 1581 de 2012 y el Decreto 1377 de 2013

La Ley 1581 de 2012 y el Decreto 1377 de 2013, enmarcan las regulaciones existentes sobre el manejo de la información personal, específicamente con lo relacionado a la protección de información personal, disponible en una empresa en sus bases de datos y sobre la cual se realicen las operaciones de los sistemas de procesamiento de transacciones, sin importar que la compañía pertenezca al sector público o privado.

En concreto, la ley exige a las compañías sin importar el sector al que estén vinculadas verificar la forma en la cual se están empleando los datos personales almacenados en sus sistemas de información, requiriendo también modificar las políticas de seguridad existentes y que se relacionen con la selección y aplicación de herramientas tecnológicas apropiadas, debido a la masificación de sistemas de información presentes en la actualidad.

A su vez, el decreto 1377 de 2013, regula los aspectos relacionados con el manejo de la información personal dispuestos en la Ley 1581.

2.2. MARCO CONTEXTUAL

2.2.1. Jardines Cristo Rey Limitada[5].

Es una empresa Nariñense prestadora de servicios funerarios debidamente registrada en La Cámara de Comercio de Pasto como persona jurídica, régimen común, con sede en la ciudad de Pasto. Su objeto social es prestar servicios en las actividades funerarias.

[5]JARDINES CRISTO REY. Servicios Exequiales Jardines Cristo Rey Ltda. [en línea] jardinescristorey.com/. 2017. [Consultado: 29 de marzo de 2018] Disponible en internet: http://www.jardinescristorey.com/

Además y en su afán de mejora permanentemente en el desarrollo de sus procesos y la prestación de los servicios, es que la compañía ha mostrado interés en el desarrollo de este estudio, razón por la cual ha brindado su autorización y ha dispuesto el apoyo del personal encargado del mantenimiento del área de sistemas para las etapas de recolección de información y acceso a las arquitecturas de datos de manera controlada (Ver Anexo 5. Carta de aprobación de la compañía).

Reseña Histórica

Jardines Cristo Rey Ltda. Inicio su actividad comercial el 7 de octubre de 1985, se fundó en la calle 19 No. 31-19 B/ Las Cuadras y posteriormente el 30 de noviembre de 1995 se trasladó a su propia cede ubicada en la carrera 31B No. 19-12, B/ Las Cuadras.

La función de la empresa se presenta en la misión empresarial que se indica a continuación:

"MISIÓN

Prestar servicios con altos niveles de calidad a través de personal competente, garantizando respeto, sensibilidad y calidez humana hacia nuestros clientes en los momentos difíciles e imprescindibles por pérdida de un ser querido. Esto se logra a través de un servicio oportuno, confiable y seguro."[6]

Al igual que la compañía tiene una orientación clara sobre su proyección hacia el futuro como se registra en la visión empresarial.

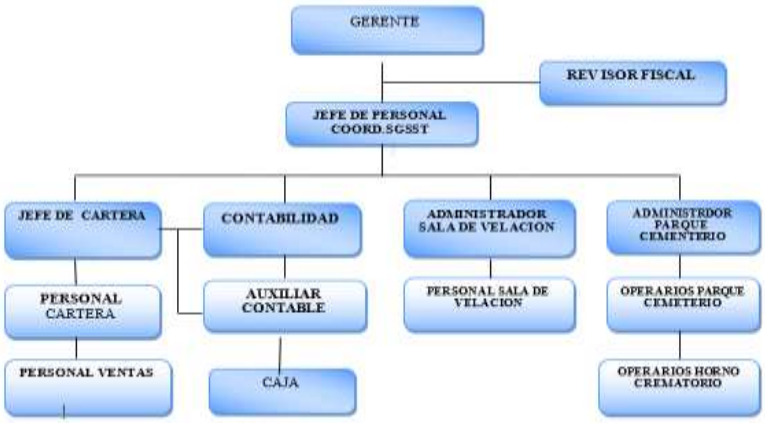
"VISIÓN

Jardines Cristo Rey Ltda. Se proyecta en ser la mejor opción en servicios funerarios, con calidad, responsabilidad y compromiso continuo para ello contamos con un capital humano eficiente y competente que busca la satisfacción plena del nuestros clientes actuales y potenciales"[7]

La compañía posee una estructura jerárquica la cual se presenta en el siguiente organigrama:

[6] JARDINESCRISTOREY.COM, Óp. Cit. p. 4
[7] JARDINESCRISTOREY.COM, Óp. Cit. p. 4

Ilustración 1. Organigrama Jardines Cristo Rey Ltda.



Fuente: http://www.jardinescristorey.com/[8]

2.2.2. Arquitectura de red existente

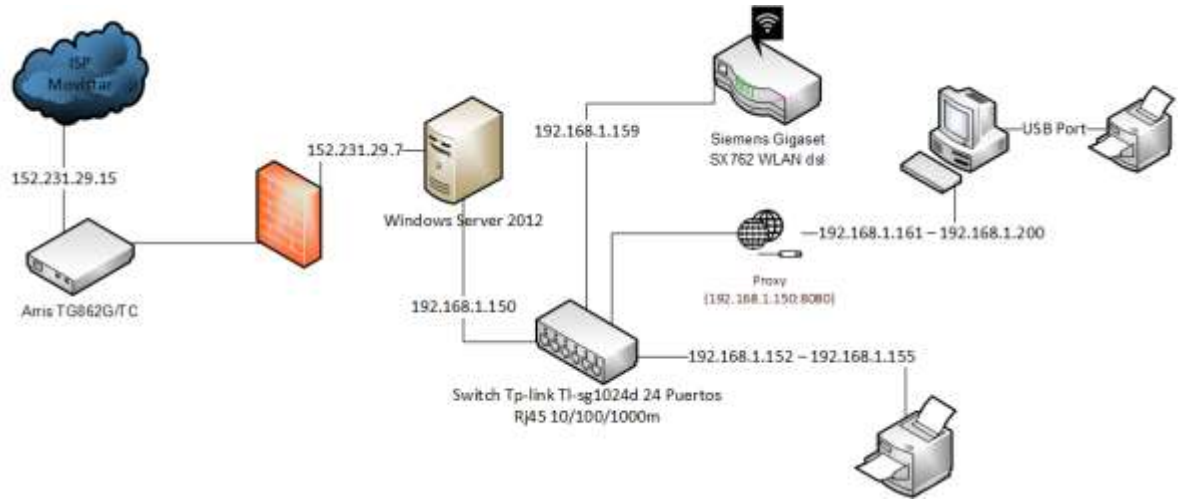
La compañía posee en sus instalaciones una infraestructura de red intranet que se compone de una conexión a un proveedor de servicios de internet (MOVISTAR) por medio de un modem “Arris TG862G/TC”.

Esta conexión se administra por medio de un servidor el cual se encuentra conectado por una tarjeta de red al proveedor de servicios de internet y otra tarjeta a la red interna de la compañía, por medio de un switch TP-LINK TL-SG1024. El servidor ha sido configurado para prestar los servicios de Servidor de Dominio, Servidor de Archivos, Servidor DHCP, Active Directory, enrutamiento de conexiones y servidor proxy.

El personal cuenta con mínimo una terminal de trabajo para cada sección representada en el organigrama de la compañía lo que conforma la Intra net de la empresa (10 equipos de cómputo, 2 impresoras en red por IP y 2 impresoras compartidas a través de terminales Windows), de igual manera existe una conexión para el servicio Wifi para salas de velación a través de un modem “Siemens Gigaset SX762 WLAN dsl”.

[8] JARDINESCRISTOREY.COM, Óp. Cit. p. 4

Ilustración 2. Arquitectura de red Jardines Cristo Rey



Fuente: El presente documento

Detalles de la arquitectura

Tabla 1. Funciones de equipos en red

Equipo	Función	Dirección IP
Modem	Conexión con ISP	152.231.29.15
Servidor	Presenta los servicios de administración de redes y Conexiones a través de enrutamientos y proxy	192.168.1.150
Wifi	Equipo prestador del servicio de Wifi en salas de	192.168.1.159
Terminales	Equipos encargados del manejo de la información	192.168.1.160 a 192.168.1.200
Impresoras de red	Equipos de impresión	192.168.1.152 a 192.168.1.155

Fuente: El presente documento

2.3. MARCO TEÓRICO

2.3.1. Seguridad de la información[9]

La seguridad de la información es considerada como las actividades tendientes a la preservación de la confidencialidad, integridad y disponibilidad de la misma, al igual que los sistemas relacionados con su tratamiento dentro de una empresa. Es de

[9] ISO27000. Sistema de gestión de la seguridad de la información. [en línea]. ISO27000 2015. 14 p. [Consultado: 30 de marzo de 2018]. Disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

ahí que estos conceptos son claves para la definición del concepto de seguridad de información:

- Confidencialidad: La información debe ser protegida de su difusión a personal no autorizado, de igual manera únicamente debe estar disponible para aquellos que la necesiten lo cual además asegura una gestión eficiente.
- Integridad: La información no debe presentar errores en las entradas, conversión o procesos que puedan afectar los resultados, de igual manera debe ser semánticamente correcta y representar transacciones válidas y autorizadas.
- Disponibilidad: Se debe brindar disposición a la información a quienes deban acceder a ella, de manera más clara es el acceso a la información por parte de personas autorizadas cuando así sea requerido.

De igual manera y para que la seguridad de la información sea gestionada de manera adecuada, se necesita ejecutar un proceso sistemático, documentado y conocido por toda la empresa, orientada a partir del uso de un enfoque centralizado en el riesgo empresarial, dicho proceso se constituye como un Sistema de Gestión de la Seguridad de la Información o ISMS Information Security Management System por sus siglas en ingles.

2.3.2. Sistema de Información de Gestión Empresarial

El Sistema de Información de Gestión Empresarial emplea el software CAFÉ el cual opera bajo la plataforma Windows, la unificación de varios módulos permite realizar tareas como[10]: Gestión Comercial, Contabilidad, Proceso Nómina, Gestión Oficial, Cartera Financiera, P.O.S y Facturación, Servicios y cuentas por cobrar y pagar. En el sistema de Gestión Empresarial se almacenan los archivos actuales e históricos de los procesos antes mencionados, los cuales a su vez se ubican físicamente en un servidor designado para tal fin. Además, el Sistema de Información de Gestión Empresarial se rige bajo las normas sistemáticas y legales vigentes en el país para su funcionamiento.

2.3.2.1. Aplicativo GESTIÓN COMERCIAL PLUS SysCafé Software Integrado de Gestión Empresarial

El software de GESTIÓN COMERCIAL PLUS SysCafé Software Integrado de Gestión Empresarial, según sus desarrolladores se considera como la solución más completa y eficiente que tiene como capacidad cubrir las necesidades de las empresas del sector comercial mediante la integración de todos los procedimientos

[10] SYSCAFE. Productos SysCafé. syscafe.com.co. 2018 [en línea]. Disponible en internet: https://www.syscafe.com.co/producto

de la compañía, como característica adicional se tiene el que permite trabajar de manera óptima la contabilidad a partir de la parametrización de documentos fuente, lo que brinda la posibilidad de generar informes generales y detallados, que se emplean como apoyo para la toma de decisiones comerciales, financieras y de servicios. Con base en lo anterior es posible afirmar que GESTIÓN COMERCIAL PLUS SysCafé permite la administración, manejo operativo, contable y tributario de cualquier empresa dedicada a actividades de comercialización, sin importar la actividad o el tamaño de la misma, entre las actividades que permite realizar el aplicativo, se encuentran[11]:

- Manejar de información exógena y fiscal para diferentes entes de control.
- Control de ventas diarias.
- Control de inventarios por bodegas, líneas y centros de costo.
- Control de flujo de caja.
- Manejo de conciliaciones bancarias.
- Estados de resultados comparativos mensuales y por año.
- Está en capacidad de implementar las Normas Internacionales de Información Financiera (NIIF)
- Posee un módulo de facturación electrónica.

A su vez este software integrado cuenta con los siguientes procesos:

- Contabilidad Fiscal y Financiera
- Facturación
- Cuentas por cobrar
- Cuentas por pagar
- Inventarios
- Tesorería

Procesos complementarios:

- Inmobiliario
- Servicios Públicos
- Fuerza de Ventas (Dispositivos Móviles)
- Cartera Financiera
- Nómina
- Activos Fijos
- Taller

[11] GUÍA TIC SOLUCIONES. GESTIÓN COMERCIAL PLUS SysCafé Software Integrado de Gestión Empresarial. 2018. [Consultado: 30 de marzo de 2018]. Disponible en internet: http://www.guiadesolucionestic.com/sistemas-de-informacion/gestion-financiera/software-contable/459-gestion-comercial-plus-syscafe-software-integrado-de-gestion-empresarial

- Arquitectura del servidor Sistema de Gestión Empresarial

Requisitos del sistema:

El Aplicativo GESTIÓN COMERCIAL PLUS SysCafé Software Integrado de Gestión Empresarial, puede ser instalado y ejecutado bajo el sistema operativo Windows 7 o en un servidor Windows Server 2008 o superiores, razón por la cual se contemplan los mismos requerimientos mínimos así:

Para terminales[12]:

- Procesador de 1 gigahercio (GHz) o más rápido de 32 bits (x86) o de 64 bits (x64)
- 1 GB de RAM (32 bits) o 2 GB de RAM (64 bits)
- 16 GB de espacio disponible en el disco duro (32 bits) o 20 GB (64 bits)
- Tarjeta gráfica DirectX 9 con controlador WDDM 1.0 o superior.

Para equipo servidor[13]

- Procesador 1 GHz (x86) o 1.4 GHz (x64)
- Memoria 512 MB RAM (podría limitarse el rendimiento y algunas características)
- Tarjeta gráfica Super VGA (800 x 600)
- Espacio libre HDD 10 GB

2.3.2.2. Arquitectura del servidor de Sistema de Gestión Empresarial14.

Para poder definir la arquitectura de sistema de gestión empresarial se analizarán las diferentes capas que pueden componerlo, debido a que cada una de ellas se asocia con los procesos de negocio de la empresa. Es así que según esta clasificación se identifican los siguientes componentes (Ver

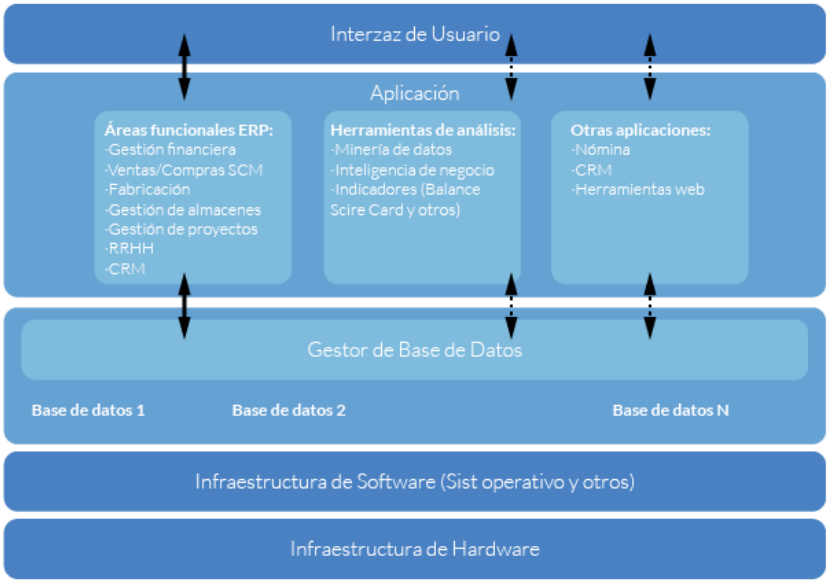
Ilustración 2):

[12]MICROSOFT. Windows 7 system requirements. [En línea]. 2008. [Consultado: 1 de abril de 2018] Disponible en internet: https://support.microsoft.com/es-co/help/10737/windows-7-system-requirements

[13] MICROSOFT. Windows server 2008 requerimientos del sistema. [en línea]. 2008. [Consultado: 1 de abril de 2018]. Disponible en internet: https://msdn.microsoft.com/es-es/library/dn383626(v=ws.11).aspx

[14] EVALUANDOSOFTWARE.COM. Estructura de un sistema de gestión empresarial. [en línea] 31 de 03 de 2015. [Consultado: 3 de abril de 2018]. Disponible en internet: http://www.evaluandosoftware.com/estructura-sistema-gestion-empresarial/

Ilustración 3. Componentes de un sistema de gestión empresarial



Fuente: https://imgur.com/xppbHmX[15].

2.3.2.3. Infraestructura de hardware y comunicaciones[16].

Se centra principalmente en los elementos componentes presentes en una red de área local o LAN (Local Area Network por sus siglas en ingles), para el presente proyecto se empleará la estructura de red de datos conformada por:

- Un gabinete o rack donde se ubican y organizan los componentes de distribución de los servicios de red (switchs, enrutadores, patch panels, entre otros).
- Los servidores equipos de cómputo encargados de ofrecer los servicios necesarios para la realización de los procesos empresariales.
- Los switchs son equipos que realizan su función en capa dos (Enlace) del Modelo OSI, administra la asignación y resuelve inconvenientes de rendimiento de ancho de banda, permite la conexión de múltiples terminales dentro de una misma red.
- Los routers son dispositivos ubicados en la capa tres (Red) del Modelo OSI, permiten la interconexión de diferentes redes permite exportar empaquetar los datos para ser transmitidas a otra red.
- Un cortafuego o dispositivo empleado para la protección y el filtrado de paquetes

[15] EVALUANDOSOFTWARE.COM, Ibíd. p. 10
[16] COMSOLTI.MX. Infraestructura Hardware. [en línea] 2018. [Consultado: 4 de abril de 2018] Disponible en internet: http://comsolti.mx/infraestructura-hardware/

haciendo uso de una secuencia de órdenes y valoraciones de permisos definidos por el administrador del sistema. Este puede ser un equipo creado para ejercer esta labor, o de igual manera un software disponible en un host conectado en red en una ubicación tal que el flujo de las comunicaciones se centre en él.

- Patch panel, ductería y cableado en general, elementos físicos empleado para la organización de los cables de cables, su distribución en el espacio físico y los medios de transporte de señales respectivamente. Para el presente proyecto la compañía cuenta con una intranet establecida con cableado categoría 6A.

En lo referente a los servicios con los que cuenta la empresa se tienen:

- Servidor Proxy. Encargado de procesar las solicitudes de los usuarios con lo relacionado a consultas de páginas web.
- Servidor de Base de Datos. Brinda al sistema de información la capacidad de almacenar los registros y la estructura de las base de datos pertenecientes a los usuarios.
- Servidores DHCP. Sistema encargado de la asignación de direcciones IP dinámicas para la LAN
- Servidores de Archivos. Brinda al sistema de información la capacidad de almacenar los archivos y documentos digitales pertenecientes a los usuarios.
- Servidor de Aplicaciones. Encargados de la prestación de los diferente servicios de red necesarios para el normal funcionamiento de la arquitectura tecnológica.
- Servidor de Dominios. Permite la definición y creación de dominós de red para la intranet

2.3.2.4. Infraestructura de software

Se procede a definir el software que se ejecutará en ella. En la actualidad, los sistemas operativos predominantes para las aplicaciones de negocio son Windows, Unix, en distintas versiones y Linux. Sobre los cuales se implementa el aplicativo conocido como el Sistema de Gestión Empresarial en sí mismo. Según como el fabricante haya seleccionado la arquitectura de diseño, la aplicación y la interfaz se pueden articular en una arquitectura cliente/servidor en dos capas, o distribuidos en componentes separados, opción empleada comúnmente en las últimas versiones permitiendo un mejor aprovechamiento de los recursos.

Gestor de base de datos, la base de datos.

Para esta capa se cuenta una gran diversidad de soluciones que varían dependiendo tanto al volumen de los datos a gestionar al igual que a las formas de

almacenar, proteger y dar soporte a la aplicación de negocio. Generalmente su oferta es realizada por fabricantes de software que brindan la posibilidad de seleccionar entre distintos motores de base de datos, siendo el usuario quien selecciona éste en función de los requerimientos del sistema, compatibilidad con la plataforma de hardware y software, política de empresa y capacidad financiera entre otras razones.

Aplicación.

Presenta el núcleo del sistema proporcionando acceso y funcionalidad a los procesos internos de la empresa. Por ello, en la mayoría de los casos requiere de un periodo de adaptación y adecuación para modificar el diseño estándar realizado por el fabricante y adaptarse aún mejor a los requisitos de la empresa.

Es necesario aclarar que los periodos de personalización y su implantación suelen incrementar el costo final del proyecto, de igual manera un exceso de modificaciones puede penalizar las actualizaciones a versiones posteriores del sistema.

En lo relacionado con los módulos que contiene el sistema de gestión, cada fabricante organiza la aplicación y el contenido de forma ligeramente distinta, pero generalmente se busca cubrir los siguientes módulos:

- Gestión Financiera. Controlando las funciones de Contabilidad, Tesorería, Presupuestos y Activos Fijos.
- Ventas/Compras/SCM. Gestiona de la cadena de suministro, aprovisionamientos, gestión del ciclo de ventas, que va desde la presentación de ofertas hasta la facturación, entre otros.
- Fabricación. Control y gestión de los procesos de fabricación.
- Gestión de Almacenes/Logística. Permitiendo la administración por parte del usuario de la gestión de almacenes.
- Gestión de Proyectos. Control y gestión de los proyectos.
- CRM (Customer Relationship Management). Manejo de clientes que se interrelaciona con el área de Ventas.
- Recursos Humanos. Gestión de empleados, datos personales, control de presencia, pago de parafiscales, entre otros.

Sin embargo, en la práctica no todos los módulos están presentes en un sistema de gestión funcional, por ejemplo, si la compañía no trabaja con proyectos no se

planteará la utilización de dicho módulo. También se puede considerar que alguno de los componentes se puede agrupar en aplicaciones distintas al sistema de gestión propiamente dicha, lo que suele ocurrir comúnmente en las áreas de Recursos Humanos o Gestión de Nóminas, Inteligencia de Negocio y Minería de Datos (Datawarehousing).

Interfaz de Usuario

En este componente se centralizan las interfaces que permita al usuario trabajar con la aplicación. Éstas suelen orientarse sobre alguna de las siguientes tipologías[17]:

- Cliente Estándar. Aplicación mono estación la cual ejecuta las reglas de negocio o tareas en las áreas funcionales en el mismo ordenador en el que se ejecuta la aplicación Cliente
- Cliente Ligero. Esta aplicación se ejecuta en el equipo del cliente por medio de una interfaz de comunicación como es navegador web sin requerir instalaciones de software adicional, brindando con elle beneficios como el consumo reducido de ancho de banda, el uso de dispositivos móviles, entre otros. A todo esto, se puede sumar que las posibilidades de estos clientes ligeros están ya muy cerca de los clientes estándar.
- Aplicaciones de hoja de cálculo. A pesar que en la práctica no suelen considerarse como parte del sistema de gestión, un gran número de los usuarios utilizan las hojas de cálculo para la presentación de informes complejos, gráficos, análisis de datos, entre otros.
- Cliente 100% Web: se ejecuta desde el navegador con un modelo cliente servidor bien definido.

El sistema de gestión empleado en el presente proyecto posee una arquitectura de cliente estándar.

2.3.3. Vulnerabilidad

Se considera como una vulnerabilidad como un punto débil en la seguridad de un sistema informático. A través de ésta es posible que se presenten amenazas que pongan en peligro la confidencialidad e integridad de la información; de igual manera se requiere la realización de un análisis para identificar el tipo y el nivel de cada vulnerabilidad lo que da como resultado la identificación del nivel de riesgo. Los

[17] EVALUANDOSOFTWARE.COM. Estructura de un sistema de gestión empresarial [en línea] www.evaluandosoftware.com/. 2015. [en línea] [Consultado: 18 de junio de 2019]. Disponible en internet: https://www.evaluandosoftware.com/

diferentes tipos de vulnerabilidades se presentan en la siguiente gráfica[18].

Ilustración 4. Tipos de vulnerabilidades

Fuente: https://capacitateparaelempleo.org/assets/4aq4l6q.pdf[19]

2.3.3.1. Diagnóstico de vulnerabilidades[20]

El diagnostico de vulnerabilidad es el proceso mediante el cual se determina el nivel de exposición y predisposición a la falla o pérdida de un elemento del sistema de red frente a una amenaza específica. El grado de vulnerabilidad se encuentra relacionado de manera directa con la organización interna existente en la empresa que a su vez se encarga de prevenir o controlar aquellos factores que originan el peligro al igual que la posible preparación encaminada a minimizar las consecuencias una vez se suceden los hechos.

[18] JLIM, F. C. capacitateparaelempleo.org. Vulnerabilidades Informáticas [en línea] 2015. P. 2. [Consultado: 10 de abril de 2018]. Disponible en internet: https://capacitateparaelempleo.org/assets/4aq4l6q.pdf

[19] JLIM Óp. Cit. p. 8

[20] SENA. Análisis De Vulnerabilidad. Curso: Planes de Emergencia. [en línea] 2007. P. 18. [Consultado: 11 de abril de 2018]. Disponible en internet: https://sena.blackboard.com/bbcswebdav/courses/32330017_1_VIRTUAL/UNIDAD%202%20An%C3%A1lisis%20de%20vulnerabilidad(1).pdf

2.3.3.2. Evaluación de vulnerabilidades[21]

Proceso que permite la medición de la seguridad de los sistemas y como los controles implementados pueden considerarse como eficientes, lo que permite mantener la confidencialidad, disponibilidad e integridad de la información, de ahí su importancia para este proyecto.

Existen diferentes metodologías y herramientas a emplearse en este proceso, una de ellas es el uso de herramientas automatizadas las cuales poseen un grupo de vulnerabilidades a identificar junto con procesos evaluativos y las medidas correctivas a implementarse, de igual manera permite cuantificar el impacto potencial presentado por las amenazas identificadas hacia los activos.

2.3.3.3. Evaluación del Riesgo[22]

El riesgo se define como la probabilidad de ocurrencia de unas consecuencias, en un sitio en particular y durante un tiempo de determinado, los cuales se pueden ver reflejados en la pérdida o deterioro de la información. Se obtiene de relacionar la amenaza con la vulnerabilidad de los elementos expuestos. Como se presenta en la fórmula de la ilustración 4.

Ilustración 5. Definición de riesgo

RIESGO = f (AMENAZA, VULNERABILIDAD)

Fuente: https://sena.blackboard.com/bbcswebdav/courses/32330017_1_VIRTUAL/UNIDAD%202%20An%C3%A1lisis%20de%20vulnerabilidad(1).pdf [23]

Esta expresión no es una fórmula matemática que se desarrolla con valores numéricos, sino que por el contrario es una expresión en la que se relacionan las variables amenaza y vulnerabilidad.

La determinación del grado o nivel de riesgo del proyecto, permite establecer los planes de acción a implementarse para prevenir la ocurrencia de una falla o minimizar las consecuencias de dichos eventos. Esta evaluación depende de la

[21] LASSO GARCÉS, L. A. Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S. Pasto: UNAD. [en línea]. 2015. P. 92. [Consultado: 20 de abril de 2018]. Disponible en internet. https://repository.unad.edu.co/handle/10596/345
[22] SENA, Ibíd. p. 9
[23] SENA, Ibíd. p. 9

aceptabilidad del riesgo o que es tolerable o no en la empresa.

En la siguiente ilustración es posible observar el proceso de análisis de riesgo con sus diferentes etapas, posibles responsables y resultados a obtener.

Ilustración 6. Proceso de análisis de riesgo

Fuente: http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/[24] (Traducción)

2.3.3.4. Tipos de riesgos

Los riesgos a los cuales se ve expuesta la información se pueden clasificar de la siguiente manera[25]:

[24] NOTICIASSEGURIDAD.COM. ¿Cómo hacer análisis de vulnerabilidades informáticas? [en línea] 2 de 3 de 2016. [Consultado: 20 de abril de 2018]. Disponible en internet: http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

[25] LASSO, Ibíd. p. 10

- Riesgos de Integridad. Relacionada con el diseño y uso de la interface del usuario, el procesamiento y manejo de errores, la administración de cambios y la información en general, entre otros.
- Riesgos de Relación. Encaminada al uso pertinente de la información originada por una aplicación.
- Riesgos de Utilidad. La cual depende del momento específico en el que se afronta el riesgo, inicialmente se debe considerar el periodo antes de la ocurrencia de fallas mediante el direccionamiento de sistemas y posteriormente la aplicación de métodos para la recuperación y reparación de información que disminuyan las fallas de los sistemas y los planes orientados hacia el control de riesgos.
- Riesgos en la infraestructura. Representado en la carencia de una infraestructura tecnológica eficaz que minimice el riesgo. Pueden surgir principalmente en los procesos: planeación organizacional, administración de seguridad, el manejo de operaciones de red y computacionales, al igual que en la administración de sistemas de bases de datos, información, definición de las aplicaciones y las reglas de negocio.
- Riesgos de Seguridad General. Aquellos que se orientan en el modelo general de la seguridad y la minimización del riesgo, principalmente orientado hacia riesgos relacionados con factores físicos.

2.3.4. Metodología de análisis de vulnerabilidades informáticas (PESA)[26]

Esta metodología de análisis de vulnerabilidades informáticas, se centra en la protección del total de activos informáticos de las empresas que presenten predisposición ante actividades mal intencionadas por parte de personas internas o externas. El proceso consta de etapas iterativas, dado que la existencia de riesgos es una constante que evoluciona generando nuevos riesgos para las empresas. Con relación a la metodología PESA, esta se estructura en diferentes módulos así:

MODULO: PLANEAR: Se comienza con el desarrollo de un módulo de planeación, en el que se establecen requerimientos, planes y prioridades necesarias para implantar la metodología.

MODULO: EVALUAR: Se continúa con la realización del análisis de vulnerabilidades de los datos, redes, aplicaciones, bases de datos y dispositivos móviles, para lo cual se emplean servicios de escaneo de vulnerabilidades. Entre los posibles pasos den módulo de evaluación pueden ser:

- Hacer análisis de los posibles riesgos, identificar las amenazas y las vulnerabilidades tanto físicas como lógicas.

[26] noticiasseguridad.com Óp. Cit, p. 10

- Revisar configuración de los sistemas operativos, las aplicaciones instaladas, archivos de registros y los dispositivos que hacen parte de la arquitectura de red.
- Autentificación de los usuarios y controlar sus accesos. Monitorear las actividades de los usuarios.
- Revisión de planes, políticas de seguridad y planes de contingencia establecidos.
- Emplear pruebas de testeo para evaluar las vulnerabilidades

MODULO: SEGURO: En este módulo se entrega el posible plan de seguridad a implementar, se definen los controles de seguridad. En esta etapa se requiere considerar la apreciación del cliente sobre la inversión en la búsqueda del aseguramiento de la arquitectura de la red, en la que se encuentran también los equipos conectados a la red, dispositivos móviles y aplicaciones empresariales. En la etapa de implantación se debe capacitar a los empleados del cliente con un curso de análisis de riesgos informáticos y otro curso de análisis de vulnerabilidades informáticas.

MODULO: AUDITAR: Permite verificar la implementación y el buen desempeño de los sistemas de seguridad. La auditoría determina si los sistemas de seguridad cumplen a cabalidad la tarea de salvaguardar los activos al igual que si mantiene la confidencialidad, integridad, disponibilidad de la información. En el desarrollo del presente proyecto se alcanzará esta etapa mediante la llegará de un posible plan de seguridad a implementar.

2.3.5. Pruebas de penetración

El termino Test de penetración o en inglés "Penetration Tests" es un procedimiento que se realiza a través de un conjunto de técnicas y métodos que simulan un ataque a un sistema lo cual permite evaluar la seguridad existente en ese momento. Esta práctica se considera como necesaria debido a que siempre existe la posibilidad de sufrir algún tipo de ataque informático, lo que requiere descubrir las posibles fallas mediante el uso de las herramientas, para con ello defenderse de posibles ataques.

Existen múltiples herramientas de pruebas de penetración entre las que se encuentran scanners de puertos, algoritmos de descifrado de claves, sistemas de intrusión por fuerza bruta, seguidores de red, como también herramientas de escaneo de vulnerabilidades de aplicaciones web y mucho más.

2.3.5.1. Tipos de pruebas de penetración[27]

Es posible caracterizar las pruebas de penetración con base en las siguientes perspectivas:

- Pruebas de penetración con objetivo: se centran en encontrar vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.
- Pruebas de penetración sin objetivo: se orientan en la examinación de la totalidad de los componentes de los sistemas informáticos.
- Pruebas de penetración a ciegas: Se caracterizan por emplear únicamente la información pública disponible sobre la organización.
- Pruebas de penetración informadas: En estas se emplea la información privada, la cual ha sido previamente otorgada por la compañía acerca de sus sistemas informáticos. Para este tipo de pruebas se procede a simular ataques que pudieran ser ejecutados por elementos internos de la organización los cuales tengan acceso a información privilegiada.
- Pruebas de penetración externas: Tienen como objetivo evaluar la seguridad perimetral de la organización, razón por la cual se realizan el exterior de las instalaciones de la empresa.
- Pruebas de penetración internas: Por el contrario, a las anteriores estas se realizan dentro de las instalaciones de la organización con y buscan evaluar las políticas y los mecanismos internos de seguridad de la organización.

Otro tipo de clasificación que puede ser asignado a las pruebas de penetración tiene relación la ubicación del atacante en relación con el sistema atacado y pueden ser:

- Black-box: El ejecutor de la prueba no tiene conocimiento del sistema. Se utiliza cuando se requiere obtener un punto de vista de un agente externo a la compañía.
- White-box: El ejecutor de la prueba tiene un conocimiento previo del funcionamiento del sistema, al igual que información relacionada con la arquitectura de la red, los sistemas operativos utilizados, entre otros aspectos. Si presenta el inconveniente de no existir un atacante externo se debe orientar para reproducir o simular el peor escenario posible, debido a que es el caso en el que un atacante ya cuenta con información antes de ingresar al sistema.
- Gray-box: En este caso el evaluador simula un empleado interno, el cual tiene acceso al sistema mediante un usuario y clave de los sistemas. La idea es encontrar posibles problemas que puedan ser aprovechados por usuarios internos.

[27] RAMOS, Jorge. Luis. Pruebas De Penetración O Pent Test. [en línea] 06 de 2013. [Consultado: 22 de abril de 2018]. Disponible en internet: http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a14.pdf

La realización de las pruebas requiere la ejecución de una serie de etapas las cuales pueden ser consideradas como el marco metodológico de su realización, las etapas a efectuar se presentan en la siguiente tabla.

Tabla 2. Etapas de pruebas de penetración

ETAPAS PRUEBAS DE PENETRACIÓN	
ETAPA	DESCRIPCIÓN
RECOLECCIÓN DE INFORMACIÓN	Se pretende recolectar gran volumen de información oficial.
EXAMINAR EQUIPAMIENTO INFORMÁTICO	Para este caso se emplearán • Querying System (sistema de consulta), y documentación DNS. • Se emplea: TraceRoute (marca el trayecto de la red), Transmisión de sector Sistema de Nombre de Dominio (brindan información de los hosts existentes en el sector y de la dirección IP). • Rastreo de puertos. El mapeo ofrece información sobre que puertos percibe un host. Considerándose como que todo puerto abierto es muy vulnerable.
ANALIZAR LOS EQUIPOS	Se aplican herramientas de escaneo de puertos y finger printing para adquirir información acerca de la versión y sistema operativo que están montados.
EXAMINAR LOS PROGRAMAS	Aplicando estudio útil, ordenado, ejecutando ataques contra la confirmación de la identidad de un individuo, permisos, información, condición última de los procedimientos y los usuarios

Fuente: Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S [28]

2.3.5.2. Herramientas penetración

Para el desarrollo del presente proyecto se emplearán las siguientes herramientas

[28] LASSO, Óp. Cít p. 10

de penetración:

- Técnicas de escaneo de puertos y uso del NMAP[29]: El escaneo de puertos es una técnica empleada para conocer que puertos están abiertos o cerrados y los servicios que son ofrecidos, de igual manera permite chequear la existencia de un firewall al igual que la verificación del funcionamiento del mismo, entre otras utilidades. Sin embargo, estas características brindan a los atacantes información que puede ser empleada para la ruptura de la seguridad de un sistema al igual que realizar un análisis preliminar del mismo.
- Por su parte NMAP es una aplicación que permite visualizar los equipos activos de red y obtener información relacionada principalmente con puertos abiertos. Este aplicativo es multiplataforma y la versión para Windows se puede descargar sin problema, se puede instalar en sistemas Linux o con la ejecución del comando sudo apt-get install.
- En este estudio se iniciará empleando NMAP para identificar que equipos hay en la red de ordenadores, recopilando la información relacionada con su sistema operativo y la configuración existente de los puertos.
- Identificación de vulnerabilidades y OpenVAS: Open Vulnerability Assessment System conocido comúnmente como OpenVAS, este se refiere al framework desarrollado por (www.openvas.org) que se ha destinado a ofrecer servicios de escaneo y administración de vulnerabilidades. OpenVAS se compone de un conjunto de servicios y herramientas, siendo su centro un escáner de vulnerabilidades[30].
- OpenVAS posee una arquitectura conformada por el OpenVAS Manager o servicio central y se encarga del escaneo completo de vulnerabilidades, este además controla una base de datos que contiene tanto la configuración como los datos resultados del escaneo.
- Además, posee módulos orientados a diferentes tipos de clientes, se encuentra el Greenbone Security Assistant (GSA) que emplea un navegador para convertir trazas del protocolo OMP directamente a HTML; de igual manera, es posible emplear la interfaz propia del aplicativo u OpenVAS CLI, que contiene la línea de comandos que permite utilizar el manager.

En la siguiente tabla se presenta un resumen de los módulos que compone OpenVAS.

[29] UNIVERSIDAD NACIONAL DE LA PATAGONIA “S.J. BOSCO”-FAC. DE INGENIERÍA – DTO. INFORMÁTICA. Escaneo de puertos. [en línea] 2012. [Consultado: 23 de abril de 2018]. Disponible en internet: http://www.ing.unp.edu.ar/asignaturas/rytd/Anexos/RyTD_Anexo_TP6_Escaneo-Puertos_IPTools.pdf

[30] OPENVAS.ORG. openvas.org. [en línea]. [Consultado: 25 de abril de 2018]. Disponible en internet: http://www.openvas.org/documentation.html

Tabla 3. Comparativa módulos OpenVAS

Scanner	Manager	GSA	CLI
Escaneo de múltiples objetivos concurrentemente	Uso de SQL Database y soporte SSL	Cliente para OMP y OAP	Cliente para OMP
Uso del protocolo OTP	Tareas de escaneo concurrentes	HTTP y HTTPS	Multiplataforma (Linux, Windows, etc…)
Soporte SSL	Programación de escaneos	Servidor web interno	Plugin Nagios
Soporte WMI opcional	Parada, pausa y reanudación de escaneos	Sistema de ayuda online	
	Estado y sincronización de fuentes.	Soporte multilenguaje	
	Administración de falsos positivos		
	Manejo de usuarios		

Fuente: http://oa.upm.es/32786/1/TFG_javier_rios_yaguez.pdf [31]

La Tabla 4 presenta el conjunto de herramientas a emplear en el proyecto al igual que el objetivo que se busca alcanzar con cada una de ellas.

Tabla 4. Relación de herramientas con pruebas a realizar

	Nmap	OpenVas
Tipo de Prueba	Sondeo Ping	Escaneo y análisis de vulnerabilidades de hosts
Objetivo	Escanear puertos de los equipos de cómputo de la red para determinar su estado (Abiertos, cerrados o custodiados)	Realizar pruebas de seguridad sobre las terminarles o el servidor a través de un equipo remoto.

Fuente: El presente documento.

2.3.6. Técnicas de intrusión

Se considera como el conjunto de acciones que buscan hacer uso de las vulnerabilidades presentes en la seguridad de los sistemas de información. Sin embargo, es necesario que este conjunto de prácticas sea conocido también por parte de los profesionales encargados de la seguridad de la información, lo anterior con el propósito de la realización de las actividades de hackeo ético que busquen brindar protección al igual que salvaguardar la información contenida en los sistemas de información existentes dentro de una compañía, de forma efectiva y precisa.

[31] YÁGUEZK, J. R. Técnicas y herramientas de análisis de vulnerabilidades [en línea]. 18 de 11 de 2014. [Consultado: 28 de abril de 2018]. Disponible en internet: http://oa.upm.es/32786/1/TFG_javier_rios_yaguez.pdf

Como se expuso anteriormente algunas de las técnicas de intrusión empleada por los atacantes son:

Escaneo de Puertos[32]: El escaneo de puertos es una técnica empleada para conocer que puertos están abiertos o cerrados y los servicios que son ofrecidos, de igual manera permite chequear la existencia de un firewall al igual que la verificación del funcionamiento del mismo, entre otras utilidades. Sin embargo, estas características brindan a los atacantes información que puede ser empleada para la ruptura de la seguridad de un sistema al igual que realizar un análisis preliminar del mismo.

Entre los vectores de riesgos que pueden ser encontrados dentro de los sistemas informáticos se presenta la mala administración de puertos, dando como resultado puertos abiertos o no supervisados que permiten el flujo de información no permitido dentro de la compañía.

En contraposición a este tipo de técnicas se define un conjunto de normas y filtros que se encargan de definir políticas dentro de la administración de la empresa sobre el uso y permisos definidos tanto para los funcionarios, como para los equipos de red, logrando con esto dar acceso a una terminal únicamente a través de puertos protegidos por procedimientos de protección.

2.3.7. Mitigación y Gestión de Riesgos[33].

Se debe considerar que la gestión del riesgo comprende tres procesos inicialmente un análisis de riesgos el que conlleva a la identificación de estos, siguiendo con un proceso de mitigación de riesgos en el cual se busca reducir o eliminar el riesgo y la evaluación o valoración continúa la cual busca la verificación de la no existencia de nuevos riesgos o el no incremento de aquellos que no han sido posible eliminar. Debe existir una persona responsable la cual determine cuándo el riesgo residual tiene un nivel aceptable o cuándo son requeridos controles adicionales que debieran

[32] UNIVERSIDAD NACIONAL DE LA PATAGONIA. Op. Cit. p. 16

[33] COLOMBIA, R. D. ANEXO 2: Metodología De Gestión Del Riesgo - Modelo De Seguridad De La Información Para La Estrategia De Gobierno En Línea. [en línea]. 12 de 2010. P. 50. [Consultado: 28 de abril de 2018]. Disponible en internet: http://www.vive.gobiernoenlínea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ANEXO_2__Metodologia_de_Gestion_del_Riesgo.pdf

implementarse para reducir o eliminar el riesgo residual.

Con base en lo anterior se puede definir que la gestión del riesgo es "*el proceso que permite a los administradores de TI establecer un balance entre los costos operativos y económicos de las medidas de protección y su efectividad versus el logro de los objetivos de la entidad y la protección real brindada a los sistemas y datos que soportan tales objetivos*"[34]**.**

Por su parte, la ejecución de medidas de intervención dirigidas a reducir o disminuir el riesgo existente se considera como la mitigación de un riesgo; esta asume que en muchas circunstancias no es posible, ni factible controlar totalmente el riesgo existente, por lo cual busca reducirlo a niveles aceptables y factibles. De igual manera, la mitigación de riesgos de desastre puede operar en el contexto de la reducción o eliminación de riesgos existentes, o aceptar estos riesgos los cuales por medio de preparativos buscar disminuir las pérdidas y daños causados por la activación del riesgo. De aquí que las medidas de mitigación tienen como fin[35]:

- evitar que se presente un fenómeno peligroso, reducir su peligrosidad o evitar la exposición de los elementos ante el mismo
- disminuir sus efectos sobre la información, reduciendo la vulnerabilidad que exhiben.

Por su parte, la mitigación es el resultado de la combinación de una decisión a nivel político con la aceptación del riesgo aceptable obtenido en un análisis extensivo del mismo y bajo el criterio de que dicho riesgo no es posible reducirlo totalmente.

2.3.8. Control de acceso a la red[36]

El Control de Acceso a la Red permite el control del acceso a red por parte de los usuarios, mediante la verificación del cumplimiento de las políticas de seguridad establecidas con lo que se pueda prevenir amenazas como la exposición a virus, la salida no autorizada de información, accesos no autorizados, entre otros. Sin

[34] COLOMBIA. Óp. Cít. p. 14
[35] CRIDLAC.ORG. Mitigación (Reducción O Atenuación) Del Riesgo. [en línea] 2008. P. 50. [Consultado: 28 de abril de 2018]. Disponible en internet: http://www.cridlac.org/VCD/files/page336.html
[36] INGENIA. Control de acceso a red (NAC). [en línea] 2018. [Consultado: 2 de mayo de 2018]. Disponible en internet: https://www.ingenia.es/es/servicio/control-de-acceso-red-nac

embargo, las empresas centran su estrategia de seguridad en la protección de los equipos de red y su información de atacantes externos, no dando la suficiente importancia a los elementos existentes en la red interna, por lo cual y si lo que se desea es mantener pleno control de la red es necesario la definición de un control de acceso a red (NAC), el cual permite realizar cuatro acciones principales (Ver *Tabla 5*):

Tabla 5. Acciones a realizar con un NAC

Ver	Acceder
Permiten una visibilidad completa de la red, comprobando qué dispositivos se están conectando y de qué tipo, de quién son, quién lo está usando, que aplicaciones está ejecutando o en qué estado se encuentra (antivirus, parches del sistema operativo, agentes de seguridad, configuración, etc.).	Según las reglas definidas, el sistema permite el acceso a aquellos dispositivos que cumplen la política de seguridad (dispositivos conocidos, antivirus actualizado, ejecutando aplicaciones corporativas, etc.). Con los dispositivos no autorizados se puede realizar todo tipo de acciones: notificar al usuario y/o al administrador, restringir o bloquear completamente el acceso a la red, etc. También se definen políticas para el acceso de invitados, determinando quién y cuándo puede acceder y a qué.
Remediar	**Proteger**
En aquellos dispositivos que no cumplen completamente nuestra política de seguridad, se puede remediar el sistema operativo o el antivirus, reparar configuraciones, parar/arrancar aplicaciones, deshabilitar dispositivos conectados, etc.	El sistema detecta comportamientos anómalos de equipos conectados a la red, permitiendo el bloqueo interno de malware, intrusiones y ataques.

Fuente: https://www.ingenia.es/es/servicio/control-de-acceso-red-nac [37]

2.3.9. Estándar ISO 27002 para la gestión de la seguridad de la información

Los estándares internacionales relacionados con la gestión de riesgos de sistemas de información son muchos, sin embargo el presente estudio se centrara en la norma ISO/IEC 27002:2013, que es un estándar en el cual se definen los términos de controles de seguridad de la información.

Este estándar proporciona directrices en la evaluación y aplicación de las normas de seguridad de la información de una organización, al igual que las prácticas de

[37] INGENIA. Óp. Cít. P.15

gestión de seguridad de la información, entre las que se incluyen la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo en la seguridad de la información[38].

2.3.10. Dominio de control estudiado del Estándar ISO 27002 para la evaluación de seguridad[39]

Como se mencionó anteriormente, el objetivo de la norma ISO 27002 busca controlar el acceso a un sistema de información mediante la definición de un conjunto de restricciones y excepciones a la información al igual que lo realiza todo Sistema de Seguridad de la Información. Ahora, con relación al acceso no autorizado al Sistema de Gestión de Seguridad de la Información según la norma ISO 27002, se debe implantar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información y se deben declarar de manera clara y formal al igual que la realización de los controles respectivos sobre su cumplimiento. Entre los aspectos a tener en cuenta se tiene las etapas de ciclo de vida de los accesos de los usuarios en todos los niveles, incluido su registro inicial hasta la privación final de los derechos de todos los usuarios que ya no requieren el acceso, estos aspectos son considerados en la norma en el domino Control de Acceso, el cual tiene las siguientes características[40].

- **Requisitos del negocio para el control de acceso**

Objetivo: controlar el acceso a la información.

El acceso a la Información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de seguridad y del negocio.

Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

---

[38] MOLINA MIRANDA, María Fernanda. Propuesta De Un Plan De Gestión De Riesgos De Tecnología Aplicado En La Escuela Superior Politécnica Del Litoral. [en línea] 2015. 89. P. [Consultado: 2 de mayo de 2018]. Disponible en internet: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

[39] ISO27002. Control de Accesos. [en línea] 2012. [Consultado: 2 de mayo de 2018]. Disponible en internet: https://iso27002.wiki.zoho.com/11ControlAccesos.html

[40] ISO27002.wiki.zoho.com, Ibid.

- **Gestión del acceso de usuarios**

Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

Se deberían establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos deberían comprender todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se debería poner atención especial, según el caso, a la necesidad de controlar la asignación de derechos de acceso privilegiado que permiten a los usuarios anular los controles del sistema.

- **Responsabilidades de los usuarios**

Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de Información.

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad.

Se deberla concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

Es recomendable implementar una política de escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de Información.

- **Control de Acceso a las Redes**

Objetivo: evitar el acceso no autorizado a los servicios en red.

Es recomendable controlar el acceso a los servicios en red, tanto internos como externos.

El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

  - existen interfaces apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones. y las redes públicas:

- se aplican mecanismos adecuados de autenticación para los usuarios y los equipos.
- se exige control de acceso de los usuarios a los servicios de información.

- **Control de Acceso al Sistema Operativo**

Objetivo: evitar el acceso no autorizado a los sistemas operativos

Se recomienda utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

- autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;
- registrar intentos exitosos y fallidos de autenticación del sistema;
- registrar el uso de privilegios especiales del sistema;
- emitir alarmas cuando se violan las políticas de seguridad del sistema;
- suministrar medios adecuados para la autenticación cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

- **Control de Acceso a las aplicaciones y a la información**

Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de aplicación.

Se deberían usar medios de seguridad para restringir el acceso a los sistemas de aplicación y dentro de ellos.

El acceso lógico al software de aplicación y a la información se debería restringir a usuarios autorizados.

Los sistemas de aplicación deberían:

- controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso;
- suministrar protección contra acceso no autorizado por una utilidad, el software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación:
- no poner en peligro otros sistemas con los que se comparten los recursos de información

- **Computación Móvil y Trabajo Remoto**

Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móvil y de trabajo remoto.

La protección necesaria debería estar acorde con los riesgos que originan estas· formas específicas de trabajo. Cuando se usa la computación móvil, se deberían tener en cuenta los riesgos de trabajar en un entorno sin protección y aplicar la protección adecuada. En el caso del trabajo remoto, la organización debería aplicar protección en el sitio del trabajo remoto y garantizar que se han establecido las disposiciones adecuadas para esta forma de trabajo.

Una vez identificados y considerados el dominio y sus componentes, para el proyecto se evaluará el dominio con base en la siguiente estructura:

Dominio: Control de acceso
Requisitos de negocio para el control de acceso: Política de Control de Acceso.
Gestión del acceso a los usuarios
Registro de usuarios.
Gestión de contraseñas para usuarios.
Responsabilidad de los usuarios
Uso de contraseñas.
Equipo de usuario desatendido.
Control de Acceso a la Red
Autenticación de usuarios para conexiones externas.
Identificación de los equipos en las redes.
Protección de los puertos de configuración y diagnóstico remoto.
Separación en las Redes.
Control de Conexiones a las Redes.
Control del Enrutamiento en la Red.
Control de acceso al sistema operativo
Procedimientos de registro de inicio seguro.
Identificación y autenticación de usuarios.
Sistema de gestión de contraseñas.
Uso de las utilidades del sistema.
Control de acceso a las aplicaciones y a la información
Aislamiento de sistemas sensibles.
Computación móvil y trabajo remoto
Trabajo remoto.

3. DISEÑO METODOLÓGICO

Para el desarrollo de este capítulo se desarrollan los aspectos que tienen que ver con el tipo de investigación a realizar, entre los que se encuentran el tamaño y tipo de muestra a analizar, de igual manera que el conjunto de herramientas y procedimientos empleados para la identificación de vulnerabilidades existentes en el Sistema de Gestión Empresarial de la compañía JARDINES CRISTO REY LTDA., mediante testeo de red.

3.1. TIPO DE INVESTIGACIÓN

Para este proyecto se ha definido que el tipo de investigación empleado es el exploratorio con el cual, al sistema de cómputo o plataforma informática bajo estudio, se le realiza un proceso de análisis el cual permite identificar las vulnerabilidades presentes en el Sistema de Gestión Empresarial, de igual manera se hace uso de la investigación aplicada dado que tomando como base los hallazgos, se procede a la elaboración de una propuesta de solución que se acoja a lo expuesto por los conceptos, normas y técnicas relacionados con la seguridad informática.

3.2. POBLACIÓN

La población a estudiar se compone de los sistemas informáticos, estaciones de trabajo ubicados en las oficinas de la compañía JARDINES REY LTDA., presente en la
Ilustración *2* e Ilustración 3.

3.3. INSTRUMENTOS.

- **Fuentes primarias:**

Por definición estas son aquellas que ofrecen una demostración o certeza sobre el tema de estudio, en general estas fuentes ofrecen una visión específica del suceso en estudio, permitiendo la transmisión de ideas nuevas, admitiendo apreciación de la sociedad.

La característica principal que este tipo de información tiene es el ser considerada como nueva o inédita y debe ser adquirida con base en la experiencia, debido a que

ha sido por primera vez transmitida o adquirida y no ha sufrido algún proceso de edición o deducida o explorada por otro autor, también se considera como el resultado de un proceso investigativo o de una función especialmente novedosa. Entre las fuentes primarias a emplearse se aplicarán:

- **Pruebas de Pentesting**

Conocidas también como pruebas de penetración, se consideran como actividades propias del hacking ético, dichas actividades se pueden realizar de forma local o remota y facilitan reconocer vulnerabilidades en medios informáticos, con ellas se logra evaluar el riesgo y valorar los procedimientos de seguridad empleados actualmente en la compañía, de igual manera presenta los lugares o condiciones en los cuales existen fallas de seguridad o es escasa y que además se puede emplear para justificar la ejecución de un proceso de mejora o actualización, la asignación de mayor presupuesto para seguridad o la validación de la valoración de los riesgos.

Este tipo de pruebas se pueden definir en dos clases, las primeras conocidas como formales cuyo objetivo es comprobar posibles falencias en las estrategias de seguridad; para cumplir su función son sujetas a técnicas que afectan los datos susceptibles de la empresa y en segundo lugar las informales que se encaminan por propósitos tecnológicos de la estructura de los sistemas de información.

- **Fuentes Secundarias:**

En esta colección de fuentes se encuentran aquellas que contienen información estructurada, formalizada, en la que se presentan los resultados de estudios previos al igual que textos originales, son empleadas para ratificar los hallazgos obtenidos en el análisis, al igual que facilitan la extensión del contenido de la información de una fuente primaria de la misma manera que proyectar los estudios realizados.

Estas fuentes tienen como característica que son elaboradas por personas o investigadores que no se encuentran en contacto directo con el proyecto de estudio y se encuentran disponibles en la documentación empresarial, libros, el Internet y Artículos de revistas entre otros.

La funcionalidad y el empleo de estas fuentes se centran en la construcción de los

elementos teórico-prácticos empleados en el desarrollo del proyecto.

Para la obtención de la información se aplicará la metodología propuesta por Serrato[41], en la cual se definen los pasos a ejecutarse para el rastreo y evaluación de vulnerabilidades en sistemas de gestión de información a nivel lógico lo que a su vez se ve soportado en la utilizando de herramientas de software libre. En esta metodología se definen las actividades a realizarse para hacer un levantamiento de información iniciando con la "*identificacion de puertos y servicios; acto seguido, se procede a hacer un análisis de vulnerabilidad*"[42].

Para la ejecucion de las pruebas de penetracion se empleara la metodologia propuesta por Lasso y que contempla las siguientes etapas (Ver

[41] Serrato Polania. Óp. Cit. p2
[42] Serrato Polania. Ibíd.

Tabla *6*):

Tabla 6. Metodología para pruebas de penetración

ETAPAS PRUEBAS DE PENETRACIÓN	
ETAPA	DESCRIPCIÓN
RECOLECCIÓN DE INFORMACIÓN	En esta etapa se procede a determinar los blancos y las amenazas, al igual que la información necesaria para determinar el tipo de pruebas a emplearse, para lo que se realizara[43]: • Detección de equipos • Detección del mapa de la red • Detección de servicios y versiones • Detección de debilidades
EXAMINAR EQUIPAMIENTO INFORMÁTICO	Para este caso se emplearán • Querying System (sistema de consulta), y documentación DNS. • Se emplea: TraceRoute (marca el trayecto de la red), Transmisión de sector Sistema de Nombre de Dominio (brindan información de los hosts existentes en el sector y de la dirección IP). • Rastreo de puertos. El mapeo ofrece información sobre que puertos percibe un host. Considerándose como que todo puerto abierto es muy vulnerable.
ANALIZAR LOS EQUIPOS	Para ellos se emplearan herramientas de escaneo de puertos y finger printing lo que permitirá información acerca de la versión y sistema operativo que se están utilizando.
EXAMINAR LOS PROGRAMAS	Para lo cual se realizara un estudio que mediante la ejecución de ataques que verifiquen la confirmación de identidad de un individuo, los permisos concedidos sobre la información, y por último los procedimientos y los usuarios

Fuente: Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S[44]

[43] ISACA. (04 de 2009). Penetration Testing, Conceptos generales y situación actual. Obtenido de https://www.isaca.org/chapters8/Montevideo/Events/Documents/penetration%20testing%20-%20conceptos%20generales%20y%20situacin%20actual.pdf

[44] LASSO, Óp. Cít p. 10

4. PRUEBAS DE PENETRACIÓN

Una vez identificadas las etapas y actividades a realizarse mediante la aplicación de la metodología se procede a su aplicación dando como resultado los siguientes apartes.

4.1. IDENTIFICACIÓN DE MACRO-PROCESOS, PROCESOS Y SERVICIOS.

Tomando como punto de partida las condiciones iniciales del proyecto se puede afirmar que en la actualidad Jardines Cristo Rey LTDA., no cuenta con un Sistema de Gestión de la seguridad de la Información, existe un procedimiento de seguridad de base de datos, encargado de realizar y velar por las copias de seguridad generadas a diario, la oficina de sistemas cuenta con acceso restringido, solo personal autorizado, aunque los funcionarios de otras áreas no poseen restricción de acceso.

Para dar claridad con respecto a la asignación de roles y funciones con respecto a la información, los componentes de red y la seguridad de los mismos, se identifican los macro procesos y procesos soportados por el área de sistemas, lo que da como resultado:

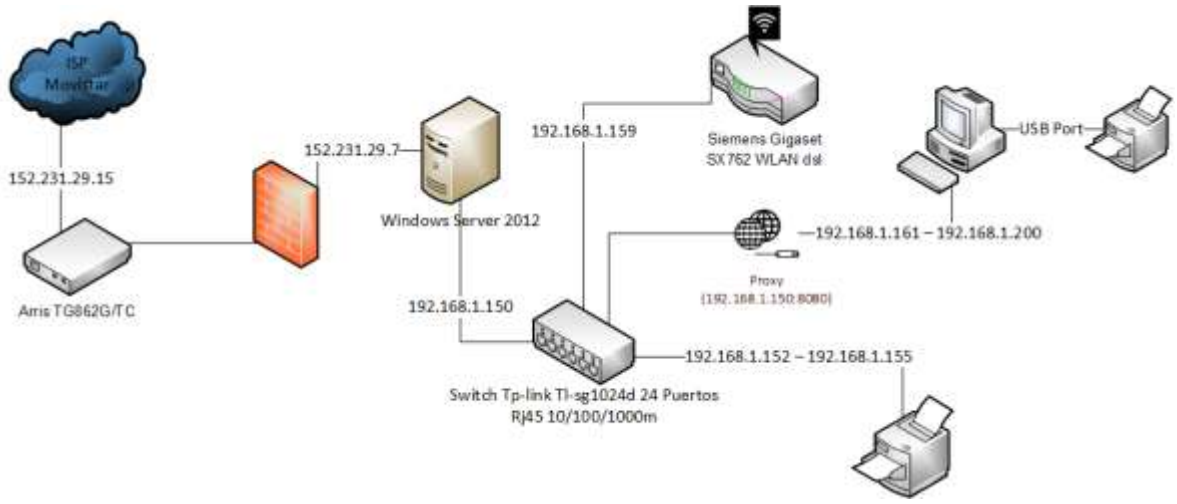
Tabla 7. Macro procesos, Procesos y Servicios - Jardines Cristo Rey

Macro Proceso	***Sistema Gestión Empresarial***
	Realizar las actividades necesarias para mantener una operatividad del sistema de gestión Empresarial, tanto en comunicación de redes, equipos, transmisión de datos y almacenamiento y seguridad de la información. Las áreas interrelacionadas son: • Gerencia • Cartera • Contabilidad • Kardex
Proceso	***Soporte***
	Encarado del prestar atención a solicitudes en TI
Servicios	• Resolver incidencias tecnológicas de las diferentes áreas • Brindar soporte técnico a los dispositivos tecnológicos como computadores, impresoras, scanner • Realizar las adecuaciones tecnológicas en las áreas de la entidad
Proceso	***Administración***
	Administra los servicios TI como servidores de correo, de archivos, copias de seguridad
Servicios	• Mantener y administrar el servidor central de la compañía • Gestionar los diferentes sistemas de información • Realizar diferentes copias de seguridad de los computadores en la entidad • Apoyar los movimientos de tipo tecnológico que se realicen en las áreas de la entidad
Proceso	***Desarrollo tecnológico***
	Desarrollo de nuevas interfaces, modelamiento y ajustes a programas existentes.
Servicios	• Atender solicitudes de tipo incidencias sobre los sistemas de información que tiene la entidad • Corregir, ajustar y arreglas los diferentes problemas que se presentan en la plataforma tecnológica de la entidad

Fuente: El presente documento

4.2. ARQUITECTURA DE RED

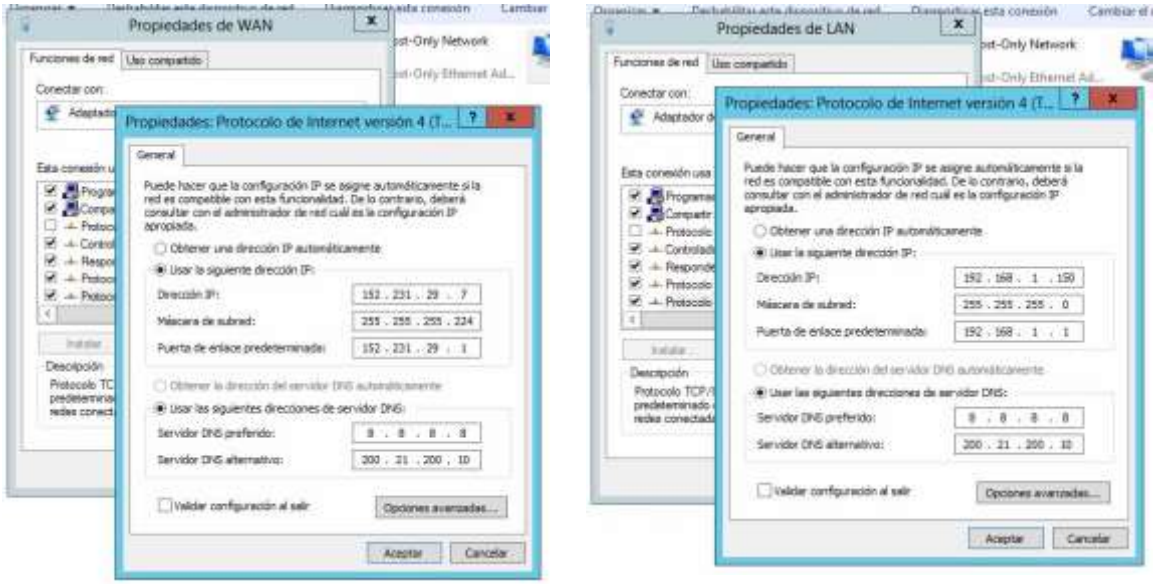
Ilustración 7. Topología de red Jardines Cristo Rey 192.168.1.0/24



Fuente: El presente documento

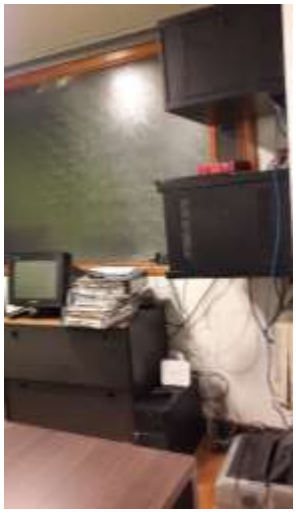
La red 192.168.1.0/24 la cual es el objeto de estudio se enfoca en el servidor de gestión documental, el cual se identifica mediante dos direcciones IP, una conectada al proveedor de servicios de Internet (ISP) identificada con la dirección IP 152.231.29.7 y otra interfaz de red conectada a la intranet de la compañía con IP 192.168.1.150 (Ver *Foto 1*), los componentes hardware se ubican en el área contable de la compañía, donde también se localiza la infraestructura de conexión de red, lo que permite el control de acceso físico, previniendo accesos no autorizados.

Foto 1. Configuración direcciones IP Servidor Jardines Cristo Rey Ltda.



Fuente: El presente documento

Foto 2. Centro de cableado Jardines Cristo Rey Ltda.



Fuente: El presente documento

Topología física: Como se puede evidenciar en la Foto *3*, en la actualidad el ISP contratado es la compañía MOVISTAR, que recoge las solicitudes del servidor de la compañía para direccionarlas al router de control acceso Internet (Ver *Foto 4*), esta configuración se aplica para prevenir el acceso a sitios web no autorizados, mediante el filtrado de paquetes, por su parte las terminales de trabajo, se

interconectan a un switch de distribución de red lo que permite el acceso de las demás áreas de trabajo de la red LAN.

Foto 3. Modem ISP Jardines Cristo Rey Ltda.

Fuente: El presente documento

Foto 4. Enrutamiento tráfico de conexiones - Jardines Cristo Rey Ltda.

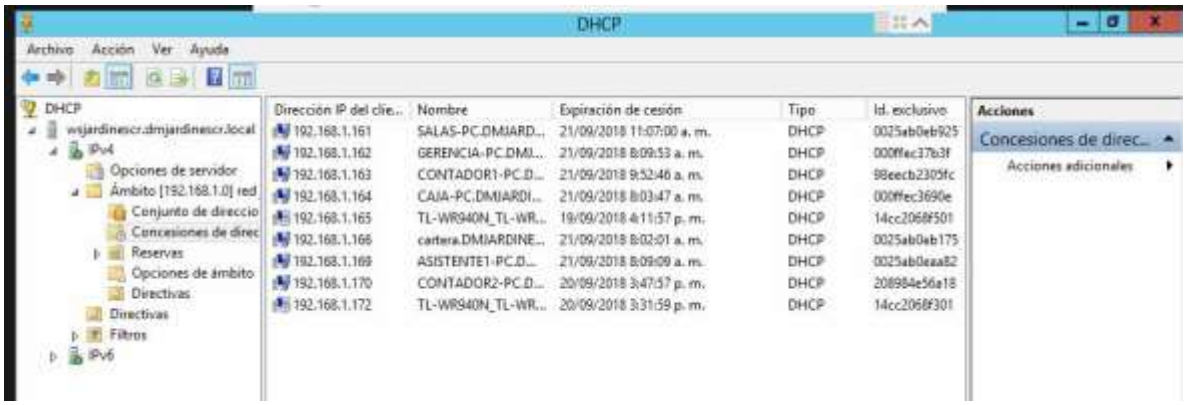
Fuente: El presente documento

En lo relacionado a la prestación de servicios, la topología lógica empleada es la de cliente/servidor, para el caso particular del sistema de gestión empresarial, el equipo central funciona como un servidor de aplicaciones compartiendo el aplicativo CAFÉ, al igual que la comunicación con un cliente de base de datos y un servidor de direcciones IP (DHCP Ver *Foto 5*, *Foto 6*), todo lo anterior sobre la red LAN de la compañía.

Foto 5. Ámbito de direcciones IP para terminales de trabajo - Jardines Cristo Rey Ltda.

Fuente: El presente documento

Foto 6. Concesión de direcciones IP para terminales de trabajo - Jardines Cristo Rey Ltda.



Fuente: El presente documento

4.3. METODOLOGÍA PARA PRUEBAS DE PENETRACIÓN

Una vez finalizada la etapa de identificación de los equipos a evaluar se determina que, según la topología lógica de la red, esta centra sus funciones en el equipo servidor razón por la cual será sobre este sobre el que se centren las pruebas de penetración y es sobre este equipo que se aplican estas mediante el aplicativo OpenVas, configurado previamente (Ver

Anexo 1), de igual manera es este framework el encargado de la realización y ejecución de las pruebas de penetración, lo que se observa con mayor detalle en el Anexo 2.

4.4. RESULTADOS PRUEBAS DE PENETRACIÓN

El uso del aplicativo en conjunto con las demás pruebas propuestas en el aparte 3.3 del presente documento da como resultado lo siguiente:

Tabla 8.Pruebas y resultados

Etapa	Proceso	Resultados	Evidencias
Escaneo de la red.	Mediante el uso de la herramienta Nmap, se escanea la red identificada con las IP 192.168.1.0/24 de Jardines Cristo Rey Ltda., con el fin de identificar y detectar puertos abiertos y los servicios activos en los equipos terminales de datos (DTE) que se encuentren en funcionamiento.	El resultado del proceso de mapeo dio como resultado 9 direcciones IP activas, correspondientes a los hosts disponibles.	Anexo 3 Evidencia 8
		192.168.1.150, Windows Server 2012, puertos abiertos 53, 80, 88, 135, 139, 389, 443, 445, 464, 593, 636, 2869, 3268, 3389, 49152, 49153, 49154, 49156, 49157, 49158, 49163	Anexo 3 Evidencia 1 Evidencia 9
		192.198.1.161, Windows 7 Profesional, puertos abiertos 139.	Anexo 3 Evidencia 10
		192.198.1.162, Windows 7 Profesional, puertos abiertos 135, 139.	Anexo 3 Evidencia 10
		192.198.1.163, Windows 7 Profesional, puertos abiertos 135.	Anexo 3 Evidencia 10
		192.198.1.172, Windows 8 Profesional, puertos abiertos 88, 443.	Anexo 3 Evidencia 13

Fuente: El presente documento

Tabla 9. Pruebas y resultados (Continuación)

Etapa	Proceso	Resultados	Evidencias
		192.198.1.164, Windows 7 Profesional, puertos abiertos 113, 135, 139, 445, 3389, 49154, 49155.	Anexo 3 Evidencia 11
		192.198.1.165, Windows 7 Profesional, puertos abiertos ninguno.	Anexo 3 Evidencia 11
		192.198.1.166, Windows 8 Profesional, puertos abiertos 113, 135, 139, 445, 3389, 49154, 49155, 49156.	Anexo 3 Evidencia 11
		192.198.1.169, Windows 7 Profesional, puertos abiertos 22, 80, 10001.	Anexo 3 Evidencia 12
Identificación del objetivo.	Con base en los servicios ofrecido y al sistema operativo.	Servidor: 192.168.1.150	Anexo 2 Evidencia 2
Identificación de vulnerabilidades de red.	Se realizan las pruebas definidas en la aplicación OpenVas en el servidor objetivo: • 192.168.1.150	192.168.1.150 se encontraron 9 vulnerabilidades (1 alta y 8 medias).	Anexo 2 Evidencia 6 Evidencia 7
Identificación de vulnerabilid	Se ejecutó la aplicación OpenVas	192.168.1.150 se encontraron 100 vulnerabilidades (35 alta, 27	Anexo 2

ades de Windows.	en el servidor objetivo: 192.168.1.150	medias y 38 bajas), calificadas entre 1,9 a 10, se tomará para el estudio aquellas con nota superior a 7.5. 192.168.1.150, se encontraron 5 exposiciones comunes	Evidencia 3 Evidencia 4 Evidencia 5

Fuente: El presente documento

5. APLICACIÓN DEL ESTÁNDAR ISO 27002 PARA LA CLASIFICACIÓN DE RIESGOS IDENTIFICADOS EN LOS TEST DE PENETRACIÓN

5.1. DESCRIPCIÓN DE LA METODOLOGÍA APLICADA

Como fundamento y para llevar a cabo una adecuada estructuración del proceso investigativo, se empleó lo expuesto en el estándar ISO IEC 27002, el cual y como se puede identificar en el aparte 2.3.9 cuenta con un conjunto de controles los cuales evalúan de forma significativa la seguridad de la información desde la perspectiva de los riesgos asociados, dicha conceptualización se orienta y enfatiza para esta investigación en analizar las vulnerabilidades del Sistema de Información de Gestión Empresarial de la empresa Jardines Cristo Rey Ltda. Cabe anotar que en este proyecto se aplica el dominio enunciado en el numeral 2.3.10 con el que se verifica la seguridad del sistema estudiado y para la realización del análisis de riesgos se selecciona los objetivos de control al igual que los controles a ser evaluados. Por su parte y para identificar el grado de cumplimiento, se toma como criterio que aquellos ítems con un cumplimiento menor al 50% son considerados como riesgos de vulnerabilidad latentes y aquellos por encima del 50% son considerados como riesgos de manejo adecuado, dedo que no manifiestan la existencia de vulnerabilidades significativas.

5.2. EVALUACIÓN DE LA SEGURIDAD EN EL SISTEMA DE INFORMACIÓN DE GESTIÓN EMPRESARIAL

Como se mencionó anteriormente, para la realización de la evaluación de la seguridad en el Sistema de Información de Gestión empresarial se toma el dominio explicado en el numeral 2.3.10 del presente documento, para la posterior aplicación de listas de chequeo estandarizadas para el dominio y los objetivos seleccionados que permiten evalúan las vulnerabilidades.

A continuación se presenta el estándar de medición del control para cada uno de los controles inspeccionados.

Tabla 10. Valoración de los controles

ALTO LEVE	SIN RIESGO
ALTO MODERADO	RIESGO MUY BAJO
ALTO CRÍTICO	RIESGO BAJO
MEDIO LEVE	RIESGO MEDIO BAJO
MEDIO MODERADO	RIESGO MEDIO
MEDIO CRÍTICO	RIESGO MEDIO ALTO
BAJO LEVE	RIESGO ALTO BAJO
BAJO MODERADO	RIESGO ALTO MEDIO
BAJO CRÍTICO	RIESGO MUY ALTO

Fuente: El presente documento

En la

Tabla *8* se definen los tipos de vulnerabilidades encontradas y se clasifican con el porcentaje de cumplimiento del control en la empresa que se define de la siguiente manera:

- ALTO cumplimiento entre el 100% y el 70%
- MEDIO cumplimiento entre el 69% y 50%
- BAJO cumplimiento de menos del 50% para este caso se consideran vulnerabilidades de ALTO RIESGO ya que el incumplimiento del control da camino para una potencial vulnerabilidad.

Además para verificar el cumplimiento de los controles se emplearán listas de chequeo estandarizadas, las cuales se proyectan y definen para cada dominio. Para la valoración del riesgo se identifican las siguientes tablas de convenciones para la valoración de amenazas.

Tabla 11. Tabla de nivel de cumplimiento

Valor	Descripción	Significado
MA	muy alta	El control se cumple en su totalidad
A	alta	El control se cumple con fallas
M	media	El control no se cumple completamente
B	baja	El control no se cumple
MB	muy baja	No existen medidas de control

Fuente: El presente documento

Tabla 12. Tabla de impacto por no cumplimiento

Valor	Descripción	Significado
MA	muy alta	El impacto por incumplimiento es alto y el daño es muy grabe
A	alta	El impacto por incumplimiento es alto y el daño no es muy grabe
M	media	El impacto por incumplimiento se considera leve pero importante
B	baja	El impacto por incumplimiento se considera leve
MB	muy baja	El impacto por incumplimiento se puede descartar

Fuente: El presente documento

La relación de estas variables mide el porcentaje de cumplimiento del control el cual se totaliza y al final de la lista de chequeo, el que se acumula para determinar el cumplimiento del dominio. Los resultados presentados en las listas de chequeo son se obtienen previa aplicación de las mismas dentro de la compañía y los valores incluidos son el resultado del proceso de verificación.

Tabla 13. Lista de chequeo, Requisitos de negocio para el control de acceso

Dominio	11. Control de acceso											
Lista de chequeo	Requisitos de negocio para el control de acceso											
A evaluar	Políticas de control de acceso											
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R1	¿Las políticas de control de acceso son desarrolladas y revisadas basadas en los requerimientos de seguridad del negocio?	1						1				100
R2	¿Los controles de acceso tanto físico como lógico son tenidos en cuenta en las políticas de control de acceso?			1					1			60
R3	¿Tanto a los usuarios como a los proveedores de servicios se les dio una clara declaración de los requisitos de la empresa en cuanto a control de acceso?		1						1			80
% Cumplimiento de la característica		80										
% Cumplimiento del objetivo		80										

Fuente: El presente documento

Tabla 14. Lista de chequeo, Gestión del acceso a los usuarios

Dominio	11. Control de acceso
Lista de chequeo	Gestión del acceso a los usuarios
A evaluar	Registro de usuarios

Riesgo	Descripción	Cumplimiento					Impacto por falla					% Cum
		MA	A	M	B	MB	MA	A	M	B	MB	
R4	¿Existen procedimientos para el registro y cancelación de usuarios para el acceso a todos los sistemas y servicios de la información?			1				1				60
% Cumplimiento de la característica		60										
A evaluar	Gestión de contraseñas para usuarios											
Riesgo	Descripción	Cumplimiento					Impacto por falla					% Cum
		MA	A	M	B	MB	MA	A	M	B	MB	
R5	¿Se restringe y controla la asignación y el uso de privilegios a los usuarios?	1						1				100
R6	¿Se identifica usuarios y sus privilegios de acceso, sistema operativo, sistema de gestión de bases de datos y aplicaciones?	1						1				100
% Cumplimiento de la característica		100										
A evaluar	Gestión de privilegios											
Riesgo	Descripción	Cumplimiento					Impacto por falla					% Cum
		MA	A	M	B	MB	MA	A	M	B	MB	
R7	¿Existe un procedimiento para la asignación de contraseñas a usuarios?				1		1					40

% Cumplimiento de la característica	40
% Cumplimiento del objetivo	67

Fuente: El presente documento

Tabla 15. Lista de chequeo Responsabilidad de los usuarios

Dominio	11. Control de acceso											
Lista de chequeo	Responsabilidad de los usuarios											
A evaluar	Uso de contraseñas											
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R8	¿Se exige a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas?			1				1				60
% Cumplimiento de la característica		60										
A evaluar	Equipo de usuario desatendido											
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R9	¿Existen procedimientos de seguridad para proteger los equipos desatendidos, así como sobre las responsabilidades en la implementación de dicha protección?					1		1				20
% Cumplimiento de la característica		20										
% Cumplimiento del objetivo		40										

Fuente: El presente documento

Tabla 16. Lista de chequeo, Control de acceso a las redes

Dominio	11. Control de acceso										
Lista de chequeo	Control de acceso a las redes										
A evaluar	Autenticación de usuarios para conexiones externas										
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R10	¿Son utilizados mecanismos apropiados de autenticación para controlar el acceso remoto de los usuarios?				1			1				40
% Cumplimiento de la característica		40										
A evaluar	identificación de los equipos en las redes										
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R11	¿La identificación automática es considerada para autenticar conexiones desde equipos y direcciones específicas?		1					1				80
% Cumplimiento de la característica		80										
A evaluar	Protección de los puertos de configuración y diagnostico remoto										
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R12	¿Los accesos físicos y lógicos a puertos de diagnóstico están apropiadamente controlados y protegidos por				1			1				40

	mecanismos de seguridad?												
% Cumplimiento de la característica		40											
A evaluar	Separación de la red												
		Cumplimiento					Impacto por falla						
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB		% Cum
R13	¿Los grupos de servicios de información, usuarios y sistemas de información son segregados en la red?		1						1				80
R14	¿La red (desde donde asociados de negocios o terceros necesitan acceder a los sistemas de información) es segregada utilizando mecanismos de seguridad perimetral como firewalls?		1						1				80

Fuente: El presente documento

Tabla 17. Lista de chequeo, Control de acceso a las redes (Continuación)

R15	¿En la segregación de la red son hechas las consideraciones para separar las redes Wireless en internas y privadas?			1					1				60
% Cumplimiento de la característica		73											
A evaluar	Control de Conexiones a las Redes												
Riesgo	Descripción	Cumplimiento					Impacto por falla						% Cum

		MA	A	M	B	MB	MA	A	M	B	MB	
R16	¿Existe una política de control de acceso que verifique conexiones provenientes de redes compartidas, especialmente aquellas que se extienden más allá de los límites de la organización?				1			1				40
% Cumplimiento de la característica		40										
A evaluar	Control del enrutamiento de la red											
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R17	¿Existen políticas de control de acceso que establezcan los controles que deben ser realizados a los ruteos implementados en la red?		1					1				80
R18	¿Los controles de ruteo, están basados en mecanismos de identificación positiva de origen y destino?			1					1			60
% Cumplimiento de la característica		70										
% Cumplimiento del objetivo		57										

Fuente: El presente documento

Tabla 18. Lista de cheque, Control de acceso al sistema operativo

Dominio	11. Control de acceso											
Lista de chequeo	Control de acceso al sistema operativo											
A evaluar	Procedimientos de registro de inicio seguro											
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R19	¿Existe controles para el acceso a los sistemas operativos mediante un procedimiento de registro de inicio seguro?		1						1			80
% Cumplimiento de la característica		80										
A evaluar	Identificación y autenticación de usuarios											
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R20	¿Existe una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario de inicio seguro?			1					1			60
R21	¿Los usuarios poseen un identificador único (ID del usuario) únicamente para su uso personal?	1							1			100
% Cumplimiento de la característica		80										
A evaluar	Sistema de gestión de contraseñas											
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum

R22	¿Los sistemas para la gestión de contraseñas son interactivos y aseguran la calidad de dichas contraseñas?				1			1					40
% Cumplimiento de la característica		40											
A evaluar	Uso de las utilidades del sistema												
		Cumplimiento					Impacto por falla						
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB		% Cum
R23	¿Se restringe y controla el uso de programas utilitarios que pueden perjudicar los controles del sistema y de la aplicación?				1			1					40
% Cumplimiento de la característica		40											
% Cumplimiento del objetivo		60											

Fuente: El presente documento

Tabla 19. Lista de chequeo, Control de acceso a las aplicaciones y a la información

Dominio	11. Control de acceso												
Lista de chequeo	Control de acceso a las aplicaciones y a la información												
A evaluar	Aislamiento de sistemas sensibles												
		Cumplimiento					Impacto por falla						
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB		% Cum
R24	¿Existe un entorno informático dedicado (aislados) para los sistemas sensibles?					1		1					20
% Cumplimiento de la característica		20											
% Cumplimiento del objetivo		20											

Fuente: El presente documento

Tabla 20. Lista de chequeo Computación móvil y trabajo remoto

Dominio	11. Control de acceso											
Lista de chequeo	Computación móvil y trabajo remoto											
A evaluar	Trabajo remoto											
		Cumplimiento					Impacto por falla					
Riesgo	Descripción	MA	A	M	B	MB	MA	A	M	B	MB	% Cum
R25	¿Existen implementados procedimientos para las actividades de trabajo remoto?					1		1				20
% Cumplimiento de la característica		20										
% Cumplimiento del objetivo		20										

Fuente: El presente documento

A continuación, se presenta la evaluación del dominio en estudio (Control de accesos) para ello se toma el porcentaje de cumplimiento de cada una de sus características (C) y en qué porcentaje se está cumpliendo en la empresa, con ello se identifican tanto los riesgos como las vulnerabilidades potenciales para la seguridad en el Sistema de Información de Gestión Empresarial en los objetivos de control (OC); como fundamento se toma los porcentajes de cumplimiento determinados para evaluar los riesgos, los cuales se obtienen del análisis de los resultados obtenidos en las listas de chequeo presentadas con anterioridad.

Tabla 21. Dominio control de acceso Porcentaje de cumplimiento por objetivo de control

Dominio	Control de acceso	
Tipo	Objetivo a evaluar	% cumplimiento
OC	Requisitos de negocio para el control de acceso	80
C	Políticas de control de acceso	80
OC	Gestión del acceso a los usuarios	60
C	Registro de usuarios	60
C	Gestión de contraseñas para usuarios	100
C	Gestión de privilegios	40
OC	Responsabilidad de los usuarios	40
C	Uso de contraseñas	60
C	Equipo de usuario desatendido	20
OC	Control de acceso a las redes	57
C	Autenticación de usuarios para conexiones externas	40
C	identificación de los equipos en las redes	80
C	Protección de los puertos de configuración y diagnostico remoto	40
C	Separación de la red	73
C	Control de Conexiones a las Redes	40
C	Control del enrutamiento de la red	70
OC	Control de acceso al sistema operativo	60
C	Procedimientos de registro de inicio seguro	80
C	Identificación y autenticación de usuarios	80
C	Sistema de gestión de contraseñas	40
C	Uso de las utilidades del sistema	40
OC	Control de acceso a las aplicaciones y a la información	20
C	Aislamiento de sistemas sensibles	20
OC	Computación móvil y trabajo remoto	20
C	Trabajo remoto	20

Fuente: El presente documento

- **Nivel del Riesgo**

De igual manera y no menos importante es la determinación del nivel del riesgo que se obtiene a partir del porcentaje de cumplimiento del control, dentro del objetivo de control, a continuación se presenta la clasificación del riesgo con base en el nivel

de obtenido como resultado de la aplicación de la lista de chequeo lo que se interpreta como una falla de seguridad en el manejo de la información de la compañía, dando lugar a la revisión de alguna vulnerabilidad potencial en el Sistema de Información de Gestión Empresarial de la compañía, a continuación se presenta el nivel del riesgo obtenido en cada uno de los controles estudiados, lo que se verá reflejado posteriormente en la conformación de la matriz de riesgo que proporciona información de los controles vulnerables:

Tabla 22. Clasificación de riesgos

Riesgo	Descripción	Nivel de riesgo
R1	Las políticas de control de acceso son desarrolladas y revisadas basadas en los requerimientos de seguridad del negocio	Riesgo muy Bajo
R2	Los controles de acceso tanto físico como lógico no siempre son tenidos en cuenta en las políticas de control de acceso	Riesgo Medio
R3	Tanto a los usuarios como a los proveedores de servicios se les dio una clara declaración de los requisitos de la empresa en cuanto a control de acceso	Riesgo muy Bajo
R4	Existen procedimientos para el registro y cancelación de usuarios, pero no se hace uso de el para el acceso a todos los sistemas y servicios de la información	Riesgo Medio
R5	Se restringe y controla la asignación y el uso de privilegios a los usuarios	Riesgo muy Bajo
R6	Se identifica usuarios y sus privilegios de acceso, sistema operativo, sistema de gestión de bases de datos y aplicaciones	Riesgo muy Bajo
R7	No existe un procedimiento para la asignación de contraseñas a usuarios	Riesgo alto
R8	No siempre se exige a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas	Riesgo Medio
R9	No existen procedimientos de seguridad para proteger los equipos desatendidos, así como sobre las responsabilidades en la implementación de dicha protección	Riesgo alto

R10	No son utilizados mecanismos apropiados de autenticación para controlar el acceso remoto de los usuarios	Riesgo alto

Fuente: El presente documento

Tabla 23. Clasificación de riesgos (Continuación)

Riesgo	Descripción	Nivel de riesgo
R11	La identificación automática es considerada para autenticar conexiones desde equipos y direcciones específicas	Riesgo Bajo
R12	Los accesos físicos y lógicos a puertos de diagnóstico no están apropiadamente controlados y protegidos por mecanismos de seguridad	Riesgo alto
R13	Los grupos de servicios de información, usuarios y sistemas de información son segregados en la red	Riesgo Bajo
R14	La red (desde donde asociados de negocios o terceros necesitan acceder a los sistemas de información) es segregada utilizando mecanismos de seguridad perimetral como firewalls	Riesgo Bajo
R15	En la segregación de la red son hechas las consideraciones para separar las redes Wireless en internas y privadas	Riesgo Medio
R16	No existe una política de control de acceso que verifique conexiones provenientes de redes compartidas, especialmente aquellas que se extienden más allá de los límites de la organización	Riesgo alto
R17	Existen políticas de control de acceso que establezcan los controles que deben ser realizados a los ruteos implementados en la red	Riesgo Bajo
R18	Los controles de ruteo, están basados en mecanismos de identificación positiva de origen y destino	Riesgo Medio

R19	Existe controles para el acceso a los sistemas operativos mediante un procedimiento de registro de inicio seguro	Riesgo Bajo
R20	Existe una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario de inicio seguro	Riesgo Medio

Fuente: El presente documento

Tabla 24. Clasificación de riesgos (Continuación)

Riesgo	**Descripción**	**Nivel de riesgo**
R21	Los usuarios poseen un identificador único (ID del usuario) únicamente para su uso personal	Riesgo muy Bajo
R22	Los sistemas para la gestión de contraseñas no son interactivos y no aseguran la calidad de dichas contraseñas	Riesgo alto
R23	No se restringe y controla el uso de programas utilitarios que pueden perjudicar los controles del sistema y de la aplicación	Riesgo alto
R24	No existe un entorno informático dedicado (aislados) para los sistemas sensibles.	Riesgo alto
R25	No existen implementados procedimientos para las actividades de trabajo remoto	Riesgo alto

Fuente: El presente documento

- **Clasificación de los riesgos detectados**

Con la clasificación y valoración de los riesgos se procede a la determinación de la matriz de riesgo donde se observa el grado de riesgo al cual se ve expuesta las comunicaciones de la empresa, con base en el dominio relacionado con las comunicaciones como se ha aplicado en este estudio:

Tabla 25. Matriz de riesgos – Jardines Cristo Rey

MB				R9, R24, R25	
B				R10, R16, R22, R23	R7
M			R2, R12, R15, R18, R20	R4, R8	
A			R3, R13, R14, R19	R5, R6, R11, R17	
MA			R21	R1	
	MB	B	M	A	MA

Fuente: El presente documento

De acuerdo con los resultados obtenidos en la aplicación de las listas de chequeo, es posible comprobar el porcentaje de cumplimiento del control y al igual que su impacto de cumplimiento; en esta caso concreto, los controles que cumplen con un porcentaje igual o superior al 60% son demarcados con color verde, ya que su impacto, en caso de ocurrencia, no es muy elevado, esto puede interpretarse como una seguridad alta en la protección de las vulnerabilidades del Sistema de Información de Gestión Empresarial.

Por otra parte, son clasificados con color amarillo los riesgos cuyos controles cumplen medianamente los aspectos de seguridad, que conlleva su revisión y posterior mejoramiento, por último se encuentran los identificados con color rojo que muestran la existencia de riesgos latentes y que pueden generar vulnerabilidades peligrosas.

6. CONJETURAS FINALES DE LA EVALUACIÓN DE LA SEGURIDAD EN EL AL SISTEMA DE GESTIÓN EMPRESARIAL DE LA COMPAÑÍA JARDINES CRISTO REY LTDA.

Con las actividades y resultados obtenidos de las evaluaciones de seguridad presentados en los numerales 4.3 y 4.4 de la presente investigación se obtuvo la identificación los riesgos categorizados en la Tabla 25 Matriz de riesgo, dichos riesgos se deben analizar como fundamento para realizar la proposición de estrategias de seguridad, cabe anotar que para el caso se trataran únicamente aquellos riesgos que presenten un riesgo tácito sobre la información existente en la empresa, por lo que se trataran aquellos cuyo impacto sobre la información del sistema sea medio, alto o muy alto y que tengan a su vez un cumplimiento medio, bajo o muy bajo, ya que es en estos niveles donde el nivel de riesgo representa menos del 50% de cumplimiento del control de seguridad evaluado. Además, aquellos riesgos que no se encuentren dentro de la categoría anteriormente enunciada, es decir que se encuentren por encima del 50% de cumplimiento se realizaran recomendaciones encaminadas a la mejora del cumplimiento del control.

Se presenta a continuación la tabla que presenta el resumen general de los resultados obtenidos a partir de las evaluaciones realizadas a los objetivos de control de comunicaciones los cuales se basan en lo expuesto por el estándar ISO 27002.

Tabla 26. Resumen de Objetivos de control, riesgo detectado y evidencia relacionada

Dominio:	11. Control de acceso	
Objetivo de control	Gestión del acceso a los usuarios	
Riesgo	Descripción del fallo o vulnerabilidad detectada	Evidencia relacionada
R4	Se evidencia un manejo inadecuado en lo relacionado a la administración, creación y eliminación de cuentas de usuario	**Anexo 4** Evidencia 14
Objetivo de control	Responsabilidad de los usuarios	
Riesgo	**Descripción del fallo o vulnerabilidad detectada**	**Evidencia relacionada**
R8	Con relación a la asignación y uso de contraseñas se tiene como resultado	**Anexo 4**

	que los usuarios no tienen la posibilidad de cambiar de contraseña, no existen políticas sobre el uso de contraseñas seguras	Evidencia 15Evidencia 16
R9	Se evidencia que los procedimientos de seguridad para proteger los equipos desatendidos, así como las responsabilidades en la implementación de dicha protección no son muy adecuados.	**Anexo 4** Evidencia 17Evidencia 18

Fuente: El presente documento

Tabla 27. Resumen de Objetivos de control, riesgo detectado y evidencia relacionada (Continuación)

Dominio:	11. Control de acceso	
Objetivo de control	Control de acceso a las redes	
Riesgo	**Descripción del fallo o vulnerabilidad detectada**	**Evidencia relacionada**
R10	Se evidencia la utilización de software de acceso remoto en la totalidad de los equipos, no se ha definido una política precisa sobre su manejo.	**Anexo 4** Evidencia 17 Evidencia 18 Evidencia 19
R12	Los accesos físicos y lógicos a puertos de diagnóstico no están apropiadamente controlados y protegidos por mecanismos de seguridad.	**Anexo 3** Evidencia 8 Evidencia 9 Evidencia 10 Evidencia 11 Evidencia 12 Evidencia 13
R16	No existe una política de control de acceso que verifique conexiones provenientes de redes compartidas.	**Anexo 3** Evidencia 8 Evidencia 9 Evidencia 10 Evidencia 11 Evidencia 12 Evidencia 13
Objetivo de control	Control de acceso al sistema operativo	
Riesgo	**Descripción del fallo o vulnerabilidad detectada**	**Evidencia relacionada**

R22	Con relación a la asignación y uso de contraseñas se tiene como resultado que los usuarios no tienen la posibilidad de cambiar de contraseña, no existen políticas sobre el uso de contraseñas seguras	**Anexo 4** Evidencia 15 Evidencia 16
R23	Se evidencia la utilización de software de acceso remoto en la totalidad de los equipos, no se ha definido una política precisa sobre su manejo.	**Anexo 4** Evidencia 17 Evidencia 18 Evidencia 19
Objetivo de control	Uso de las utilidades del sistema	
Riesgo	**Descripción del fallo o vulnerabilidad detectada**	**Evidencia relacionada**
R24	No existe un entorno informático dedicado (aislados) para los sistemas sensibles.	**Anexo 4** Evidencia 20
Objetivo de control	Trabajo remoto	
Riesgo	**Descripción del fallo o vulnerabilidad detectada**	**Evidencia relacionada**
R25	Se evidencia la utilización de software de acceso remoto en la totalidad de los equipos, no se ha definido una política precisa sobre su manejo.	**Anexo 4** Evidencia 17 Evidencia 18 Evidencia 19

Fuente: El presente documento

7. ESTRATEGIAS DE MITIGACIÓN PARA VULNERABILIDADES DETECTADAS EN EL SISTEMA DE INFORMACIÓN DE GESTIÓN EMPRESARIAL DE LA COMPAÑÍA JARDINES CRISTO REY LTDA.

La cultura de la seguridad, debe ser entendida como una responsabilidad global dentro de una organización la cual permite garantizar el funcionamiento eficaz de los sistemas de gestión de seguridad, requiere por parte de todos los componentes de la compañía para la aportación de normas, procedimientos, responsabilidades, recursos, compromisos y demás acciones que conlleven buenas prácticas[45]. Además, la seguridad de la Información conlleva el asegurar que los recursos del Sistema de Información de la empresa se utilicen de la forma en la cual se ha decidido permitiendo el acceso de información de manera contenida, así como que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización[46].

Como resultado de los procesos y en la búsqueda de un compromiso por parte del personal de la compañía Jardines Cristo Rey Ltda., se presentan las siguientes estrategias de mitigación que requieren a su vez de un proceso de difusión, consolidación y cumplimiento permanente.

[45] UNIVERSIDAD VERACRUZANA. Seguridad de la información. [en línea] 2015. [Consultado: 21 de junio de 2018]. Disponible en internet: https://www.tuv-sud.es/uploads/images/149546769692712254135 7/es-tuv-sud-process-safety-cultura-seguridad.pdf

[46] TUV SUD, Cultura de seguridad. [en línea] 2013. P. 2. [Consultado: 3 de julio de 2018]. Disponible en internet: www.uv.mx: https://www.uv.mx/celulaode/seguridad-info/tema1.html

Tabla 28. Estrategias de seguridad recomendadas

Dominio:	11. Control de acceso	
Objetivo de control	Gestión del acceso a los usuarios	
Riesgo	**Control a implementar**	**Estrategia de mitigación**
R4	El administrador del sistema debe aplicar procedimientos formales definidos para el registro y cancelación de usuarios	"Debería existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información. Guía de implementación El procedimiento de control del acceso para el registro y cancelación de usuarios debería incluir: a) uso de la identificación única de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso de identificadores (ID) de grupo únicamente se debería permitir cuando son necesarios por razones operativas o del negocio, y deberían estar aprobados y documentados; b) verificación de que el usuario tenga autorización del dueño del sistema para el uso del sistema o servicio de información, también pueden ser conveniente que la dirección apruebe por separado los derechos de acceso; c) verificación de que el nivel de acceso otorgado sea adecuado para los propósitos del negocio y sea consistente con la política de seguridad de la organización, es decir, no pone en peligro la distribución de funciones d) dar a los usuarios una declaración escrita de sus derechos de acceso; e) exigir a los usuarios firmar declaraciones que indiquen que ellos

		entienden las condiciones del acceso; f) mantenimiento de un registro formal de todas las personas registradas para usar el servicio; g) retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización; h) verificar, retirar o bloquear periódicamente las identificaciones (ID) y cuentas redundantes de usuarios ; i) garantizar que las identificaciones (ID) de usuario redundantes no se otorgan a otros usuarios."[47]

Fuente: El presente documento

Tabla 29. Estrategias de seguridad recomendadas (Continuación)

Dominio:	11. Control de acceso	
Objetivo de control	Responsabilidad de los usuarios	
Riesgo	**Control a implementar**	**Estrategia de mitigación**
R8	Se deben definir políticas de gestión y empleo adecuado de contraseñas seguras.	"La asignación de contraseñas se debería controlar a través de un proceso formal de gestión. Guía de implementación El proceso debería incluir los siguientes requisitos: a) se debería exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste; esta declaración firmada se podría incluir en los términos y condiciones laborales; b) cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura que estén forzados a cambiar

[47] QUINTERO, Edith. ISO 27002. [en línea]. Control de Acceso. 04 de junio de 2015. [Consultado 23 de junio de 2018]. Disponible en internet: http://isoedith18.blogspot.com/2015/06/11-control-del-acceso.html

		inmediatamente; c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva; d) las contraseñas temporales se deberían suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección; e) las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables; f) los usuarios deberían confirmar la entrega de las contraseñas; g) las contraseñas nunca se deberían almacenar en sistemas de computador en un formato no protegido; h) las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software."[48]
R9	Es responsabilidad de los usuarios el asegurar cualquier equipo desatendido mediante la protección apropiada.	"Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de seguridad para proteger los equipos desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre: a) terminar las sesiones activas cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña; b) realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión (es decir, no solo apagar el interruptor de la pantalla del computador o terminal); c) cuando no están en uso, asegurar los computadores personales o los terminales contra el uso no autorizado mediante una clave de bloqueo o un control equivalente como, por ejemplo, el acceso por contraseña." [49]

Fuente: El presente documento

Tabla 30. Estrategias de seguridad recomendadas (Continuación)

Dominio:	11. Control de acceso
Objetivo de control	Control de acceso a las redes

[48] QUINTERO, Óp. Cít. p. 75
[49] QUINTERO, Óp. Cít. p. 75

Riesgo	Control a implementar	Estrategia de mitigación
R10	El acceso para usuarios remotos se debe realizar mediante métodos apropiados de autenticación.	"Los procedimientos y controles de devolución de marcación, por ejemplo, empleando módems de retorno de marcación, pueden suministrar protección contra conexiones no deseadas o no autorizadas a los servicios de procesamiento de información de la organización. Este tipo de control autentica a los usuarios tratando de establecer una conexión con una red de la organización desde sitios remotos." [50]
R12	Se debe controlar el acceso lógico y físico a los puertos de diagnóstico y configuración.	"Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o de red, que no se requieren específicamente para la funcionalidad del negocio, se deberían inhabilitar o retirar. Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnóstico y configuración solo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/software que requiere el acceso."[51]

[50] QUINTERO, Óp. Cít. p. 75
[51] QUINTERO, Óp. Cít. p. 75

R16	En caso de existir redes compartidas, es decir aquellas que se extienden más allá de las fronteras de la organización, se requiere definir restricciones sobre la capacidad de los usuarios para conectarse a la red, para ello se deben definir y aplicar políticas de control de acceso en los que se especifiquen los requisitos de aplicación del negocio establecidos.	"Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según se requiera a través de la política de control de acceso de la organización. La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace (Gateway) de red que filtren el tráfico por medio de tablas o reglas predefinidas. Los siguientes son algunos ejemplos de aplicaciones a las cuales se deberían aplicar restricciones: 1) mensajería. Por ejemplo, el correo electrónico 2) transferencia de archivos 3) acceso interactivo 4) acceso a las aplicaciones Es conveniente tomar en consideración el enlace de los derechos de acceso a la red con algunas horas del día o fechas. Información adicional. La política de control del acceso puede exigir la incorporación de controles para restringir la capacidad de conexión de los usuarios a redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización." [52]

Fuente: La presente investigación

Tabla 31. Estrategias de seguridad recomendadas (Continuación)

Dominio:	11. Control de acceso	
Objetivo de control	Control de acceso al sistema operativo	
Riesgo	**Control a implementar**	**Estrategia de mitigación**
R22	Se deben definir políticas de gestión y empleo	"La asignación de contraseñas se debería controlar a través de un proceso formal de gestión. Guía de implementación El proceso debería incluir los siguientes requisitos: a) se debería exigir a los usuarios la firma de una

[52] QUINTERO, Óp. Cít. p. 75

	adecuado de contraseñas seguras.	declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste; esta declaración firmada se podría incluir en los términos y condiciones laborales; b) cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura que estén forzados a cambiar inmediatamente; c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva; d) las contraseñas temporales se deberían suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección; e) las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables; f) los usuarios deberían confirmar la entrega de las contraseñas; g) las contraseñas nunca se deberían almacenar en sistemas de computador en un formato no protegido; h) las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software."[53]
R23	Se debe definir políticas para evitar el acceso no autorizado a los sistemas operativos, se recomienda restringir el acceso a usuarios no autorizados o emplear políticas de identificación o control de acceso.	"El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro. Guía de implementación El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos: a) No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente; b) mostrar una advertencia de notificación general indicando que sólo deberían tener acceso al computador los usuarios autorizados; c) no suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado;

[53] QUINTERO, Óp. Cít. p. 75

		d) validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta; e) limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos, y considerar: 1) registrar intentos exitosos y fallidos 2) forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización específica; 3) desconectar las conexiones de enlaces de datos; 4) enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio; 5) establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege; f) limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación; g) mostrar la siguiente información al terminar un registro de inicio exitoso: 1) fecha y hora del registro de inicio exitoso previo; 2) detalles de los intentos fallidos de registro de inicio desde el último registro exitoso; h) no mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos; i) no transmitir contraseñas en texto claro en la red. Información adicional Si las contraseñas se transmiten en texto claro durante la sesión de registro de inicio pueden ser capturadas en la red por un programa "husmeador" de red.”[54]

Fuente: La presente investigación

[54] QUINTERO, Óp. Cít. p. 75

Tabla 32. Estrategias de seguridad recomendadas (Continuación)

Dominio:	11. Control de acceso	
Objetivo de control	Uso de las utilidades del sistema	
Riesgo	**Control a implementar**	**Estrategia de mitigación**
R24	Aquellos sistemas considerados como sensibles deben ser provistos de un entorno informático dedicado (aislados).	"Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles: a) la sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del dueño de la aplicación b) cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el dueño de la aplicación sensible. Los sistemas de aplicación son lo suficientemente sensibles a la pérdida potencial que requieren manejo especial. La sensibilidad puede indicarle el sistema de aplicación se debería: a) ejecutarse en un computador dedicado, o b) únicamente debería compartir recursos con sistemas de aplicaciones confiables. El aislamiento se puede lograr utilizando métodos físicos o lógicos"[55]
Objetivo de control	Trabajo remoto	
Riesgo	**Control a implementar**	**Estrategia de mitigación**
R25	Para el desarrollo de actividades propias de trabajo remoto, es necesario desarrollar e implementar políticas,	"Las organizaciones sólo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de seguridad de la organización. Se recomienda considerar los siguientes

[55] QUINTERO, Óp. Cít. p. 75

	planes operativos y procedimientos.	aspectos: a) la seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local; b) el entorno físico de trabajo remoto propuesto; c) los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el enlace de comunicación y la sensibilidad del sistema interno; d) la amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio, por ejemplo familiares y amigos; e) el uso de redes domésticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica; f) las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada; g) el acceso a equipo de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), el cual puede estar prohibido por la ley; h) los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes; i) protección antivirus y requisitos de barreras contra fuego (firewall). Las directrices y disposiciones a considerar deberían incluir las siguientes: a) disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que

		no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización; b) definición del trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado; c) disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto; d) seguridad física; e) reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información; f) disposición de soporte y mantenimiento de hardware y software; g) disposición de pólizas de seguros; h) procedimientos para el respaldo y la continuidad del negocio; i) auditoría y monitoreo de seguridad; j) revocación de autoridad y derechos de acceso, y la devolución del equipo al finalizar las actividades de trabajo remoto.”[56]

Fuente: El presente documento

[56] QUINTERO, Óp. Cít. p. 75

CONCLUSIONES

La realización del presente estudio requirió la identificación y selección de pruebas de testeo que se aplicaron en la red de datos que soporta los procesos de manejo de información del sistema de información de gestión empresarial de la compañía Jardines Cristo Rey Ltda., para lo cual se identifica y selecciona el framework denominado Open Vas, que posee un conjunto de pruebas de penetración a implementarse y que a su vez permite la identificación de vulnerabilidades existentes tanto en el sistema operativo como en la interconexión de los elementos existentes en la red.

El uso de Open Vas para la realización de las pruebas de penetración permite la identificación de vulnerabilidades las que deben ser atendidas para la mitigación de riesgos, entre las que se encuentra el manejo adecuado de usuarios, la asignación correcta de permisos y el manejo adecuado de estaciones desatendidas; sin embargo, estas condiciones requieren ser atendidas mediante el fortalecimiento de un esquema de seguridad sobre este segmento de red, debido y como se ha evidenciado, actualmente no se encuentra implementado. Entre las características de la solución se ha tenido en cuenta el control y administración adecuado de puertos de los dispositivos de comunicación y las debilidades propias del sistema operativo, entre otras como se demuestra para el manejo de estos aspectos.

Como se ha mencionado durante la investigación, el sistema de información de gestión empresarial de la compañía Jardines Cristo Rey Ltda., presenta vulnerabilidades, evidenciadas de manera óptima con el uso de Open Vas la cual ha dado como resultado el escaneo de puertos, la infraestructura de la red y las deficiencias presentadas en la misma.

Por otra parte, mediante el empleo de prácticas de hackeo ético se evalúa la seguridad existente dentro del sistema de información de gestión empresarial, los protocolos y aplicaciones empleadas por la compañía Jardines Cristo Rey Ltda., lo que permite corroborar las vulnerabilidades detectadas y reportar a la empresa información necesaria para la toma de medidas dirigidas hacia la mejora de la integridad de la seguridad de la red de datos de la empresa.

Además, haciendo uso de la norma ISO 27002 en su dominio 11, Control de Acceso acompañado de la metodología de listas de chequeo se realiza la evaluación e

identificación de riesgos, lo que da como resultado la matriz de riesgos el nivel de afectación que estos tienen sobre la información y la selección de estrategias a implementarse.

Con relación a la identificación e implementación de estrategias para la optimización de la seguridad del sistema de información de gestión empresarial de la compañía Jardines Cristo Rey Ltda. y los sistemas conexos, es requerido la identificación de vulnerabilidades, la posibilidad de ocurrencia y el impacto que estas puedan causar; una vez adquirida esta información es posible plantear estrategias de solución las cuales con un adecuado empoderamiento de la directivas y personal de la empresa brindará la aplicación correcta de los controles sugeridos en este documento, actividades que requieren sean desarrolladas de manera rutinaria y con el registro documental necesario para una evaluación constante, buscando lograr con esto la mitigación de los riesgos y vulnerabilidades que presentan un alto grado de ocurrencia.

RECOMENDACIONES

Para lograr alcanzar el aseguramiento del sistema de información de gestión empresarial de la compañía Jardines Cristo Rey Ltda. Y la aplicación adecuada de los planes propuestos en este documento se realiza las siguientes recomendaciones:

Con relación a los accesos no autorizados al sistema de información documental, la compañía Jardines Cristo Rey Ltda., debe definir y aplicar políticas que controlen esta vulnerabilidad.

Emplear técnicas anti intrusión para controlar la seguridad en la conexión entre la Intranet y otras redes públicas o privadas.

Realizar el registro documental de eventos y actividades llevadas que se consideren críticas llevadas a cabo por los usuarios en el sistema.

Aplicar políticas sobre la seguridad para el trabajo remoto y la computación móvil.

Definir y aplicar estrategias que impidan el acceso no autorizado al sistema de información de gestión empresarial de la compañía Jardines Cristo Rey Ltda.

Definir políticas con relación al uso seguro de contraseñas y equipos.

Realizar campañas de capacitación encaminadas a la concientización de los usuarios sobre su responsabilidad en la seguridad de la información al igual que capacitarlos sobre el uso de contraseñas seguros y equipos desatendidos.

Definir controles y asegurar físicamente los componentes hardware de red, principalmente el centro y la infraestructura de comunicaciones para garantizar la seguridad de los componentes y servicios, contra el acceso no autorizado.

Asegurar y mejorar la distribución lógica de la red de datos mediante el uso de equipos de enrutamiento capa 3 que permitan la realización adecuada de sub neteo, conexiones VPN y permisos a usuarios de red, al igual que definir y documentar los perímetros de seguridad, firewall, y gateways para filtrar el tráfico entre los dominios y evitar el acceso no autorizado.

Adquirir y configurar equipos que permitan limitar la capacidad de conexión de los usuarios al igual que establecer políticas dentro de dichos equipos para el cumplimiento de los objetivos propuestos.

Se recomienda al personal encargado de los procesos de administración y mantenimiento de equipos e infraestructura de red la aplicación y apropiación de las estrategias propuestas en el presente documento, con el fin de alcanzar mejores prácticas en seguridad al igual que controlar y minimizar los riesgos.

Con relación a la autorización de manejos personales de los clientes se recomienda registrar la aprobación mediante un formato pre impreso.

BIBLIOGRAFÍA

ACUNETIX. Mongoose Web Server Remote Buffer Overflow Vulnerability. [en línea]. 25 de 03 de 2015. [Consultado: 15 de septiembre de 2018]. Disponible en internet: https://www.acunetix.com/vulnerabilities/network/vulnerability/mongoose-web-server-remote-buf. (s.f.).

BEYOND SECURITY. Finding and Fixing Vulnerabilities in SSL Suites Weak Ciphers, a Medium Risk Vulnerability. [en línea]. 2018. [Consultado: 15 de octubre de 2018]Disponible en internet: https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_s. (s.f.).

COLOMBIA, R. D. ANEXO 2: Metodología De Gestión Del Riesgo - Modelo De Seguridad De La Información Para La Estrategia De Gobierno En Línea. [en línea]. 12 de 2010. P. 50. [Consultado: 28 de abril de 2018]. Disponible en internet: http://www.vive.gobiernoe. (s.f.).

COMSOLTI.MX. Infraestructura Hardware. [en línea] 2018. [Consultado: 4 de abril de 2018] Disponible en internet: http://comsolti.mx/infraestructura-hardware/. (s.f.).

CRIDLAC.ORG. Mitigación (Reducción O Atenuación) Del Riesgo. [en línea] 2008. P. 50. [Consultado: 28 de abril de 2018]. Disponible en internet: http://www.cridlac.org/VCD/files/page336.html. (s.f.).

CVE (COMMON VULNERABILITIES AND EXPOSURES) CVE-2018-0886. [en línea]. 01 de 12 de 2017. [Consultado: 4 de agosto de 2018]. Disponible en internet: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0886. (s.f.).

CVE (COMMON VULNERABILITIES AND EXPOSURES). CVE-2016-0800. [en línea]. 16 de 12 de 2015. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2016-0800. (s.f.).

CVE (COMMON VULNERABILITIES AND EXPOSURES). CVE-2016-0800. [en línea]. 16 de 12 de 2015. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2016-0800. (s.f.).

CVE (COMMON VULNERABILITIES AND EXPOSURES). CVE-2018-8174. [en línea]. 14 de 03 de 2018. [Consultado: 3 de agosto de 2018]. Disponible en internet: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174. (s.f.).

CVEDETAILS. Details. [en línea] 13 de 10 de 2017.[Consultado: 24 de julio de 2018]. Disponible en internet://www.cvedetails.com/cve/cve-2017-8717. (s.f.).

EVALUANDOSOFTWARE.COM. Estructura de un sistema de gestión empresarial [en línea] www.evaluandosoftware.com/. 2015. [en línea] [Consultado: 18 de

junio de 2019]. Disponible en internet: https://www.evaluandosoftware.com/. (s.f.).
EVALUANDOSOFTWARE.COM. Estructura de un sistema de gestión empresarial. [en línea] 31 de 03 de 2015. [Consultado: 3 de abril de 2018]. Disponible en internet: http://www.evaluandosoftware.com/estructura-sistema-gestion-empresarial/. (s.f.).
GUIA TIC SOLUCIONES. GESTIÓN COMERCIAL PLUS SysCafé Software Integrado de Gestión Empresarial. 2018. [Consultado: 30 de marzo de 2018]. Disponible en internet: http://www.guiadesolucionestic.com/sistemas-de-informacion/gestion-financiera/software-contable. (s.f.).
INCIBE-CERT.ES. Vulnerabilidad en el componente Microsoft Windows Search en productos Microsoft (CVE-2017-11771) [en línea]. 2017. [Consultado: 20 de julio de 2018]. Disponible en internet: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2. (s.f.).
INGENIA. Control de acceso a red (NAC). [en línea] 2018. [Consultado: 2 de mayo de 2018]. Disponible en internet: https://www.ingenia.es/es/servicio/control-de-acceso-red-nac. (s.f.).
ISO27000. Sistema de gestión de la seguridad de la información. [en línea]. ISO27000 2015. 14 p. [Consultado: 30 de marzo de 2018]. Disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf. (s.f.).
ISO27002. Control de Accesos. [en línea] 2012. [Consultado: 2 de mayo de 2018]. Disponible en internet: https://iso27002.wiki.zoho.com/11ControlAccesos.html. (s.f.).
JARDINES CRISTO REY. Servicios Exequiales Jardines Cristo Rey Ltda. [en línea] jardinescristorey.com/. 2017. [Consultado: 29 de marzo de 2018] Disponible en internet: http://www.jardinescristorey.com/. (s.f.).
JLIM, F. C. capacitateparaelempleo.org. Vulnerabilidades Informáticas [en línea] 2015. P. 2. [Consultado: 10 de abril de 2018]. Disponible en internet: https://capacitateparaelempleo.org/assets/4aq4l6q.pdf. (s.f.).
LASSO GARCÉS, L. A. Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa ingelec S.A.S. Pasto: UNAD. [en línea]. 2015. P. 92. [Consultado: 20 de abril de . (s.f.).
MICROSOFT. Soporte Tenico de Microsoft. Actualización de seguridad para la vulnerabilidad de ejecución remota de código de Windows Search: 8 de agosto de 2017. [en línea] 8 de 08 de 2017. [Consultado: 20 de julio de 2018]. Disponible en internet:btenido d. (s.f.).
MICROSOFT. Windows 7 system requirements. [en línea]. 2008. [Consultado: 1 de abril de 2018] Disponible en internet: https://support.microsoft.com/es-co/help/10737/windows-7-system-requirements. (s.f.).
MICROSOFT. Windows server 2008 requerimientos del sistema. [en línea]. 2008. [Consultado: 1 de abril de 2018]. Disponible en internet: https://msdn.microsoft.com/es-es/library/dn383626(v=ws.11).aspx. (s.f.).
MOLINA MIRANDA, María Fernanda. Propuesta De Un Plan De Gestión De Riesgos De Tecnología Aplicado En La Escuela Superior Politécnica Del

Litoral. [en línea] 2015. 89. P. [Consultado: 2 de mayo de 2018]. Disponible en internet: http://www.dit.upm.es/~posg. (s.f.).
NAJAR, Jose Custodio. Information Security: A Valuable Asset of the Organization. En: Vínculos Vol. 12 Núm. 1. 2015. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2011-2900 Detail. [en línea]. 08 de 05 de 2011. [Consultado: 10 de septiembre de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2011-2900. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2013-2566 Detail. [en línea]. 15 de 03 de 2013. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2013-2566. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2014-3566 Detail. [en línea]. 10 de 14 de 2014. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2014-3566. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2014-3566 Detail. [en línea]. 10 de 14 de 2014. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2014-3566. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2016-0170 Detail. [en línea]. 05 de 10 de 2016. [Consultado: 30 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2016-0170. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2016-2183 Detail. [en línea]. 31 de 08 de 2016. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2016-2183. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2016-2183 Detail. [en línea]. 31 de 08 de 2016. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2016-2183. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0023 Detail. [en línea]. 16 de 03 de 2017. [Consultado: 13 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0023. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0158 Detail. [en línea]. 14 de 04 de 2017. [Consultado: 13 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0158. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0166 Detail. [en línea]. 12 de 04 de 2017. [Consultado: 30 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0166. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0250 Detail. [en línea]. 08 de 08 de 2017. [Consultado: 30 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0250. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0293 Detail. [en línea]. 08 de 08 de 2017. [Consultado: 10 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0293. (s.f.).
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-11847 Detail. [en línea]. 14 de 11 de 2017. [Consultado: 30 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-11847. (s.f.).

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-8633 Detail. [en línea]. 08 de 08 de 2017. [Consultado: 2 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-8633. (s.f.).

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2018-0825 Detail. [en línea]. 14 de 02 de 2018. [Consultado: 10 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2018-0825. (s.f.).

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). Vulnerability Details: CVE-2017-8717.[en línea] 13 de 10 de 2017. [Consultado: 20 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-8718. (s.f.).

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. CVE-2018-0883 Detail. [en línea]. 14 de 03 de 2018. [Consultado 5 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2018-0883. (s.f.).

NOTICIASSEGURIDAD.COM. ¿Cómo hacer análisis de vulnerabilidades informáticas? [en línea] 2 de 3 de 2016. [Consultado: 20 de abril de 2018]. Disponible en internet: http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informatic. (s.f.).

OPENVAS.ORG. openvas.org. [en línea]. [Consultado: 25 de abril de 2018]. Disponible en internet: http://www.openvas.org/documentation.html. (s.f.).

PRESIDENCIA DE LA REPUBLICA. Decreto 1377 de 2013. [en línea] http://wsp.presidencia.gov.co. 2013. [Consultado: 19 de junio de 2019] Disponible en internet: http://http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20D. (s.f.).

QUINTERO, Edith. ISO 27002. [en línea]. Control de Acceso. 04 de junio de 2015. [Consultado 23 de junio de 2018]. Disponible en internet: http://isoedith18.blogspot.com/2015/06/11-control-del-acceso.html. (s.f.).

RAMOS RAMOS, Jorge. Luis. Pruebas De Penetración O Pent Test. [en línea] 06 de 2013. [Consultado: 22 de abril de 2018]. Disponible en internet: http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a14.pdf. (s.f.).

SECURITY SPACE. DCE/RPC and MSRPC Services Enumeration Reporting. [en línea] 2017. [Consultado: 15 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.10736. (s.f.).

SECURITY SPACE. SSL/TLS: Certificate Signed Using A Weak Signature Algorithm. [en línea]. 2016. [Consultado 25 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.105880. (s.f.).

SECURITY SPACE. SSL/TLS: Report Vulnerable Cipher Suites for HTTPS. [en línea]. 2016. [Consultado: 25 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108031. (s.f.).

SECURITY SPACE. SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE). [en línea]. 2014. [Consultado: 15 de

octubre de 2018] Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1. (s.f.).
SECURITY SPACE. The SSL/TLS service uses Diffie-Hellman groups with insufficient strength; (key size < 2048). [en línea]. 2016. [Consultado: 20 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.2. (s.f.).
SECURITYSPACE. SSL/TLS: Missing `secure` Cookie Attribute. [en línea]. 2012. [Consultado: 10 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.902661. (s.f.).
SENA. Análisis De Vulnerabilidad. Curso: Planes de Emergencia. [en línea] 2007. P. 18. [Consultado: 11 de abril de 2018]. Disponible en internet: https://sena.blackboard.com/bbcswebdav/courses/32330017_1_VIRTUAL/UNIDAD%202%20An%C3%A1lisis%20de%20vulnerabi. (s.f.).
SYSCAFE. Productos SysCafé. syscafe.com.co. 2018 [en línea]. Disponible en internet: https://www.syscafe.com.co/producto. (s.f.).
TUV SUD, Cultura de seguridad. [en línea] 2013. P. 2. [Consultado: 3 de julio de 2018]. Disponible en internet: www.uv.mx: https://www.uv.mx/celulaode/seguridad-info/tema1.html. (s.f.).
UDG.MX. Delincuentes informáticos ya no atacan empresas grandes, sino a usuarios de smartphone. [en línea] www.udg.mx. 2018. [Consultado: 29 de marzo de 2018] Disponible en internet: http://www.udg.mx/es/noticia/delincuentes-informaticos-ya-no-atacan-empr. (s.f.).
UNIVERSIDAD NACIONAL DE LA PATAGONIA “S.J. BOSCO”-FAC. DE INGENIERIA – DTO. INFORMATICA. Escaneo de puertos. [en línea] 2012. [Consultado: 23 de abril de 2018]. Disponible en internet: http://www.ing.unp.edu.ar/asignaturas/rytd/Anexos/RyTD_Anexo_TP6_Escan. (s.f.).
UNIVERSIDAD VERACRUZANA. Seguridad de la information. [en línea] 2015.[Consultado: 21 de junio de 2018]. Disponible en internet: https://www.tuv-sud.es/uploads/images/1495467696927122541357/es-tuv-sud-process-safety-cultura-seguridad.pdf. (s.f.).
WWW.CEUPE.COM. Analisis de viabilidad riesgo de proyecto. [en línea] www.ceupe.com. 2019. [Consultado: 19 de junio de 2019] Disponible en internet: https://www.ceupe.com/blog/analisis-de-viabilidad-riesgo-de-proyecto.html. (s.f.).
YÁGUEZK, J. R. Técnicas y herramientas de análisis de vulnerabilidades [en línea]. 18 de 11 de 2014. [Consultado: 28 de abril de 2018]. Disponible en internet: http://oa.upm.es/32786/1/TFG_javier_rios_yaguez.pdf. (s.f.).

ANEXOS

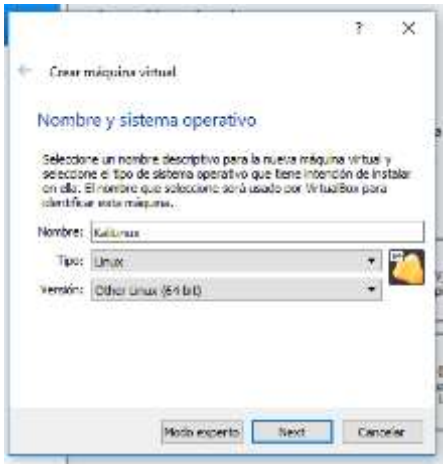
Anexo 1. Instalación y configuración OpenVas

Para el presente proyecto y durante la etapa metodológica se define la utilización de un servidor OpenVas para la Identificación de vulnerabilidades haciendo uso de este framework se ha efectuado el escaneo y administración de vulnerabilidades sobre el equipo principal de la compañía Jardines Cristo Rey Ltda., para el caso de estudio el servidor central.

Para su aplicación se requirió la instalación de un sistema operativo que fuera capaz de almacenar y administrar OpenVas por lo que se eligió e instalo la versión de Linux denominada, Kali Linux en una máquina virtual haciendo uso de Oracle VirtualBox, a continuación, se presentan evidencias de la instalación de la máquina virtual Kali Linux en el servidor de la compañía Jardines Cristo Rey Ltda.

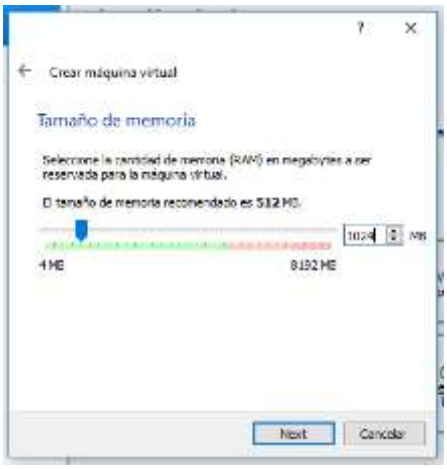
Se procede a configurar una maquina virtual en VirtualBox

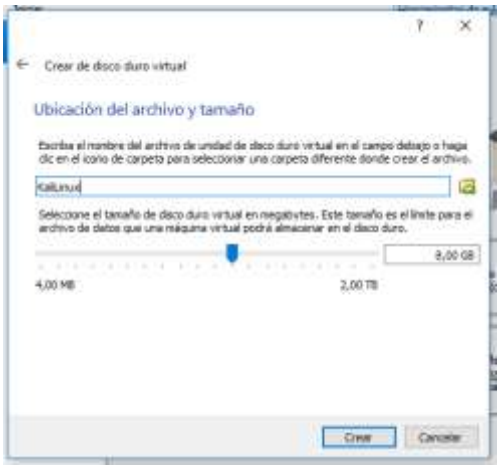
Captura de Pantalla 1. CP_01 Selección tipo de maquina virtual



Fuente: El presente documento

Captura de Pantalla 2. CP_02 Asignación de recursos a la máquina (memoria, disco duro).

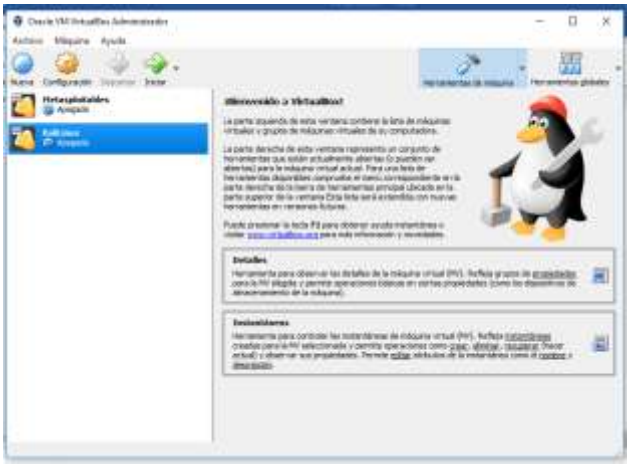




Fuente: El presente documento

Una vez creada se procede a insertar la imagen ISO de Kali Linux, en una unidad virtual y se procede a iniciar la instalación

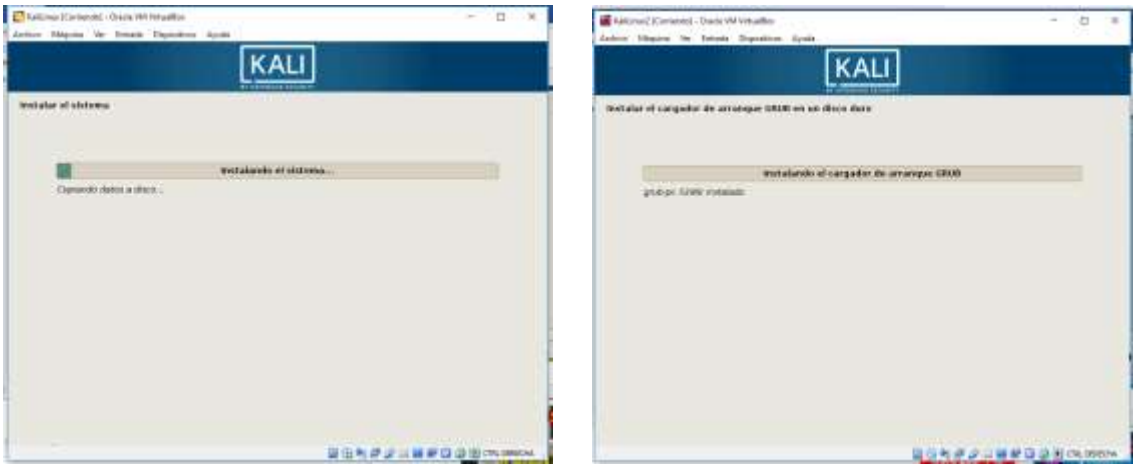
Captura de Pantalla 3. CP_03 Inicializacion de la maquina virtual y del proceso de Instalacion



Fuente: El presente documento

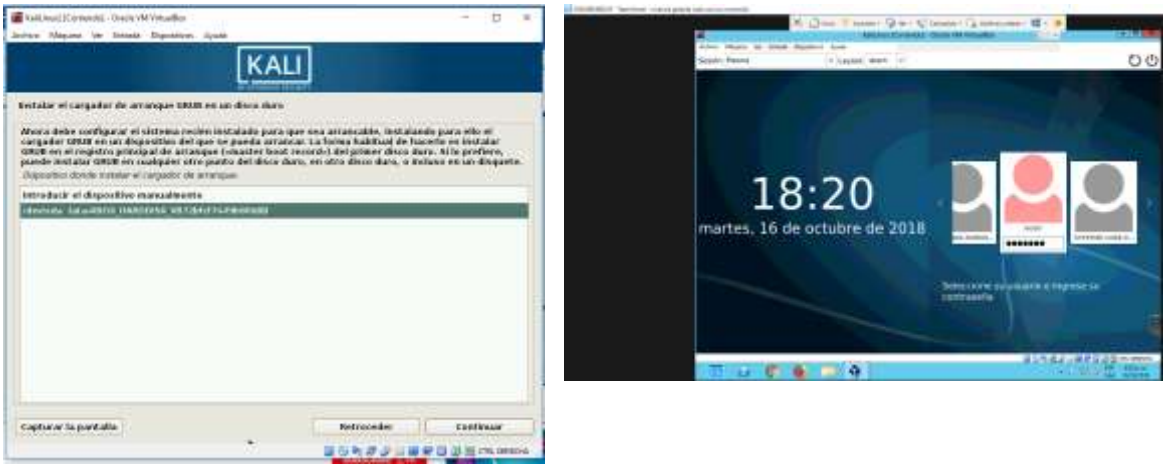
Se desarrolla el proceso de instalación dando como resultado:

Captura de Pantalla 4. CP_04 Proceso de instalacion y configuracion de paquetes



Fuente: El presente documento

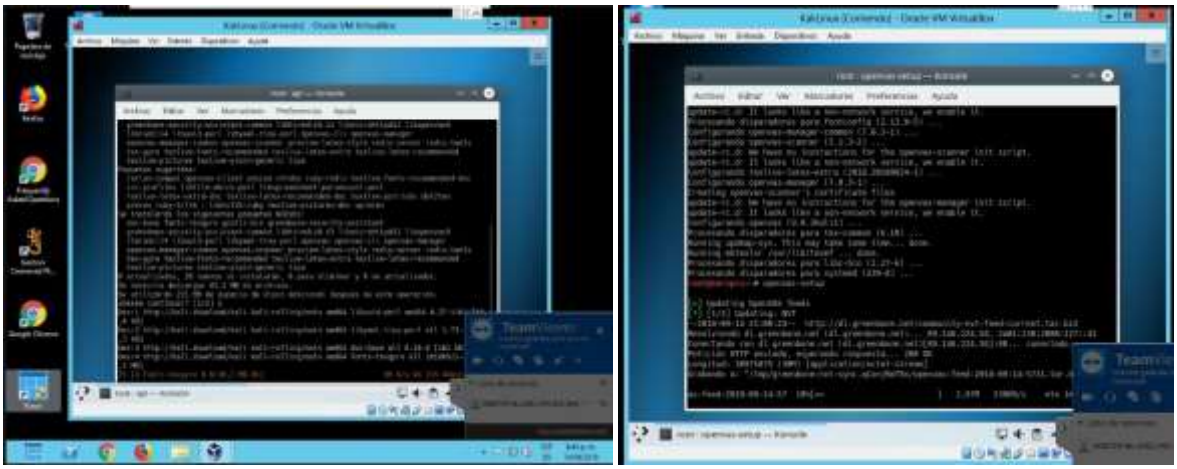
Captura de Pantalla 5. CP_05 Configuracion GRUB, inicio de la maquina virtual



Fuente: El presente documento

Una vez y con la maquina KaliLinux en funcionamiento se procede a instalar el aplicativo OpenVas.

Captura de Pantalla 6. CP_06 Instalacion y configuracion OpenVas



Fuente: El presente documento

Una vez instalado se procede a configurar y a poner en marcha el framework y se define la tarea o el equipo sobre el cual se va a realizar la identificación de vulnerabilidades que para el presente proyecto es el servidor de la compañía que se reconoce a través de la IP 192.168.1.150.

Para ello se emplea el navegador instalado por defecto en Kali Linux y se hace un llamado al servidor OpenVas (Localhost:9392), se configura el “target” mediante la dirección IP.

Captura de Pantalla 7. CP_07 Configuracion destino OpenVas

Fuente: El presente documento

Con la identificación del destino se configura la tarea a ejecutar.

Captura de Pantalla 8. CP_08 Configuracion tarea OpenVas

Fuente: El presente documento

La ejecución de la tarea da como resultado el siguiente reporte.

Captura de Pantalla 9. CP_09 Reporte tarea OpenVas

Fuente: El presente documento

De la ejecución de este proceso se obtienen las evidencias referenciadas en el *Anexo 2. Evidencias evaluación del* **servidor con OpenVas**

Anexo 2. Evidencias evaluación del servidor con OpenVas

Previa la identificación de la arquitectura de red e identificando como equipo servidor el identificado con IP 192.168.1.150, se procede a la realización de las pruebas de vulnerabilidades haciendo uso de OpenVas. De estas pruebas se obtiene como resultados las siguientes evidencias:

Con lo relacionado a puertos en el servidor, el aplicativo hace un escaneo de un total de 40 puertos y encuentra vulnerabilidades en 8 de estos como se enuncian a continuación:

Evidencia 1: Lista de puertos identificados con vulnerabilidades

Port	Severidad
135/tcp	5.0
443/tcp	6.4
636/tcp	4.3
3269/tcp	4.3
3389/tcp	4.3
26790/tcp	7.5
65500/tcp	5.0
65520/tcp	5.0

Fuente: El presente documento

Con base en el sistema operativo instalado:

Evidencia 2: Evaluación del sistema operativo

Descripción del sistema operativo

Sistema operativo	CPE	Severidad
Microsoft Windows	cpe:/o: Microsoft: windows_server_2012	7.5 (High)

Fuente: El presente documento

Los detalles de las vulnerabilidades identificadas en el servidor Windows se especifican a continuación

Evidencia 3: Lista de vulnerabilidades encontradas para el sistema operativo Windows Server 2012, IP 192.168.1.150

Nombre	Sev.	Nombre	Sev.	Nombre	Sev.	Nombre	Sev.
CVE-2017-11771	10.0	CVE-2017-0296	7.2	CVE-2017-0169	5.2	CVE-2018-0904	1.9
CVE-2017-8718	9.3	CVE-2016-3250	7.2	CVE-2018-0824	5.1	CVE-2018-0901	1.9
CVE-2017-8717	9.3	CVE-2016-0197	7.2	CVE-2018-0888	4.7	CVE-2018-0900	1.9
CVE-2017-8620	9.3	CVE-2016-0196	7.2	CVE-2017-11831	4.7	CVE-2018-0899	1.9
CVE-2017-11847	9.3	CVE-2016-0180	7.2	CVE-2018-0846	4.6	CVE-2018-0898	1.9
CVE-2017-0250	9.3	CVE-2016-0176	7.2	CVE-2018-0844	4.6	CVE-2018-0897	1.9
CVE-2017-0166	9.3	CVE-2016-0174	7.2	CVE-2018-8167	4.4	CVE-2018-0896	1.9
CVE-2016-0170	9.3	CVE-2016-0173	7.2	CVE-2017-11927	4.3	CVE-2018-0895	1.9
CVE-2017-8633	8.5	CVE-2016-0171	7.2	CVE-2017-11853	4.3	CVE-2018-0894	1.9
CVE-2018-8174	7.6	CVE-2016-0041	7.2	CVE-2017-0211	4.3	CVE-2017-8554	1.9
CVE-2018-0886	7.6	CVE-2018-8166	6.9	CVE-2017-0192	4.3	CVE-2017-8479	1.9
CVE-2018-0883	7.6	CVE-2018-0881	6.9	CVE-2016-0168	4.3	CVE-2017-8477	1.9
CVE-2018-0825	7.6	CVE-2018-0842	6.9	CVE-2017-0191	3.5	CVE-2017-8476	1.9
CVE-2017-0293	7.6	CVE-2017-8593	6.9	CVE-2017-0076	2.9	CVE-2017-8475	1.9

CVE-2017-0158	7.6	CVE-2018-0885	6.3	CVE-2017-0097	2.3	CVE-2017-8474	1.9
CVE-2017-0023	7.6	CVE-2017-0186	6.3	CVE-2017-0074	2.3	CVE-2017-8473	1.9
CVE-2018-0959	7.4	CVE-2017-0185	6.3	CVE-2018-8116	2.1	CVE-2017-8472	1.9
CVE-2017-0181	7.4	CVE-2017-0183	6.3	CVE-2018-0926	2.1	CVE-2017-8471	1.9
CVE-2017-0180	7.4	CVE-2017-0182	6.3	CVE-2018-0814	2.1	CVE-2017-8470	1.9
CVE-2017-0163	7.4	CVE-2017-0179	6.3	CVE-2018-0813	2.1	CVE-2017-11850	1.9
CVE-2018-8164	7.2	CVE-2017-0168	6.3	CVE-2018-0811	2.1	CVE-2017-11849	1.9
CVE-2018-1009	7.2	CVE-2017-0174	6.1	CVE-2018-0760	2.1	CVE-2017-11842	1.9
CVE-2017-8664	7.2	CVE-2017-8495	6.0	CVE-2017-8668	2.1	CVE-2017-11832	1.9
CVE-2017-8624	7.2	CVE-2017-0184	5.2	CVE-2017-8666	2.1	CVE-2017-0297	1.9
CVE-2017-8591	7.2	CVE-2017-0178	5.2	CVE-2017-0188	2.1	CVE-2017-0058	1.9

Fuente: El presente documento

Para el presente estudio se analizarán y evaluarán las vulnerabilidades con severidad (Sev.) superior a 7,5

Lo que da como resultado

Evidencia 4: Descripción de las vulnerabilidades analizadas

Nombre	Severidad	Descripción
CVE-2017-11771	10.0	El componente Microsoft Windows Search en Microsoft Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, y 1703 y Windows Server 2016 permite una vulnerabilidad de ejecución remota de código cuando no gestiona correctamente respuestas DNS. Esto también se conoce como "Windows Search Remote Code Execution Vulnerability"[57].
CVE-2017-8718	9.3	El motor de base de datos JET de Microsoft en Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1 y RT 8.1, Windows Server 2012 y R2, Windows 10 Gold, 1511, 1607, 1703 y Windows Server 2016 permiten que un atacante tome el control de un sistema afectado, debido a la forma en que maneja los objetos en la memoria, también conocida como "Vulnerabilidad de ejecución remota de código en el motor de base de datos JET de Microsoft". Este ID de CVE es único de CVE-2017-8717[58].
CVE-2017-8717	9.3	El motor de base de datos JET de Microsoft en Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1 y RT 8.1, Windows Server 2012 y R2, Windows 10 Gold, 1511, 1607, 1703 y Windows Server 2016 permiten que un atacante tome el control de un sistema afectado, debido a la forma en que maneja los objetos en la memoria, también conocida como "Vulnerabilidad de ejecución remota de código en el motor de base de datos JET de Microsoft". Este ID de CVE es único de CVE-2017-8718[59].

[57] INCIBE-CERT.ES. Vulnerabilidad en el componente Microsoft Windows Search en productos Microsoft (CVE-2017-11771) [en línea]. 2017. [Consultado: 20 de julio de 2018]. Disponible en internet: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-11771

[58] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). Vulnerability Details: CVE-2017-8717. [en línea] 13 de 10 de 2017. [Consultado: 20 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-8718

[59]CVEDETAILS. Details. [en línea] 13 de 10 de 2017.[Consultado: 24 de julio de 2018]. Disponible en internet://www.cvedetails.com/cve/cve-2017-8717

CVE-2017-8620	9.3	Una vulnerabilidad de ejecución remota de código existe cuando Windows Search administra objetos en la memoria. Un atacante que explote con éxito esta vulnerabilidad podría lograr el control del sistema afectado. El atacante podría instalar programas; ver, cambiar o eliminar datos; o crear cuentas nuevas con derechos de usuario completos[60].
CVE-2017-11847	9.3	El kernel de Windows en Windows 7 SP1, Windows Server 2008 SP2 y R2 SP1, Windows 8.1 y RT1, Windows Server 2012 y R2, Windows 10 Gold, 1511, 1607, 1703 y 1709, Windows Server 2016 y Windows Server, versión 1709, permiten un atacante para ejecutar código arbitrario en modo kernel, instalar programas, ver, cambiar o eliminar datos, y crear nuevas cuentas con derechos de usuario completos debido a la entrega indebida de objetos en la memoria, también conocido como "Vulnerabilidad de la elevación de privilegios en el kernel de Windows"[61].
CVE-2017-0250	9.3	Microsoft JET Database Engine en Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, y Windows Server 2016 permite una ejecución remota de código vulnerabilidad debida al desbordamiento de búfer, también conocida como "Vulnerabilidad de ejecución remota de código en el motor de base de datos JET de Microsoft"[62].
CVE-2017-0166	9.3	Existe una vulnerabilidad de elevación de privilegios en Windows cuando las longitudes del búfer de solicitud LDAP se calculan incorrectamente. En un escenario de ataque remoto, un atacante podría aprovechar esta vulnerabilidad al ejecutar una aplicación especialmente diseñada para

[60]MICROSOFT. Soporte Técnico de Microsoft. Actualización de seguridad para la vulnerabilidad de ejecución remota de código de Windows Search: 8 de agosto de 2017. [en línea] 8 de 08 de 2017. [Consultado: 20 de julio de 2018]. Disponible en internet: obtenido de https://support.microsoft.com/es-co/help/4034034/windows-search-remote-code-execution-vulnerability

[61] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-11847 Detail. [en línea]. 14 de 11 de 2017. [Consultado: 30 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-11847

[62] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0250 Detail. [en línea]. 08 de 08 de 2017. [Consultado: 30 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0250

		enviar tráfico malicioso a un controlador de dominio, también conocido como "vulnerabilidad de elevación de privilegios de LDAP"[63].
CVE-2016-0170	9.3	GDI en Microsoft Windows Vista SP2, Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1 y Windows 10 Gold y 1511 permiten a atacantes remotos ejecutar código atacante a través de un documento elaborado, también conocido como "Vulnerabilidad de RCE del componente de gráficos de Windows"[64].
CVE-2017-8633	8.5	Windows Error Reporting (WER) en Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, y Windows Server 2016 permite una elevación de vulnerabilidad de privilegio, también conocida como "Vulnerabilidad de privilegio de privilegio de notificación de errores de Windows"[65].
CVE-2018-8174	7.6	Existe una vulnerabilidad de ejecución remota de código en la forma en que el motor VBScript maneja los objetos en la memoria, también conocida como "Vulnerabilidad de ejecución remota de código en el motor VBScript de Windows". Esto afecta a Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servidores[66].

[63] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0166 Detail. [en línea]. 12 de 04 de 2017. [Consultado: 30 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0166

[64]NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2016-0170 Detail. [en línea]. 05 de 10 de 2016. [Consultado: 30 de julio de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2016-0170

[65] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-8633 Detail. [en línea]. 08 de 08 de 2017. [Consultado: 2 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-8633

[66] CVE (COMMON VULNERABILITIES AND EXPOSURES). CVE-2018-8174. [en línea]. 14 de 03 de 2018. [Consultado: 3 de agosto de 2018]. Disponible en internet: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174

CVE-2018-0886	7.6	El protocolo del proveedor de soporte de seguridad de credenciales (CredSSP) en Microsoft Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1 y RT 8.1, Windows Server 2012 y R2, Windows 10 Gold, 1511, 1607, 1703 y 1709 Windows Server 2016 y Windows Server, versión 1709 permite una vulnerabilidad de ejecución remota de código debido a cómo CredSSP valida la solicitud durante el proceso de autenticación, también conocida como "Vulnerabilidad de ejecución remota de código de CredSSP"[67].
CVE-2018-0883	7.6	Windows Shell en Microsoft Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1 y RT 8.1, Windows Server 2012 y R2, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016 y Windows Server, la versión 1709 permite un control remoto vulnerabilidad de ejecución de código debida a la forma en que se validan los destinos de copia de archivos, también conocida como "Vulnerabilidad de ejecución remota de código en el shell de Windows"[68].
CVE-2018-0825	7.6	StructuredQuery en Windows 7 SP1, Windows 8.1 y RT 8.1, Windows Server 2008 SP2 y R2 SP1, Windows Server 2012 y R2, Windows 10 Gold, 1511, 1607, 1703 y 1709, Windows Server 2016 y Windows Server, versión 1709 permite un control remoto vulnerabilidad de ejecución de código debida a cómo se manejan los objetos en la memoria, también conocida como "Vulnerabilidad de ejecución remota de código en StructuredQuery"[69].
CVE-2017-0293	7.6	Microsoft Windows PDF Library en Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703 y Windows Server 2016 permite una vulnerabilidad de ejecución remota de código cuando maneja objetos de

[67] CVE (COMMON VULNERABILITIES AND EXPOSURES) CVE-2018-0886. [en línea]. 01 de 12 de 2017. [Consultado: 4 de agosto de 2018]. Disponible en internet: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0886

[68]NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2018-0883 Detail. [en línea]. 14 de 03 de 2018. [Consultado 5 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2018-0883

[69] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2018-0825 Detail. [en línea]. 14 de 02 de 2018. [Consultado: 10 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2018-0825

		manera incorrecta en la memoria, también conocida como "Vulnerabilidad de ejecución remota de código en Windows PDF"[70].
CVE-2017-0158	7.6	Existe una vulnerabilidad de elevación de privilegios cuando Microsoft Windows se ejecuta en Windows 10, Windows 10 1511, Windows 8.1 Windows RT 8.1 y Windows Server 2012 R2 no puede desinfectar adecuadamente los identificadores en la memoria, también conocida como "Vulnerabilidad de corrupción de memoria en el motor de scripting"[71].
CVE-2017-0023	7.6	La biblioteca de PDF en Microsoft Edge; Windows 8.1; Windows Server 2012 y R2; Windows RT 8.1; y Windows 10, 1511 y 1607 permiten a los atacantes remotos ejecutar código arbitrario a través de un archivo PDF creado, también conocido como "Vulnerabilidad de ejecución remota de código en Microsoft PDF"[72].

Fuente: El presente documento

[70] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0293 Detail. [en línea]. 08 de 08 de 2017. [Consultado: 10 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0293

[71] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0158 Detail. [en línea]. 14 de 04 de 2017. [Consultado: 13 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0158

[72] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2017-0023 Detail. [en línea]. 16 de 03 de 2017. [Consultado: 13 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2017-0023

Evidencia 5: Vulnerabilidades y exposiciones comunes (CVE Common vulnerabilities and exposures)

CVE	Ocu.	Sev.	Descripción
CVE-2016-2183, CVE-2016-6329	4	5.0	Los cifrados DES y Triple DES, tal como se utilizan en los protocolos TLS, SSH e IPSec y otros protocolos y productos, tienen un límite de datos de aproximadamente cuatro mil millones de bloques, lo que facilita que los atacantes remotos obtengan datos de texto claro mediante un ataque de datos contra una sesión encriptada de larga duración, como lo demuestra una sesión HTTPS usando Triple DES en modo CBC, también conocido como ataque "Sweet32"[73].
CVE-2016-0800, CVE-2014-3566	6	4.3	El protocolo SSLv2, tal como se usa en OpenSSL antes de 1.0.1s y 1.0.2 antes de 1.0.2g y otros productos, requiere que un servidor envíe un mensaje de verificación de servicio antes de establecer que un cliente posee ciertos datos RSA de texto sin formato, lo que facilita el acceso a los atacantes remotos para descifrar datos de texto cifrado TLS aprovechando un dato de relleno RSA de Bleichenbacher, también conocido como un ataque "DROWN"[74].
CVE-2014-3566	6	4.3	El protocolo SSL 3.0, tal como se utiliza en OpenSSL a través de 1.0.1i y otros productos, utiliza un relleno CBC no determinista, lo que facilita que los atacantes de man-in-the-middle obtengan datos de texto claro a través de un ataque oráculo de relleno, también conocido como "POODLE". “problema[75].
CVE-2013-2566, CVE-2015-2808, CVE-2015-4000	7	4.3	El algoritmo RC4, tal como se utiliza en el protocolo TLS y el protocolo SSL, tiene muchos sesgos de un solo byte, lo que facilita que los

[73] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2016-2183 Detail. [en línea]. 31 de 08 de 2016. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2016-2183

[74] CVE (COMMON VULNERABILITIES AND EXPOSURES). CVE-2016-0800. [en línea]. 16 de 12 de 2015. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2016-0800

[75] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2014-3566 Detail. [en línea]. 10 de 14 de 2014. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2014-3566

			atacantes remotos realicen ataques de recuperación de texto simple mediante el análisis estadístico del texto cifrado en una gran cantidad de sesiones que utilizan el mismo texto simple[76].
CVE-2011-2900	1	7,5	Desbordamiento de búfer basado en la pila en la (1) función put_dir en mongoose.c en Mongoose 3.0, (2) función put_dir en yasslEWS.c en el servidor web incorporado de yaSSL (yasslEWS) 0.2, y (3) _shttpd_put_dir function en io_dir.c in HTTPD simple (shttpd) 1.42 permite a los atacantes remotos ejecutar código arbitrario a través de una solicitud HTTP PUT, como se explotó en la naturaleza en 2011[77].

Fuente: El presente documento

Evidencia 6: Vulnerabilidades de red encontradas en el servidor 192.168.1.150

Vulnerabilidad	Ocurrencia	Severidad
Mongoose Web Server Remote Buffer Overflow Vulnerability	1	7.5 (High)
SSL/TLS: Missing `secure` Cookie Attribute	1	6.4 (Medium)
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	4	5.0 (Medium)
DCE/RPC and MSRPC Services Enumeration Reporting	1	5.0 (Medium)
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	6	4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites	7	4.3 (Medium)
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	6	4.3 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	6	4.0 (Medium)
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	2	4.0 (Medium)

[76] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2013-2566 Detail. [en línea]. 15 de 03 de 2013. [Consultado: 20 de agosto de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2013-2566

[77] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). CVE-2011-2900 Detail. [en línea]. 08 de 05 de 2011. [Consultado: 10 de septiembre de 2018]. Disponible en internet: https://nvd.nist.gov/vuln/detail/CVE-2011-2900

Fuente: El presente documento

A continuación, se presenta a detalle la especificación de cada una de las vulnerabilidades encontradas:

Tabla 33. Detalle de especificaciones de las vulnerabilidades encontradas

Vulnerabilidad	Detalle
Mongoose Web Server Remote Buffer Overflow Vulnerability	**Resumen** El host ejecuta Mongoose Web Server y es propenso a la vulnerabilidad de desbordamiento de búfer remoto. **Impacto** La explotación exitosa permitirá a los atacantes remotos ejecutar código dañino en el contexto de la aplicación afectada. Los intentos fallidos de explotación darán como resultado una condición de denegación de servicio. Nivel de impacto: Aplicación del Sistema **Solución** Aplicar parche desde el siguiente enlace, https://code.google.com/p/mongoose/source/detail?r=025b11b1767a311b0434a385f5115463f6293ce9 **Análisis** La falla se debe a un error en la función 'put_dir ()' (mongoose.c) al procesar solicitudes web HTTP PUT. Esto se puede explotar para provocar un error de aserción o un desbordamiento de búfer basado en el desbordamiento de pila. **Afectado** Mongoose Web Server versión 3.0[78]
SSL/TLS: Missing `secure` Cookie Attribute	**Resumen**: El host está ejecutando un servidor con SSL / TLS y es propenso a la información vulnerabilidad de divulgación. **Perspectiva de la vulnerabilidad:** La falla se debe a que la cookie no está usando el atributo 'seguro', que permite que el cliente pase las cookies al servidor a través de canales no seguros (http) y permite al atacante para llevar a cabo ataques de secuestro de sesión. **Software / OS afectado:** Servidor con SSL / TLS. **Solución:**

[78] ACUNETIX. Mongoose Web Server Remote Buffer Overflow Vulnerability. [en línea]. 25 de 03 de 2015. [Consultado: 15 de septiembre de 2018]. Disponible en internet: https://www.acunetix.com/vulnerabilities/network/vulnerability/mongoose-web-server-remote-buffer-overflow-vulnerability/

	Establezca el atributo 'seguro' para cualquier cookie que se envíe a través de una conexión SSL / TLS[79].
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	**Resumen:** Esta rutina informa todos los conjuntos de cifrado SSL / TLS aceptados por un servicio donde los vectores de ataque solo existen en los servicios HTTPS. **Perspectiva de la vulnerabilidad:** Estas reglas se aplican para la evaluación de las suites de cifrado vulnerables: - Cifrado 3DES de bloque de 64 bits vulnerable al ataque SWEET32 (CVE-2016-2183). **Software / OS afectado:** Servicios que aceptan suites de cifrado SSL / TLS vulnerables a través de HTTPS. **Solución:** La configuración de estos servicios debe ser cambiada para que ya no acepta las suites de cifrado enumeradas[80].

Fuente: El presente documento

Tabla 34. Detalle de especificaciones de las vulnerabilidades encontradas (Continuación)

Vulnerabilidad	Detalle
DCE/RPC and MSRPC Services Enumeration Reporting	**Resumen:** Entorno de computación distribuida / Llamadas a procedimientos remotos (DCE / RPC) o servicios MSRPC en ejecución en el host remoto se puede enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas. **Impacto de vulnerabilidad:** Un atacante puede usar este hecho para obtener más conocimiento sobre el host remoto. **Solución:** Filtra el tráfico entrante a estos puertos[81].
SSL/TLS: SSLv3 Protocol CBC	**Resumen:** Este host es propenso a una vulnerabilidad de divulgación de información.

[79] SECURITYSPACE. SSL/TLS: Missing `secure` Cookie Attribute. [en línea]. 2012. [Consultado: 10 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.902661

[80] SECURITYSPACE, Ibid. p. 86

[81] SECURITY SPACE. DCE/RPC and MSRPC Services Enumeration Reporting. [en línea] 2017. [Consultado: 15 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.10736

Cipher Suites Information Disclosure Vulnerability (POODLE)	**Perspectiva de la vulnerabilidad:** La falla se debe a que el relleno del cifrado del bloque no es determinista y no está cubierto por el Código de autenticación del mensaje **Impacto de vulnerabilidad:** La explotación exitosa permitirá a ataques de hombre en el medio obtener acceso al flujo de datos de texto sin formato. **Solución:** Las posibles mitigaciones son: - Desactivar SSLv3 - Deshabilite las suites de cifrado compatibles con los modos de cifrado CBC - Habilite TLS_FALLBACK_SCSV si el servicio está proporcionando TLSv1.0 +[82]
SSL/TLS: Report Weak Cipher Suites	**Resumen:** el host remoto admite el uso de cifrados SSL que ofrecen un cifrado débil o ningún cifrado. **Pruebas de penetración (pentest) para esta vulnerabilidad:** Las vulnerabilidades de las suites SSL Cifras débiles son propensas a informes falsos positivos por la mayoría de las soluciones de evaluación de vulnerabilidades. AVDS está solo en el uso de pruebas basadas en el comportamiento que elimina este problema. Para todas las demás herramientas de VA, los consultores de seguridad recomendarán la confirmación mediante observación directa. **Solución:** Actualizaciones de seguridad sobre vulnerabilidades en las suites SSL Cifrados débiles[83].

Fuente: El presente documento

[82] SECURITY SPACE. SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE). [en línea]. 2014. [Consultado: 15 de octubre de 2018] Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.802087

[83] BEYOND SECURITY. Finding and Fixing Vulnerabilities in SSL Suites Weak Ciphers, a Medium Risk Vulnerability. [en línea]. 2018. [Consultado: 15 de octubre de 2018]Disponible en internet: https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_ssl_suites_weak_ciphers

Tabla 35. Detalle de especificaciones de las vulnerabilidades encontradas (Continuación)

Vulnerabilidad	**Detalle**
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	**Resumen:** Fue posible detectar el uso de la Protocolo SSLv2 y / o SSLv3 obsoletos en este sistema. **Perspectiva de la vulnerabilidad:** Los protocolos SSLv2 y SSLv3 que contienen fallas criptográficas conocidas como: - Relleno de Oracle en cifrado heredado degradado (POODLE, CVE-2014-3566) - Descifrando RSA con eNcryption obsoleto y debilitado (DROWN, CVE-2016-0800) **Impacto de vulnerabilidad:** Un atacante podría ser capaz de usar lo conocido sobre fallas criptográficas para espiar la conexión entre los clientes y el servicio, para acceder a datos confidenciales transferidos dentro de la conexión segura. **Software afectado:** Todos los servicios que proporcionan una comunicación encriptada utilizando los protocolos SSLv2 y / o SSLv3. **Solución:** Se recomienda deshabilitar el desaprobado. Protocolos SSLv2 y / o SSLv3 a favor de los protocolos TLSv1 +[84].
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	**Resumen:** El servicio SSL / TLS utiliza grupos Diffie-Hellman con una resistencia insuficiente (tamaño de clave <2048). **Perspectiva de la vulnerabilidad:** El grupo Diffie-Hellman son algunos números grandes que se utilizan como base para los cálculos de DH. Pueden ser, y con frecuencia son, fijas. La seguridad final depende del tamaño de estos parámetros. Se encontró que 512 y 768 bits eran débiles, 1024 bits pueden ser rompibles por atacantes como los gobiernos. **Impacto de vulnerabilidad:** Un atacante podría descifrar la comunicación SSL / TLS sin conexión.

[84] SECURITY SPACE. The SSL/TLS service uses Diffie-Hellman groups with insufficient strength; (key size < 2048). [en línea]. 2016. [Consultado: 20 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.106223

	Solución: Despliegue de curva elíptica Diffie-Hellman (ECDHE) o use un grupo Diffie-Hellman de 2048 bits o más fuerte. Para servidores web Apache: A partir de la versión 2.4.7, mod_ssl usará parámetros DH que incluyen números primos con longitudes de más de 1024 bits[85].

Tabla 36. Detalle de especificaciones de las vulnerabilidades encontradas (Continuación)

Vulnerabilidad	**Detalle**
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	**Resumen:** El servicio remoto está utilizando un certificado SSL / TLS en la cadena de certificados que se ha firmado con un criptográficamente débil algoritmo hash. **Perspectiva de la vulnerabilidad:** Los siguientes algoritmos de hashing utilizados para firmar certificados SSL / TLS se consideran criptográficamente débiles y no lo suficientemente seguro para su uso continuo: - Secure Hash Algorithm 1 (SHA-1) - Mensaje Digest 5 (MD5) - Mensaje Digest 4 (MD4) - Mensaje Digest 2 (MD2) A partir de enero de 2017 y junio de 2016, los desarrolladores de navegadores como Microsoft y Google empezarán a advertir a los usuarios cuando visiten sitios web que utilizan SHA-1 certificados Secure Socket Layer (SSL) firmados. NOTA: La preferencia de script permite establecer una o más huellas dactilares SHA-1 personalizadas de certificados de CA que son de confianza para esta rutina. Las huellas dactilares deben ser pasado por comas y no debe distinguir entre mayúsculas y minúsculas: Huella dactilar1 o huella digital1, huella digital2 **Solución:** Los servidores que utilizan certificados SSL / TLS firmados con un algoritmo hash SHA-1, MD5, MD4 o MD2 débil deberán obtener

[85] SECURITY SPACE. SSL/TLS: Certificate Signed Using A Weak Signature Algorithm. [en línea]. 2016. [Consultado 25 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.105880

	nuevos SHA-2 para firma de certificados SSL / TLS para evitar advertencias de certificados SSL / TLS del navegador web[86].

Fuente: El presente documento

Evidencia 7: Detalles de las Vulnerabilidades de red encontradas por puertos

Vulnerabilidad	Severidad	QoD	Localización
Mongoose Web Server Remote Buffer Overflow Vulnerability	7.5 (High)	99%	26790/tcp
SSL/TLS: Missing `secure` Cookie Attribute	6.4 (Medium)	99%	443/tcp
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98%	65520/tcp
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98%	65500/tcp
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98%	26790/tcp
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98%	443/tcp
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	135/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	65520/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	65500/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	26790/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	3269/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	636/tcp

[86] SECURITY SPACE. SSL/TLS: Report Vulnerable Cipher Suites for HTTPS. [en línea]. 2016. [Consultado: 25 de octubre de 2018]. Disponible en internet: http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108031

SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	443/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	65520/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	65500/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	26790/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	3389/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	3269/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	636/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	443/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	65520/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	65500/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	26790/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	3269/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	636/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	443/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	65520/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	65500/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	3389/tcp

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	3269/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	636/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	443/tcp
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	26790/tcp
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	3389/tcp

Fuente: El presente documento

Anexo 3. Evidencias y resultados comando NMAP red 192.168.1.0/24

Para la identificación de puertos y equipos disponibles en la red al momento de realizar las pruebas se ha hecho uso del comando NMAP el que ha permitido el mapeo de la red de los equipos disponibles en la etapa de recolección de información, con base en este proceso de recolección de evidencias se pudo determinar que los hosts disponibles con sus respectivas direcciones IP son los siguientes:

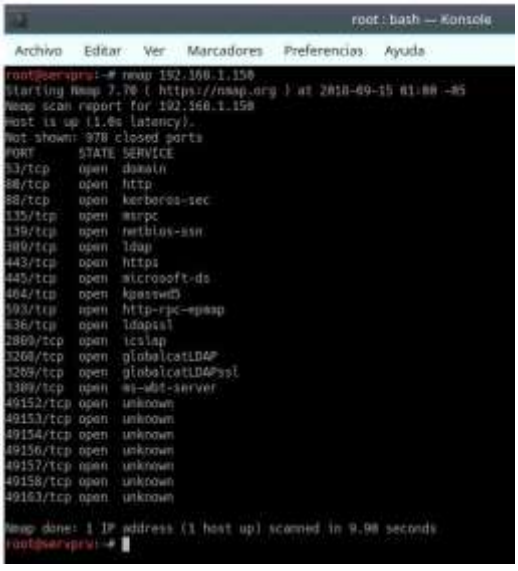
Evidencia 8: Relación direcciones IP hosts identificados

Dirección IP	Descripción
192.168.1.172	Equipo Portátil Gerencia
192.168.1.169	Equipo Asistente 1
192.168.1.164	Equipo Caja
192.168.1.165	Equipo Asistente 2
192.168.1.166	Equipo Cartera
192.168.1.161	Equipo Salas de velación
192.168.1.162	Equipo Gerencia
192.168.1.163	Equipo Contador
192.168.1.150	Servidor Jardines Cristo Rey Ltda.

Fuente: El presente documento

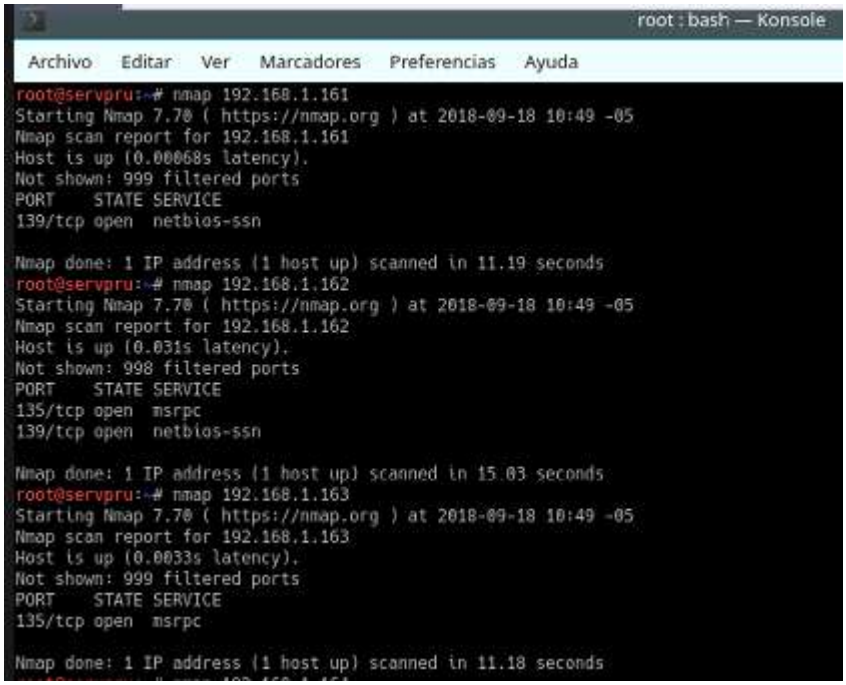
Una vez identificados los equipos activos en red se procede a la identificación de puertos disponibles en cada uno dando como resultado las siguientes evidencias:

Evidencia 9: Resultado NMAP 192.168.1.150



Fuente: El presente documento

Evidencia 10: Resultado NMAP 192.168.1.161, 192. 168..1.162, 192.168.1.163



Fuente: El presente documento

Evidencia 11: Resultado NMAP 192.168.1.164, 192.168.1.165, 192.168.1.166

Fuente: El presente documento

Evidencia 12: Resultado NMAP 192.168.1.169

Fuente: El presente documento

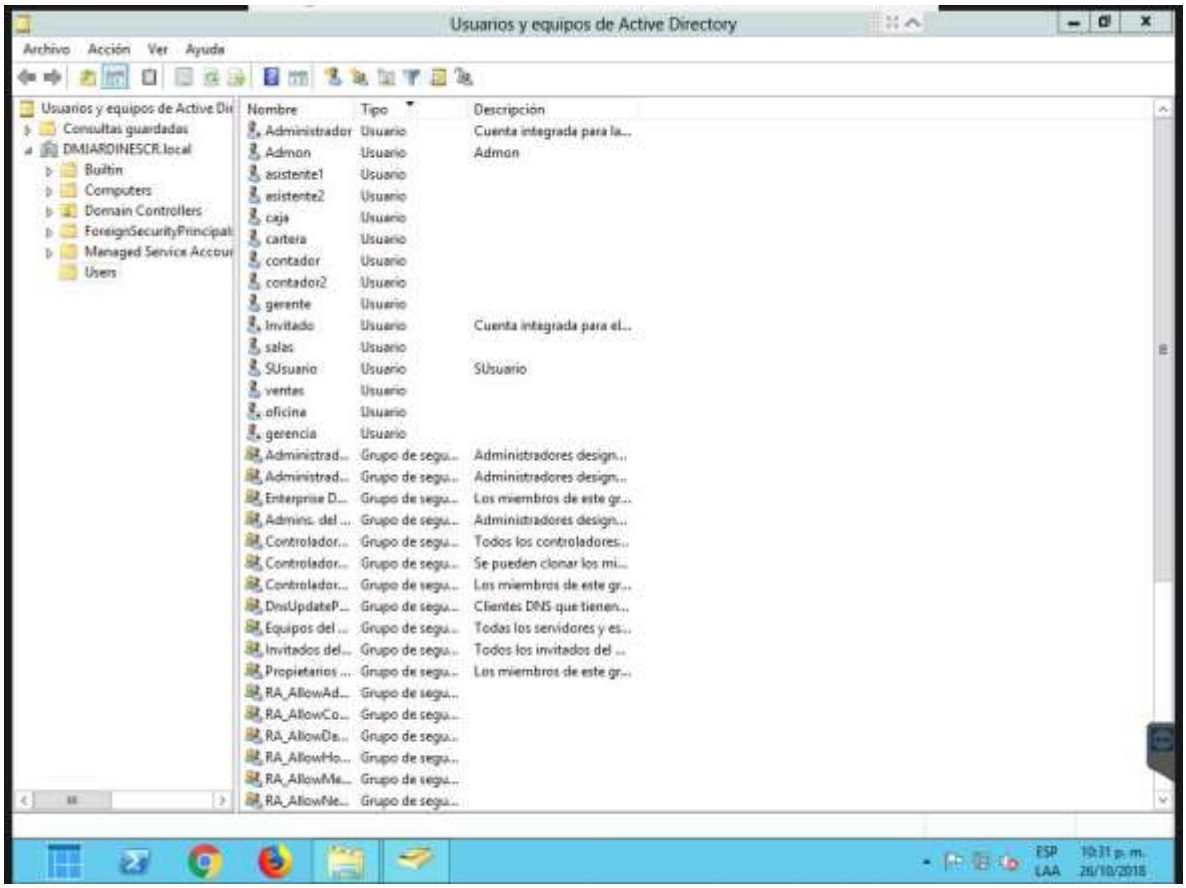
Evidencia 13: Resultado NMAP 192.168.1.172

Fuente: El presente documento

Anexo 4. Evidencias configuraciones cuentas y prácticas de seguridad sobre equipos

Sobre el manejo de cuentas de usuario y tomando en cuenta que se requiere identificar de manera acertada la forma en la cual se administran y configuran las cuentas de usuario, se procede a verificar dichas configuraciones, dando como resultado las siguientes evidencias:

Evidencia 14: Listado cuentas de usuarios configurados



Fuente: El presente documento

De la lista de cuentas de usuario activas se puede identificar cuales corresponden con equipos activos actualmente y cuales se debieron deshabilitar o eliminar por no estar en uso.

Tabla 37. Relación de cuentas con equipos de cómputo

Usuario	IP	Descripción
Administrador	Cuenta Integrada de Windows	Cuenta administradora por defecto de Windows
Admon	Sin emplearse	Cuenta administradora para comunicaciones remotas
asistente1	192.168.1.169	Equipo en oficina de asistente de ventas
asistente2	192.168.1.165	Equipo en oficina de asistente de personal
caja	192.168.1.164	Equipo en oficina de caja
cartera	192.168.1.166	Equipo en oficina de cartera
contador	192.168.1.163	Equipo en oficina de contador
contador2	192.168.1.170	Equipo en oficina de contador
gerente	192.168.1.162	Equipo en oficina de gerencia
Invitado	Cuenta Integrada de Windows	Sin equipo
salas	192.168.0.161	Equipo en oficina de salas de velación
Susuario	192.168.1.150	Cuenta administradora del sistema
ventas	192.168.1.172	Equipo en oficina de ventas
oficina	Sin emplearse	Sin equipo
gerencia	Sin emplearse	Sin equipo

Fuente: El presente documento

En cuanto al manejo de contraseñas, los permisos de usuarios asignados al respecto presentan las siguientes evidencias:

Evidencia 15: Listado cuentas de usuarios configurados

Fuente: El presente documento

Evidencia 16: Listado cuentas de usuarios configurados

Fuente: El presente documento

Con relación al manejo y control que se tienen sobre equipos desatendidos, de lo que se obtienen las siguientes evidencias:

Evidencia 17: Equipo asistente de ventas desatendido con sesión abierta

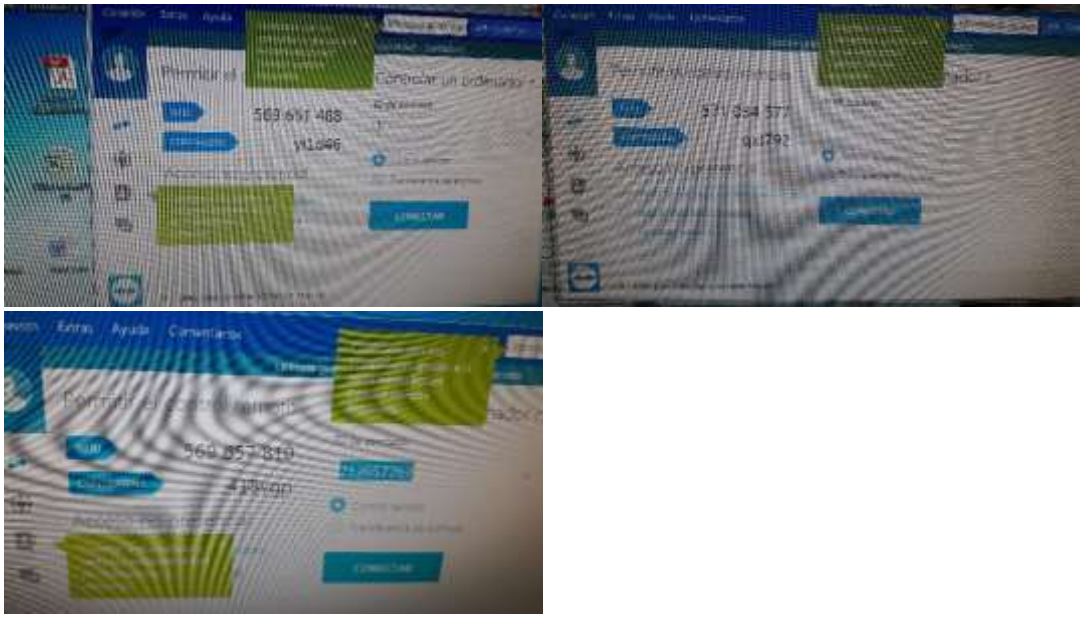
Fuente: El presente documento

Evidencia 18: Equipo de salas de velación desatendido con sesión abierta

Fuente: El presente documento

Sobre la posibilidad de acceso de manera remota a los equipos se tiene que todos los equipos de la compañía tienen instalado el aplicativo TeamViewer, sin embargo, no existen políticas sobre la forma en la cual debe ser utilizado, de lo cual se obtiene la siguiente evidencia:

Evidencia 19: Uso de TeamViewer para conexiones remotas.



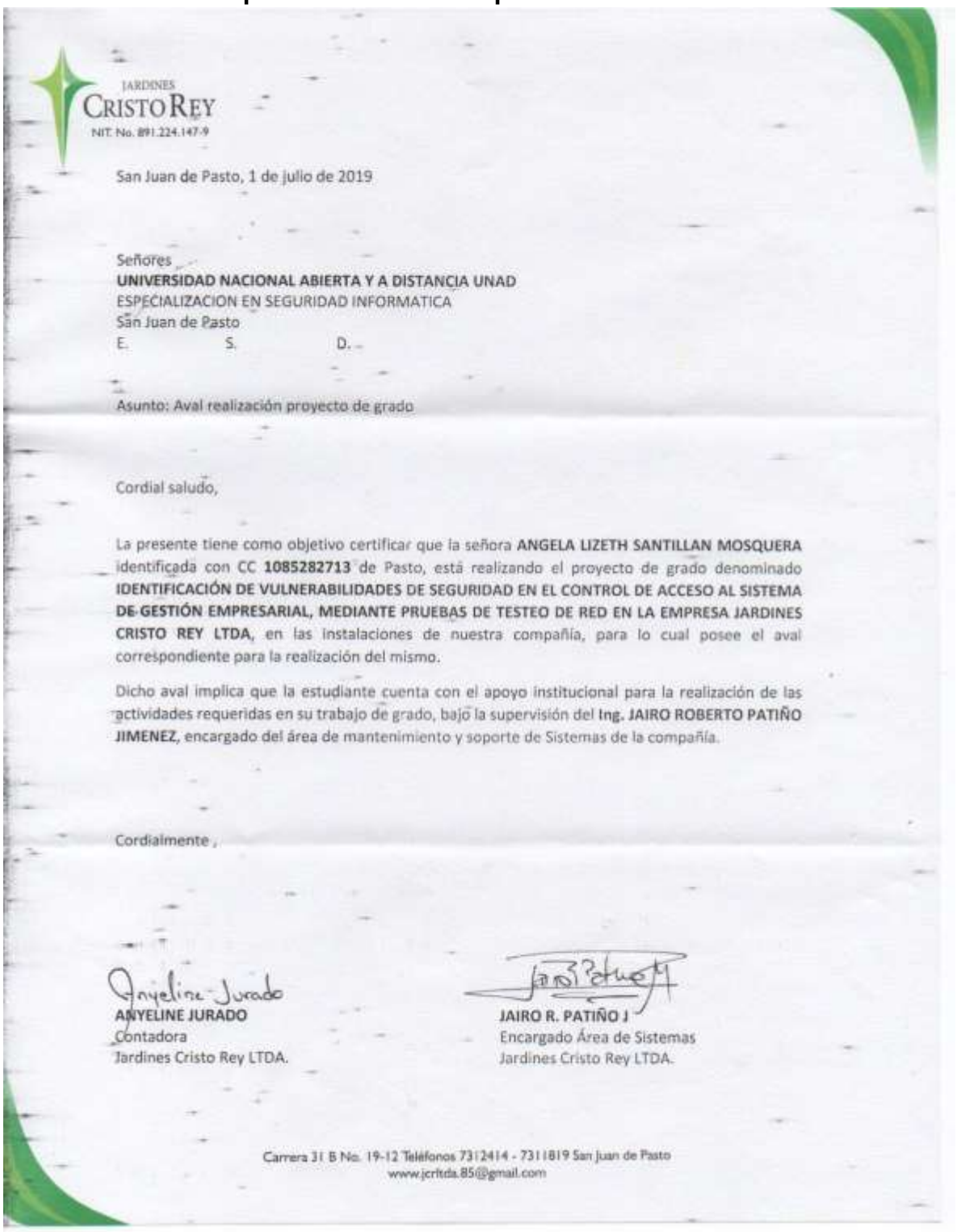
Fuente: El presente documento

En cuanto al entorno informático dedicado para los sistemas sensibles, el servidor, el rack de comunicaciones, se tienen las siguientes evidencias:

Evidencia 20: Cuarto de comunicaciones y ubicación del servidor.

Fuente: El presente documento

Anexo 5. Carta de aprobación de la compañía



JARDINES
CRISTO REY
NIT. No. 891.224.147-9

San Juan de Pasto, 1 de julio de 2019

Señores
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
San Juan de Pasto
E. S. D.

Asunto: Aval realización proyecto de grado

Cordial saludo,

La presente tiene como objetivo certificar que la señora **ANGELA LIZETH SANTILLAN MOSQUERA** identificada con CC **1085282713** de Pasto, está realizando el proyecto de grado denominado **IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN EMPRESARIAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA JARDINES CRISTO REY LTDA**, en las instalaciones de nuestra compañía, para lo cual posee el aval correspondiente para la realización del mismo.

Dicho aval implica que la estudiante cuenta con el apoyo institucional para la realización de las actividades requeridas en su trabajo de grado, bajo la supervisión del **Ing. JAIRO ROBERTO PATIÑO JIMENEZ**, encargado del área de mantenimiento y soporte de Sistemas de la compañía.

Cordialmente,

Anyeline Jurado
ANYELINE JURADO
Contadora
Jardines Cristo Rey LTDA.

JAIRO R. PATIÑO J
Encargado Área de Sistemas
Jardines Cristo Rey LTDA.

Carrera 31 B No. 19-12 Teléfonos 7312414 - 7311819 San Juan de Pasto
www.jcrltda.85@gmail.com