UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA METODOLOGÍA NIST SP 800-30 Y NIST SP 800-115 PARA LA EMPRESA TEXTILES JHONATEX

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Ingeniero en Sistemas Computacionales e Informáticos

LÍNEA DE INVESTIGACIÓN: Normas y Estándares

AUTOR: Jefersson Vinicio Bonilla Guerrero
TUTOR: Ing.David Omar Guevara Aulestia

Ambato - Ecuador
Febrero, 2021

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Investigación con el Tema: “ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA METODOLOGÍA NIST SP 800-30 Y NIST SP 800-115 PARA LA EMPRESA TEXTILES JHONATEX”, desarrollado bajo la modalidad Proyecto de Investigación por el señor Jefersson Vinicio Bonilla Guerrero, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, febrero de 2021

Firmado electrónicamente por:
DAVID OMAR
GUEVARA
AULESTIA

Ing. David Omar Guevara Aulestia, Mg

EL TUTOR

AUTORÍA

El presente trabajo de investigación titulado: "ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA METODOLOGÍA NIST SP 800-30 Y NIST SP 800-115 PARA LA EMPRESA TEXTILES JHONATEX". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, febrero de 2021

Jefersson Vinicio Bonilla Guerrero

CC: 1804399648

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Jefersson Vinicio Bonilla Guerrero, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado "ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA METODOLOGÍA NIST SP 800-30 Y NIST SP 800-115 PARA LA EMPRESA TEXTILES JHONATEX", nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, febrero de 2021

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.

PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
RUBEN EDUARDO NOGALES PORTERO

Ing. Rubén Nogales, Mg.
DOCENTE CALIFICADOR

Firmado electrónicamente por:
OSCAR FERNANDO IBARRA TORRES

Ing. Fernando Ibarra, Mg.
DOCENTE CALIFICADOR

DERECHOS DE AUTOR

Ambato, febrero de 2021

Jefersson Vinicio Bonilla Guerrero

CC: 1804399648

DEDICATORIA

El presente proyecto de tesis primeramente está dirigido a ti mi Dios, por bendecirme para llegar hasta donde he llegado, porque hiciste realidad el sueño de mis padres y el mío.

A mis padres, que en todo momento han sido mi pilar principal para lograr el cumplimiento de mis objetivos, por el apoyo incondicional y sus consejos llenos de sabiduría, lo que me permitió ser la persona que soy en la actualidad.

A la señora, Lidia Marlene Arcos Miranda, por su apoyo incondicionalmente desde que era un niño y ahora permitirme aplicar los conocimientos adquiridos durante estos nueve semestres de formación académica en su prestigiosa empresa.

Jefersson Vinicio Bonilla Guerrero

AGRADECIMIENTO

Agradezco a cada uno de los ingenieros que formaron parte de mi formación universitaria, en especial a mi tutor Ing. Guevara que me guió y me apoyo para la realización de este proyecto.

A mis padres por darme la oportunidad de estudiar, a mi hermano por no darme no dejarme solo en los momentos más difíciles de mi vida.

Y a mis amigos de la universidad que son pocos, sin embargo, cada uno de ellos me apoyaron de distintas maneras para llegar a este punto de mi vida.

Jefersson Vinicio Bonilla Guerrero

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

En la encuesta sobre Tendencias de Cyber Riesgos y Seguridad de la Información, realizado en el año 2018 en el Ecuador, muestra que las organizaciones se encuentran inmersas en un contexto de fuerte desarrollo de negocios digitales, implementando nuevas tecnologías en sus sistemas de información, por tal motivo se exponen a mayores riesgos inherentes a este nuevo contexto de negocio, ocasionando pérdidas económicas significativas o la perdida de la reputación, causadas por el surgimiento de vulnerabilidades en las nuevas tecnologías, que los criminales cibernéticos están a la espera de aprovechar esas vulnerabilidades.

Por tal motivo, para proteger proactivamente a la empresa Textiles Jhonatex, se propone un proceso de gestión de vulnerabilidades adoptado la metodología NIST 800-115 con un enfoque defensivo en las vulnerabilidades en tecnologías de la información, puesto que cada día se descubren miles de estas, mediante software de auditoría que permitirá identificar, analizar y remediar las vulnerabilidades de mayor preocupación. La definición de un esquema para administrar vulnerabilidades técnicas, mejoraría la seguridad informática de la empresa, sin embargo, es necesario conocer los riesgos a los que está expuesto la empresa, con el propósito de mejorar los niveles de protección, haciendo uso de la metodología NIST 800-30 se logrará definir estrategias que permitirán disminuir el impacto adverso que puede causar una o varias fuentes de amenazas. Al utilizar ambas metodologías, se logrará niveles óptimos en la seguridad de la información.

Palabras clave: Seguridad Informática, Metodología NIST SP 800:30, Gestión de Vulnerabilidades, Evaluación de Seguridad.

ABSTRACT

In the survey on Trends in Cyber Risks and Information Security, carried out in 2018 in Ecuador, it shows that organizations are immersed in a context of strong development of digital businesses, implementing new technologies in their information systems, for For this reason, they are exposed to greater risks inherent in this new business context, causing significant economic losses or loss of reputation, caused by the emergence of vulnerabilities in new technologies, that cyber criminals are waiting to exploit these vulnerabilities.

For this reason, to proactively protect the Textiles Jhonatex company, a vulnerability management process is proposed, adopted the NIST 800-115 methodology with a defensive approach to vulnerabilities in information technology, since thousands of these are discovered every day. , by means of auditing software that will allow to identify, analyze and remedy the vulnerabilities of greatest concern. The definition of a scheme to manage technical vulnerabilities, would improve the computer security of the company, however, it is necessary to know the risks to which the company is exposed, in order to improve protection levels, use of the NIST 800 methodology -30 it will be possible to define strategies to reduce the adverse impact that one or more sources of threats can cause. By using both methodologies, optimal levels of information security will be achieved.

Keywords: Computer Security, NIST SP 800: 30 Methodology, Vulnerability Management, Security Assessment.

INTRODUCCIÓN

El presente Proyecto "ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA METODOLOGÍA NIST SP 800-30 Y NIST SP 800-115 PARA LA EMPRESA TEXTILES JHONATEX", consta de capítulos los cuales se detallan a continuación:

Capítulo 1: "MARCO TEÓRICO", en este capítulo se define el problema, delimita su alcance, se justifica la investigación, asimismo, la recopilación de información para comprender el problema y plantear una propuesta para la solución, y se plantean los objetivos que se obtendrán después de culminar el trabajo de investigación.

Capítulo 3: "METODOLOGÍA", se especifica la metodología y las modalidades de investigación, igualmente el proceso de recolección de información, además se define las etapas del desarrollaro el proyecto.

Capítulo 3: "RESULTADOS Y DISCUSIÓN", se describe el desarrollo de la propuesta de la solución de manera precisa, haciendo énfasis en las partes esenciales del desarrollo

Capítulo 4: "CONCLUSIONES Y RECOMENDACIONES", en esta sección se muestra las conclusiones y recomendaciones que se encontraron en las diferentes etapas del desarrollo del proyecto.

CAPÍTULO I

MARCO TEÓRICO

1.1. Tema de Investigación

ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA METODOLOGÍA NIST SP 800-30 Y NIST SP 800-115 PARA LA EMPRESA TEXTILES JHONATEX.

1.2. Antecendentes Investigativos

1.2.1. Contextualización del problema

El presente trabajo de investigación está basado por los siguientes antecedentes investigativos obtenidos por medio de la revisión bibliográfica de los repositorios digitales, tanto nacionales como extranjeros.

Según el trabajo de los señores Johari Chris García Porras y Sarita Cecilia Huamani Pastor en el año 2019 de título “Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú”, de la Universidad de Ciencias Aplicadas de la ciudad de Lima. Manifiestan que el emplear un modelo de gestión de riesgos para empresas pequeñas como el caso de la empresa Pymes es de gran utilidad, debido a que la mayoría de estas no cuenta con el presupuesto suficiente para que una empresa evalué la situación actual referente a la seguridad de la información.

Concluyeron que se logró una reducción del riesgo de seguridad de información sobre los activos más críticos de la empresa, proponiendo controles e indicadores que permitan mejorar la gestión de riesgos y manteniendo un constante monitoreo del mismo [1].

El ingeniero Quirumba y Yagual Daniel en el 2015 realizó el proyecto de investigación “Desarrollo del esquema de seguridad, plan de recuperación ante desastres informáticos y solución para el nivel de exposición de amenazas y vulnerabilidades aplicada a los servidores y equipos de comunicación del centro de datos de la municipalidad de la ciudad de Guayaquil", de la Escuela Superior politécnica del Litoral. Manifiesta que el implementar seguridad informática a las infraestructuras tecnológicas concretamente para el Centro de Procesamiento de Datos se ha convertido en una requisito debido a que si se logra estimar la regularidad con la cual se materializan los riesgos, así también como determinar la intensidad de sus posibles consecuencias teniendo en cuenta las debidas precauciones, se tomaría de forma preventiva optar por medidas para reducir su efecto y evitar la paralización parcial o total de las organizaciones o empresas.

Concluye que para este tipo de instituciones Gubernamentales se debe dar prioridad a la gestión de inversión Tecnológica que permita ofrecer seguridad y las garantías necesarias, y de esta manera preservar la integridad de la información [2].

Elizabeth Magdalena Torres Núñez en el año 2015 realizó el proyecto de investigación "Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato". El autor manifiesta que es importante que la información y centros de procesamiento tengan restringido el acceso, estableciendo lineamientos de seguridad para la información en base a la norma International Organization for Standardization (ISO) 27002, que ayuda a protegerla, debido a que las políticas de seguridad disminuyen el riesgo de pérdida de información, de esta manera se asegura el correcto funcionamiento de los procesos [3].

La parte operativa de toda institución pública o privada hoy en día depende esencialmente del nivel tecnológico que esta tenga. La utilización de la Informática en las empresas es vital para el manejo de la información, pues en los actuales momentos sin el uso de las mismas no se puede realizar ningún proceso o mantener un negocio, inclusive la Informática ha traspasado sus límites y al integrarse al Internet los procesos se vuelven más dinámicos sin embargo los procedimientos de seguridad en muchas ocasiones no se toman en cuentas por no existir políticas de seguridad [4].

Según los datos del ESET Security Report en el año del 2019, revela que la mayor preocupación de las empresas está asociada a la explotación de vulnerabilidades y el impacto que esta podría tener en su operatoria. De hecho, este año, el 58 % de las empresas la nombró como su mayor preocupación. Al comparar este porcentaje con los incidentes de seguridad que efectivamente se concretaron asociados a la explotación de vulnerabilidades, se encontró que con tan solo una de cada diez empresas sufrió de la explotación de una vulnerabilidad durante el último año [5].

En Ecuador la empresa de seguridad informática vpnMentor el 6 de septiembre del 2019 reveló que datos de 17 millones de ecuatorianos fueron expuestos en línea aparentemente por la empresa Novaestrat, causando la filtración de información confidencial que contiene datos personales y financieros de millones de ciudadanos de Ecuador [6].

1.2.2. Delimitación

Línea de investigación: Seguridad de Unidades Informáticas.
Sublínea de investigación: Normas y Estándares.

Delimitación Espacial:

El proyecto de investigación se realizará en la empresa Textiles Jhonatex de la ciudad de Ambato, por lo que la delimitación espacial del proyecto es a nivel Cantonal.

Delimitación Temporal:

El proyecto de investigación se desarrollará durante los 6 meses posteriores a la aprobación del proyecto por parte del organismo pertinente de la facultad del periodo abril – septiembre 2020.

1.2.3. Justificación

Actualmente el aumento de los delitos informáticos en el país permite tener una percepción de las amenazas a los que están propensos los sistemas de procesamiento de información y con ello los datos se ven expuestos a daños irreparables que pueden causar un gran impacto en la empresa.

Textiles Jhonatex al igual que las demás empresas manejan a diario información que le genera valor al negocio, la cual tiene diferente nivel de importancia para cada área, pues lo que puede ser importante o confidencial para un área para otra puede no ser tan relevante, por esa razón antes de implementar controles de seguridad se debe analizar y considerar la situación actual en cuánto a la seguridad de la información, de tal forma que se pueden mitigar vulnerabilidades y amenazas a las cuales puede estar propenso la empresa.

Por tal motivo se requiere el uso de estándares que se encuentren alineados a las mejores prácticas y permitan brindar una propuesta de calidad. Tomando en cuenta las características de la empresa Textiles Jhonatex, se ha seleccionado las metodologías NIST SP 800-30 y NIST 800-115 ya que son aplicables a cualquier empresa categorizada en el rubro de PYME (Pequeñas y Medianas Empresas). De acuerdo a la NIST SP 800-30, es necesario atravesar por nueve fases ya que de esta manera permitirá identificar, analizar y proponer controles de Tecnologías de la Información (TI) para mantener niveles de riesgos óptimos para la organización. En relación a la NIST SP 800-115, que se encuentra conformada por técnicas de evaluación de vulnerabilidades y recomendaciones que permiten lograr una integración absoluta con la metodología NIST SP 800-30. Al aplicar las dos metodologías se logrará óptimos resultados con el trabajo de investigación propuesto.

1.3. Fundamentación teórica

A continuación, se describe los conceptos que se utilizaran para el desarrollo de la investigación propuesta, teniendo como objetivo indicar un procedimiento coordinado y coherente de conceptos, aportando de esta manera una forma clara a la interpretación de los resultados de la investigación.

1.3.1. Sistema de gestión de seguridad de la información

.Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información, ayudando a monitorear, verificar, sostener, y aumentar la seguridad de la información de una empresa [7].

1.3.2. Seguridad de la Información

La Seguridad de la Información se enfoca en los riesgos, amenazas, análisis de escenarios, acerca de las buenas prácticas y esquemas normativos, que requiere niveles de aseguramiento de procesos y tecnologías para aumentar el nivel de confianza en la creación, manejo, almacenamiento, comunicación, restauración de la información [8].

1.3.3. Seguridad Informática

Se encarga de poner en funcionamiento técnicas que ayudan a la protección de la información, como son antivirus, firewalls, detección de intrusos, relación de eventos, atención de percances, entre otros elementos, que enlazados con prácticas de gobierno de tecnología de información disponen la forma de proceder y asegurar las situaciones de fallas parciales o totales, en el momento que la información que se encuentra en riesgo [8].

Existen diferentes definiciones del término Seguridad Informática. Una de ellas es la definición otorgada por el estándar para la seguridad de la información ISO/IEC 27001 lo define como "La implantación de un conjunto de reglas técnicas destinadas a proteger la confidencialidad, la integridad y la disponibilidad de la información" [9].

1.3.4. Sistema Informático

Es un conjunto de partes que se relacionan entre sí, con el objetivo de funcionar de forma precisa. Sus partes son: hardware, software y las personas que lo utilizan [10]. Para que un sistema se lo pueda definir como seguro debe cumplir con siguientes características, como se lo observa en la tabla 1.1:

Tabla 1.1: Características de un sistema seguro

Características	**Descripción**
Integridad	La información no puede ser modificada por quien no está autorizado.
Confidencialidad	La información solo debe ser legible para los usuarios autorizados.
Disponibilidad	Debe estar disponible cuando se necesita.
Irrefutabilidad	(No-Rechazo o No Repudio) Que no se pueda negar la autoría.
Bugs	Se refiere a una debilidad o defecto o error en un sistema informático, el cual lo hace vulnerable a ataques informáticos (virus, ciberdelincuentes, etc.). También se le conoce como agujeros de seguridad.

Fuente: Elaboración propia a partir de [10]

1.3.5. Manual de Políticas de Seguridad de la Información

Es un documento donde se describe los controles necesarios de seguridad que se encuentran implementados en una empresa, de igual manera define las responsabilidades para cada una de las actividades [11].

1.3.6. Propietario de la información

El término propietario en esta definición no significa ser el dueño de los activos de información, se refiere a la persona o personas responsables de custodiar que se le dé el buen manejo de los activos, y evaluar quien debe obtener acceso a los mismos [11].

1.3.7. Delitos informáticos

Los delitos informáticos es un conjunto de comportamientos criminales que son realizadas por medio de un ordenador electrónico, que perjudica al buen funcionamiento de los sistemas informáticos [12].

1.3.8. Hacker

Es una persona que tiene conocimientos avanzados en el área de la tecnología y los usa para encontrar debilidades en un ordenador o de una red informática, muchas veces lo realizan para obtener fines de lucro [13].

1.3.9. Crackers

Es el conjunto de individuos que utilizan su conocimiento, mediante el uso de herramientas tecnológicas con el objetivo de ingresar ilegalmente a información que es de carácter privado, muchas veces con fines de lucro. Consiguiendo así robar información confidencial de la empresa [13].

1.3.10. Virus Informático

Es un programa, diseñado por uno o varios individuos, en cualquier lenguaje de programación, con el objetivo de causar algún tipo de daño total o parcial al ordenador que lo aloja [14].

1.3.11. Metodología

Se avoca a estudiar los elementos de cada método relacionados con su génesis, fundamentación, articulación ética, razonabilidad; su capacidad explicativa, su utilidad aplicada, los procedimientos de control que utiliza, por ejemplo, en el trabajo empírico y el modo en que se estructura para producir resultados. Si los métodos tienen pasos, reglas y procedimientos para llevar a cabo la manipulación inteligente de la realidad categorizada como problema, la metodología se encamina a su análisis y comprensión, con el fin de verificar sus fortalezas y debilidades [15].

1.3.12. Metodologías de gestión de riesgos

Existen metodologías que permiten hacer un uso adecuado del análisis de riesgos y así asegurar los sistemas de información de las organizaciones. Entre las principales tenemos: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS, NIST SP 800:30. En la tabla 1.2 se hace referencia a las fases que componen cada una de las metodologías mencionadas anteriormente [16].

Tabla 1.2: Fases de las metodologías para el análisis de riesgos

Fases	**Metodologia**							
	1	1A	1B	2	3	4	5	6
Caracterización del sistema	X	X	X	X	X	X	X	X
Identificación de amenazas	X	X	X		X	X	X	X
Identificación de vulnerabilidades	X		X		X			X
Análisis de controles	X	X	X	X		X	X	X
Determinación de la probabilidad								X
Análisis de impacto								X
Determinación del riesgo	X	X	X	X	X			X
Recomendaciones de control	X	X	X	X		X	X	X
Documentación de resultados	X			X				X
Establecimiento de parámetros			X		X			
Necesidades de Seguridad	X					X	X	

Fuente: Elaboración propia a partir de [16]

(1) OCTAVE, (1A) OCTAVE 1, (1B) OCTAVE ALLEGRO, (2) MEHARI, (3) MAGERIT, (4) CRAMM, (5) EBIOS, (6) NIST SP 800 – 30

1.3.13. Metodología NIST SP 800-30

Introducción

La publicación especial 800-30 fue elaborado para proporcionar una guía de evaluaciones de riesgos de los sistemas y organizaciones. Las evaluaciones de riesgos, llevadas a cabo en los tres niveles de la jerarquía de gestión de riesgos, son parte de un proceso general de gestión de riesgos, proporcionando a los líderes un alto nivel la información necesaria para determinar los cursos de acción adecuados en respuesta a los riesgos identificados [17]. En la figura 1.1 se describe los niveles de jerarquía de gestión de riesgo.

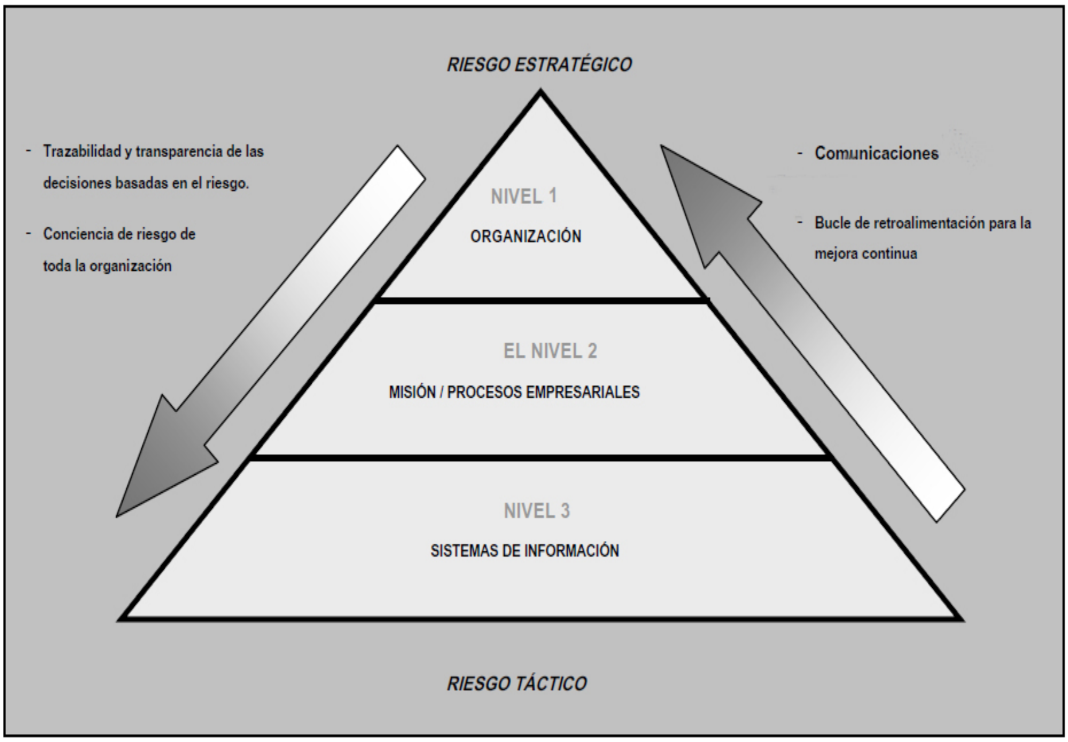


Figura 1.1: Jerarquia de gestión de riesgos
Fuente: [17]

Asimismo, ofrece a las organizaciones una guía de cómo realizar evaluaciones de riesgos a la Seguridad de la Información que incluye:

1. Visión general de alto nivel del proceso de evaluación de riesgos.
2. Actividades necesarias para prepararse para las evaluaciones de riesgos.
3. Actividades necesarias para realizar evaluaciones de riesgos efectivas.
4. Actividades necesarias para comunicar los resultados de la evaluación y compartir información relacionada con el riesgo
5. Actividades necesarias para mantener los resultados de las actividades de riesgos de manera continua.

Este proceso de evaluación de riesgos comprende de cuatro pasos, los cuales son detallados en la figura 1.2.

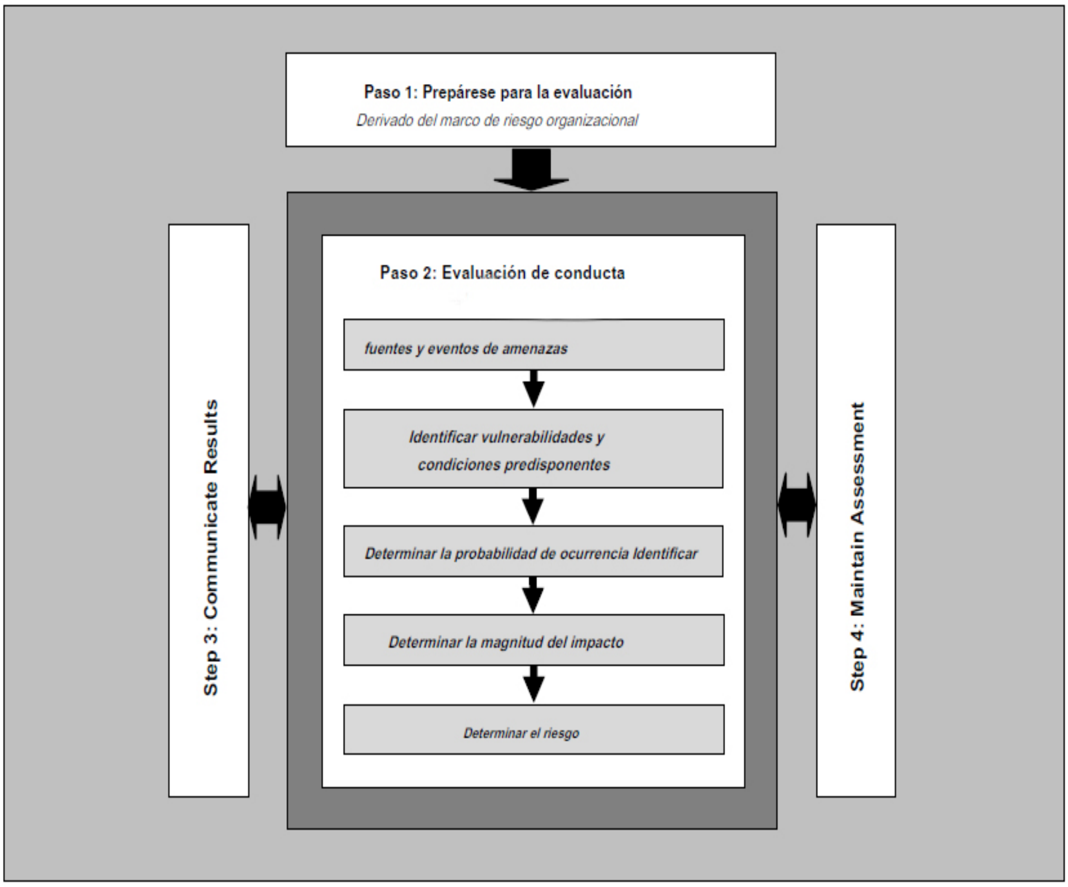


Figura 1.2: Proceso de evaluación de riesgos
Fuente: [17]

Además, ofrece un modelo de riesgo que ayuda a definir los factores de riesgo que deben ser evaluados y que relaciones existen entre esos factores. Los factores de riesgos son características utilizadas en los modelos de riesgo como insumos para determinar los niveles de riesgo en las evaluaciones de riesgos. Los factores de riesgos también se usan ampliamente en las comunicaciones de riesgos para resaltar lo que afecta significativamente los niveles de riesgo en situaciones, circunstancias o contextos particulares. Los factores de riesgos más comunes incluyen amenazas, vulnerabilidades, impacto, probabilidad y condición predisponente. Los factores de riesgo se lo podrían descomponer en características más detalladas: amenazas descompuestas en fuentes de amenazas y eventos de amenazas. Estas definiciones son importantes para que las organizaciones documenten antes de realizar evaluaciones de riesgos porque las evaluaciones se basan en atributos bien definidos de amenazas, vulnerabilidades, impacto y otros factores de riesgo que para determinar el riesgo de manera efectiva [17].

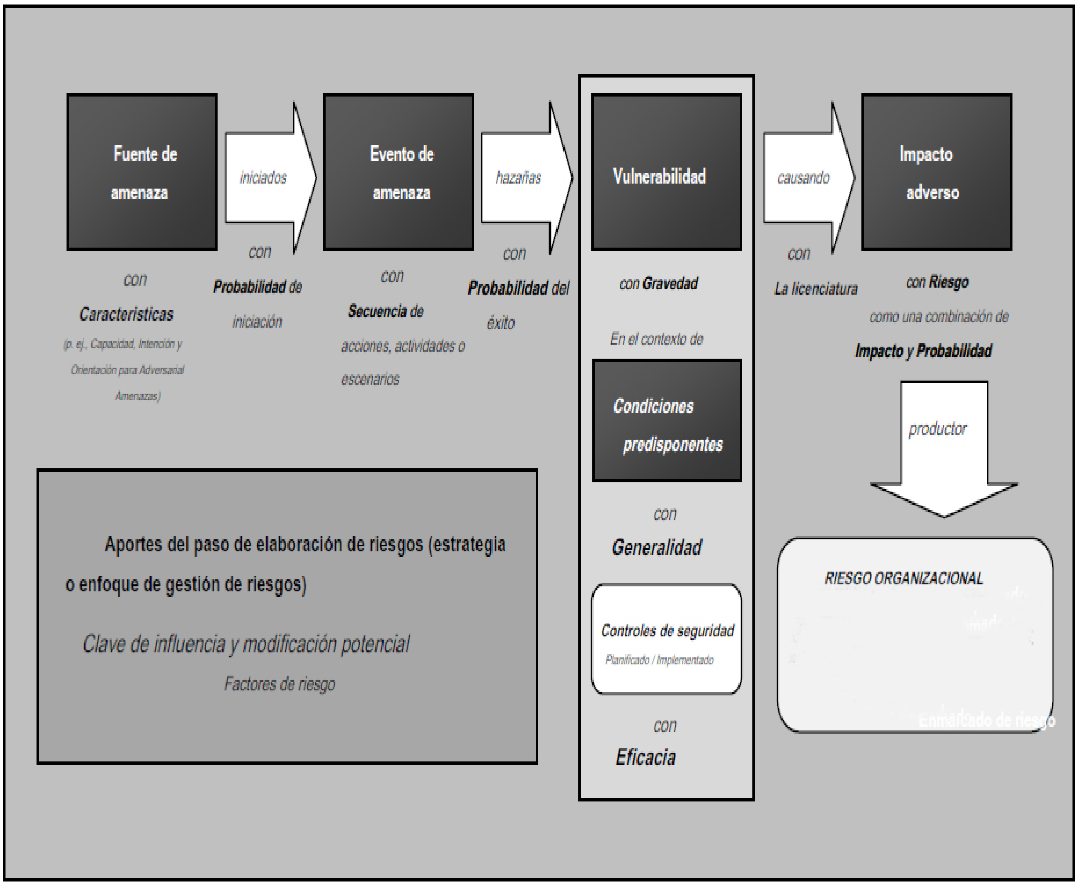


Figura 1.3: Modelo de riesgo genérico con factores de riesgo clave
Fuente: [17]

En la presente figura 1.3, se muestra un modelo genérico de los factores de riesgos que son clave para la elaboración de un plan de gestión de riesgos.

Caracterización del sistema

La primera fase de esta metodología está orientada a especificar los componentes que forman parte de un sistema de información, se lo caracteriza por:

- Hardware.
- Software.
- Sistemas de conectividad interna y externa.
- Datos e información.
- Usuarios del sistema.
- Nivel de criticidad de datos.

Identificación de amenazas

Una amenaza es cualquier circunstancia o evento potencial de impactar negativamente las operaciones de la organización, activos, individuos, a través del acceso no autorizado, destrucción, divulgación, modificación de información o denegación de servicio.

El objetivo de esta fase es identificar las posibles amenazas que puedan desarrollarse sobre los activos informáticos que se evaluarán, para identificar las amenazas de la organización se lo puede realizar a través de históricos de ataques previos, información de agencias o datos de medios de comunicación.

Identificación de vulnerabilidades

Una vulnerabilidad es una debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podrían ser explotados por una fuente de amenaza. La mayor parte de las vulnerabilidades que existen en un sistema se los pueden asociar con controles de seguridad que no se han aplicado (ya sea intencionalmente o no), o se han aplicado, pero conservan cierta debilidad. Sin embargo, es importante mencionar la posibilidad de vulnerabilidades emergentes que pueden surgir naturalmente con el tiempo a medida que evolucionan las misiones organizacionales, cambian los entornos de operación, proliferan las nuevas tecnologías y surgen nuevas amenaza[18]. En el contexto de dicho cambio, los controles de seguridad existentes pueden volverse inadecuados y es posible que sea necesario mantener evaluaciones continuas durante el ciclo de vida de los sistemas.

Las entradas generalmente en esta fase se lo realizan a través de informes de evaluaciones de riesgo anteriores, resultados de auditoria, requerimientos de seguridad y resultados de pruebas de seguridad, con el objetivo de identificar las vulnerabilidades que afectan la probabilidad de que una amenaza presente impactos adversos en la organización.

Tabla 1.3: Plantilla - Identificación de fuentes de amenaza

Identificador	**Fuente de información de evento de amenaza**	**Fuente de amenaza**	**Relevancia**
Definido por la organización	Definido por la organización	Definido por la organización	Definido por la organización

Fuente: Elaboración propia a partir de [17]

En la presente tabla 1.3, **se** muestra una plantilla estándar, la cual puede ser usada para listar las posibles amenazas de la organización evaluada.

Análisis de Control

El objetivo es analizar los controles y procedimientos implementados o planificados por la organización para mitigar la probabilidad de que una amenaza explote una vulnerabilidad del sistema.

Determinación de Probabilidad

En este paso se determina la probabilidad de que los eventos de amenaza, estos presenten impactos negativos, para esto se considera siguientes factores:

- Características de fuentes de amenaza que pueden iniciar los eventos
- Vulnerabilidades identificadas
- Análisis de controles

De esta forma poder calificar a la probabilidad, la cual se determina con tres niveles: alto, medio, bajo.

Tabla 1.4: Definición de niveles de probabilidad

Nivel de probabilidad	**Definición de probabilidad**
Alto	La fuente de amenaza está fuertemente motivada y los controles existentes para prevenir que la vulnerabilidad sea explotada son ineficientes.
Medio	La fuente de amenaza está motivada y los controles implantados pueden prevenir que las vulnerabilidades sean explotadas.
Bajo	La fuente de amenaza carece de motivación o capacidad y los controles actuales pueden impedir de forma significativa la explotación de las vulnerabilidades.

Fuente: Elaboración propia a partir de [17]

En la tabla 1.4**, se** muestra los criterios que se deben tomar para determinar el nivel de probabilidad de la vulnerabilidad identificada.

Análisis de impacto

Este paso está orientado a determinar el impacto de los eventos de amenaza, considerando los siguientes factores.

- Características de fuentes de amenaza que pueden iniciar los eventos
- Vulnerabilidades identificadas
- Análisis de controles

Tabla 1.5: Plantilla - Análisis de impacto

Valores cualitativos	**Descripción**
Alto	Se podría esperar que el evento de amenaza ocasione un severo o catastrófico efecto adverso sobre las operaciones organizacionales, los activos organizacionales, los individuos.
Medio	Se podría esperar que el evento de amenaza tenga un grave efecto adverso en las operaciones organizacionales, activos organizacionales, individuos.
Bajo	Se podría esperar que el evento de amenaza tenga un limitado efecto adverso en las operaciones organizacionales, activos organizacionales, individuos.

Fuente: Elaboración propia a partir de [17]

Como se observa en la tabla 1.5, el nivel de impacto de un evento de amenaza es la magnitud del daño que se puede esperar que resulte de las consecuencias de la divulgación no autorizada de información, la modificación no autorizada de información, la destrucción no autorizada de información o la pérdida de información o la disponibilidad del sistema de información. Tal daño puede ser experimentado por una variedad de partes interesadas en la organización, internas o externas, que incluyen:

- Alta gerencia.
- Propietarios de información.
- Propietarios de procesos de negocio.
- Propietarios de sistemas de información.

Determinación de Riesgo

El objetivo de este paso es valorar el nivel de riesgo de la organización. Para la determinación de los riesgos de toma en cuenta los siguientes puntos:

- Probabilidad de una amenaza.
- Magnitud de impacto.
- Controles planeados y actuales.

Tabla 1.6: Cálculo de riesgo

Probabilidad	**Impacto**		
	Baja (10)	Media (50)	Alta (100)
Alta (1.0)	Baja: 10x1.0 =10	Media: 5x1.0 =50	Alta: 100x1.0 =100
Media (0.5)	Baja: 10x0.15 =5	Media: 5x0.5 =25	Media: 100x0.5 =50
Baja (0.1)	Baja: 10x0.1 =1	Baja: 5x0.1 =5	Baja: 100x0.1 =10

Fuente: Elaboración propia a partir de [17]

En la presente tabla 1.6, se muestra la forma de determinar el nivel de riesgo, para considerarse un riesgo de nivel bajo tiene que estar en el rango de 1 a 20, asimismo de 21 a 79 se le considera al riesgo de nivel medio, por último, de 81 a 100 el riesgo es alto.

Recomendaciones de control

Este paso está orientado a proponer controles necesarios para mitigar el nivel de riesgo inherente, a partir de los riesgos identificados en el paso previo.

Resultado y documentación

Este es el paso final de la metodología la cual está orientada a brindar información esencial que las organizaciones requieren para comunicar de forma eficiente los resultados de una evaluación de riesgos. Los resultados de una evaluación de riesgos sirven de soporte para la toma de decisiones, y brinda un entendimiento global de los riesgos de una seguridad de la información relacionados con los activos, individuos u otras organizaciones [17].

1.3.14. Metodología NIST SP 800-115

Introducción

La publicación especial NIST SP 800-115 es una guía de los aspectos técnicos básicos de la realización de evaluaciones de seguridad de la información. Presenta métodos, técnicas de evaluación, exámenes técnicos que una organización podría usar como parte de una evaluación, ofrece información a los evaluadores sobre su ejecución, el impacto potencial que pueden tener en los sistemas, redes. Para que una evaluación se la considere exitosa y tenga un impacto positivo en la postura de seguridad de un sistema, los elementos más allá de la ejecución de las pruebas, exámenes deben respaldar el proceso técnico. Además, esta guía presenta sugerencias para estas actividades, incluido un proceso de planificación [19]. Se describe a continuación los beneficios, al implementar esta metodología en una organización:

- Desarrollar una política de evaluación de seguridad de la información, metodología, roles y responsabilidades individuales relacionados con los aspectos técnicos de la evaluación.
- Planificar con precisión una evaluación de seguridad de la información técnica al proporcionar orientación sobre cómo determinar que sistemas evaluar y el enfoque para la evaluación, abordar las consideraciones logísticas, desarrollar un plan de evaluación y garantizar que se aborden las consideraciones legales y políticas.
- Ejecutar de manera segura y efectiva una evaluación de seguridad de la información técnica, utilizando los métodos y técnicas presentados, y responda a cualquier incidente que pueda ocurrir durante la evaluación.
- Realizar análisis e informes para traducir los hallazgos técnicos en acciones de mitigación de que mejorarán la postura de seguridad de la organización.

Técnicas de revisión

- Revisión de documentación

La revisión de la documentación determina si los aspectos técnicos de las políticas y los procedimientos son actuales y completos. Estos documentos proporcionan la base para la postura de seguridad de una organización, pero a menudo se pasan por alto durante las evaluaciones técnicas. Los grupos de seguridad dentro de la organización deben proporcionar a los evaluadores la documentación adecuada para garantizar una revisión exhaustiva. Los documentos para revisar en cuanto a precisión técnica e integridad incluyen políticas de seguridad, arquitecturas y requisitos, procedimientos de operación estandarizados, planes de seguridad del sistema y acuerdos de autorización; acuerdo de interconexiones del sistema y planes de respuesta a incidentes.

La revisión de la documentación puede descubrir brechas y debilidades que podrían conducir a controles de seguridad faltantes o implementados incorrectamente. Las debilidades comunes de la documentación incluyen los procedimientos o protocolos de seguridad del sistema operativo que ya no se usan, y la falta de incluir un nuevo sistema operativo y sus protocolos. La revisión de la documentación no garantiza que los controles de seguridad se implementen correctamente, solo que la dirección y la orientación existen para soportar la infraestructura de seguridad [19].

- Revisión de registros

La revisión de registros determina si los controles de seguridad registran la información adecuada, y si la organización cumple con sus políticas de administración de registros. Como fuente de información histórica, los registros de auditoría se pueden usar para ayudar a validar que el sistema funciona de acuerdo con las políticas establecidas. De igual forma, si la política de registro establece que todos los intentos de autenticación en servidores críticos deben registrarse, la revisión del registro determinará si se está recopilando esta información y muestra el nivel de detalle apropiado [19]. La revisión de registros también puede revelar problemas tales como servicios mal configurados y controles de seguridad, accesos no autorizados e intentos de intrusiones. A continuación, se presenta una lista de ejemplos de información de registro que pueden ser útiles al realizar evaluaciones de seguridad en las organizaciones:

- El servidor de autenticación o los registros del sistema pueden incluir intentos de autenticación exitosos y fallidos. Los registros del sistema pueden incluir información de inicio y apagado del sistema y del servicio, instalación de software no autorizado, acceso a archivos, cambios en la política de seguridad, cambios en la cuenta (por ejemplo, creación y eliminación de cuentas, asignación de privilegios de cuenta) y uso de privilegios.

- Los registros del sistema de detección y prevención de intrusiones pueden incluir actividad maliciosa y uso inapropiado.

- Los registros de firewall y enrutador pueden incluir conexiones salientes que indican dispositivos internos comprometidos (p. Ej., Rootkits, bots, troyanos, spyware).

- Los registros de firewall pueden incluir intentos de conexión no autorizados y uso inapropiado. Los registros de aplicaciones pueden incluir intentos de conexión no autorizados, cambios de cuenta, uso de privilegios e información de uso de aplicaciones o bases de datos.

- Los registros de antivirus pueden incluir fallas de actualización y otras indicaciones de firmas y software obsoletos.

- Revisión del conjunto de reglas

Un conjunto de reglas es una colección de reglas o firmas con las que se compara el tráfico de red o la actividad del sistema, para determinar qué acción tomar. La revisión de estos conjuntos de reglas se realiza para garantizar un alto nivel de comprensión e identificar brechas y debilidades en los dispositivos de seguridad y en todas las defensas en capas, tales como vulnerabilidades de red, violaciones de políticas y rutas de comunicación no intencionadas o vulnerables. Una revisión también puede descubrir ineficiencias que afectan negativamente el rendimiento de un conjunto de reglas en la organización [19].

- Revisión de la configuración del sistema

La revisión de la configuración del sistema es el proceso de identificar vulnerabilidades en los controles de configuración de seguridad, tales como sistemas que no se fortalezcan o configuren de acuerdo con las políticas de seguridad. Por ejemplo, este tipo de revisión revelará servicios y aplicaciones innecesarios, configuraciones de cuenta y contraseña de usuario inadecuadas, y configuraciones incorrectas de registro y respaldo.

Los evaluadores que utilizan técnicas de revisión manual se basan en guías de configuración de seguridad o listas de verificación, que les ayuda a asegurar que la configuración del sistema esté configurada para minimizar los riesgos de seguridad. Para realizar una revisión manual de la configuración del sistema, los evaluadores acceden a varias configuraciones de seguridad en el dispositivo que se está evaluando y las comparan con las configuraciones recomendadas de la lista de verificación. Las configuraciones que no cumplen con los estándares mínimos de seguridad se marcan e informan [19].

- Detección de redes

La detección de redes es una técnica pasiva que monitorea la comunicación de red, decodifica protocolos, y examina las cabeceras de los paquetes para obtener información de interés. Además de ser utilizado como una técnica de revisión, la detección de redes también se puede utilizar como una técnica de identificación y análisis de objetivos. Las razones para usar el rastreo de red incluyen las siguientes:

- Captura y reproducción de tráfico de red.
- Realización de descubrimiento de red pasiva.
- Identificación de sistemas operativos, aplicaciones, servicios y protocolos, incluidos protocolos no seguros.
- Identificar actividades no autorizadas e inapropiadas, como la transmisión no cifrada de información confidencial.
- Recolección de información, tales como usuarios y contraseñas no encriptados.

La detección de redes tiene poco impacto en los sistemas y redes, con el impacto más notable en el ancho de banda o la utilización de la potencia informática. El sniffer, la herramienta utilizada para realizar el sniffing de la red, requiere un medio para conectarse a la red, como un hub, tap o switch con expansión de puertos. La expansión de puertos es el proceso de copiar el tráfico transmitido en todos los demás puertos al puerto donde está instalado el sniffer. Las organizaciones pueden implementar rastreadores de red en varias ubicaciones dentro de un entorno [19]. Estos comúnmente incluyen lo siguiente:

- En el perímetro, para evaluar el tráfico que ingresa y sale de la red.
- Detrás de los firewalls, para evaluar que los conjuntos de reglas filtran con precisión el tráfico.
- Detrás de IDS / IPS, para determinar si las firmas se activan y se responden de manera adecuada frente a un sistema crítico o aplicación para evaluar la actividad.
- En un segmento de red específico, para validar protocolos cifrados.

- Verificación de integridad de archivos

Los verificadores de integridad de archivos proporcionan una forma de identificar que los archivos del sistema han sido modificados y almacenan registros de auditoría para cada archivo, y estableciendo una base de datos como repositorio de estos cambios. Posteriormente, el registro de cambios almacenados es procesado para comparar el valor actual con el valor almacenado, de modo que se identifica las modificaciones realizadas al archivo analizado. Por lo general, se incluye una capacidad de verificación de integridad de archivos con cualquier IDS basado en host, y también está disponible como una utilidad independiente [19].

Aunque un verificador de integridad no requiere un alto grado de interacción humana, debe usarse con cuidado para garantizar su efectividad. La verificación de integridad de archivos es más efectiva cuando los archivos del sistema se comparan con una base de datos de referencia creada usando un sistema que se sabe que es seguro; esto ayuda a garantizar que la base de datos de referencia no se haya creado con archivos comprometidos. La base de datos de referencia debe almacenarse fuera de línea para evitar que los atacantes comprometan el sistema y cubran sus huellas modificando la base de datos. Además, debido a que los parches y otras actualizaciones cambian los archivos, la base de datos de registros debe mantenerse actualizada.

Técnicas de identificación y análisis de objetivos

- Descubrimiento de red

El descubrimiento de la red utiliza varios métodos para descubrir hosts activos y que responden en una red, identificar debilidades y aprender cómo funciona la red. Existen técnicas pasivas (examen) y activas (prueba) para descubrir dispositivos en una red. Las técnicas pasivas utilizan un sniffer de red para monitorear el tráfico de red y registrar las direcciones IP de los hosts activos, y pueden informar qué puertos están en uso y qué sistemas operativos se han descubierto en la red. El descubrimiento pasivo también puede identificar las relaciones entre los hosts, incluido qué hosts se comunican entre sí, con qué frecuencia se produce su comunicación y el tipo de tráfico que se está llevando a cabo, y generalmente se realiza desde un host en la red interna donde puede monitorear el host [19].

- Identificación del puerto de red y servicio

La identificación de puertos y servicios de red implica el uso de un escáner de puertos para identificar puertos y servicios de red que operan en hosts activos, como FTP y HTTP, entre otros, y la aplicación que ejecuta cada servicio identificado, como Microsoft Internet Information Server (IIS) o Apache para Servicio HTTP, entre otros. Las organizaciones deben llevar a cabo la identificación del puerto de red y el servicio para identificar hosts si esto no se ha hecho ya por otros medios (descubrimiento de red) y marcar servicios potencialmente vulnerables. Esta información puede usarse para determinar objetivos para pruebas de penetración [19].

- Escaneo de vulnerabilidades

Al igual que la identificación de puertos y servicios, el escaneo de vulnerabilidades identifica hosts y atributos de host (sistemas operativos, aplicaciones, puertos abiertos), pero también intenta identificar vulnerabilidades en lugar de depender de la interpretación humana de los resultados del escaneo. Muchas herramientas para escanear vulnerabilidades están equipados para aceptar resultados de descubrimiento de redes e identificación de puertos y servicios de red, lo que reduce la cantidad de trabajo necesario para el escaneo de vulnerabilidades. Además, algunos escáneres pueden realizar su propio descubrimiento de red e identificación de puerto y servicio de red. El análisis de vulnerabilidades puede ayudar a identificar versiones de software desactualizadas, parches faltantes y configuraciones incorrectas, y validar el cumplimiento o las desviaciones de la política de seguridad de una organización. Esto se hace identificando los sistemas operativos y las principales aplicaciones de software que se ejecutan en los hosts y relacionándolos con información sobre vulnerabilidades conocidas almacenadas en las bases de datos de vulnerabilidades de los escáneres [19]. Los escáneres de vulnerabilidad pueden:

- Verificar el cumplimiento del uso de la aplicación host y las políticas de seguridad.
- Brindar información sobre los objetivos para las pruebas de penetración.
- Brindar información sobre cómo mitigar las vulnerabilidades descubiertas.

Técnicas de validación de vulnerabilidad objetivo

Utilizan información producida a partir de la identificación y el análisis del objetivo para explorar más a fondo la existencia de vulnerabilidades potenciales. El objetivo es demostrar que existe una vulnerabilidad y demostrar las exposiciones de seguridad que ocurren cuando se explota. La validación de vulnerabilidad objetivo implica la mayor cantidad de riesgo en las evaluaciones, ya que estas técnicas tienen más potencial para impactar el sistema o la red objetivo que otras técnicas.

- Descifrado de contraseñas

Cuando un usuario ingresa una contraseña, se genera un hash de la contraseña ingresada y se compara con un hash almacenado de la contraseña real del usuario. Si los hashes coinciden, el usuario se autentica. El descifrado de contraseñas es el proceso de recuperar contraseñas de hashes de contraseñas almacenadas en un sistema informático o transmitidas a través de redes. Por lo general, se realiza durante las evaluaciones para identificar cuentas con contraseñas débiles. El descifrado de contraseñas se realiza en hashes que son interceptados por un sniffer de red mientras se transmiten a través de una red o se recuperan del sistema de destino, que generalmente requiere acceso de nivel administrativo o acceso físico al sistema de destino. Una vez que se obtienen estos valores hash, un descifrador automático de contraseñas genera rápidamente valores hash adicionales hasta que se encuentra una coincidencia o el evaluador detiene el intento de descifrado [19].

- Pruebas de penetración

Las pruebas de penetración son pruebas de seguridad en las que los evaluadores imitan los ataques del mundo real para identificar métodos para eludir las características de seguridad de una aplicación, sistema o red. A menudo implica lanzar ataques reales contra sistemas y datos reales que utilizan herramientas y técnicas comúnmente utilizadas por los atacantes. La mayoría de las pruebas de penetración implican la búsqueda de combinaciones de vulnerabilidades en uno o más sistemas que pueden usarse para obtener más acceso del que podría lograrse a través de una sola vulnerabilidad. Las pruebas de penetración también pueden ser útiles para determinar:

- Qué tan bien tolera el sistema los patrones de ataque de estilo real.
- El nivel probable de sofisticación que un atacante necesita para comprometer con éxito el sistema.
- Contramedidas adicionales que podrían mitigar las amenazas contra la capacidad de los defensores del sistema para detectar ataques y responder adecuadamente.

Las pruebas de penetración pueden ser invaluables, pero requieren mucha mano de obra y requieren una gran experiencia para minimizar el riesgo para los sistemas específicos, a pesar de que la organización se beneficia al saber cómo un intruso podría ocasionar, que un sistema dejará de funcionar. Aunque los evaluadores de penetración experimentados pueden mitigar este riesgo, nunca se puede eliminar por completo. Las pruebas de penetración deben realizarse solo después de una cuidadosa consideración, notificación y planificación [19].

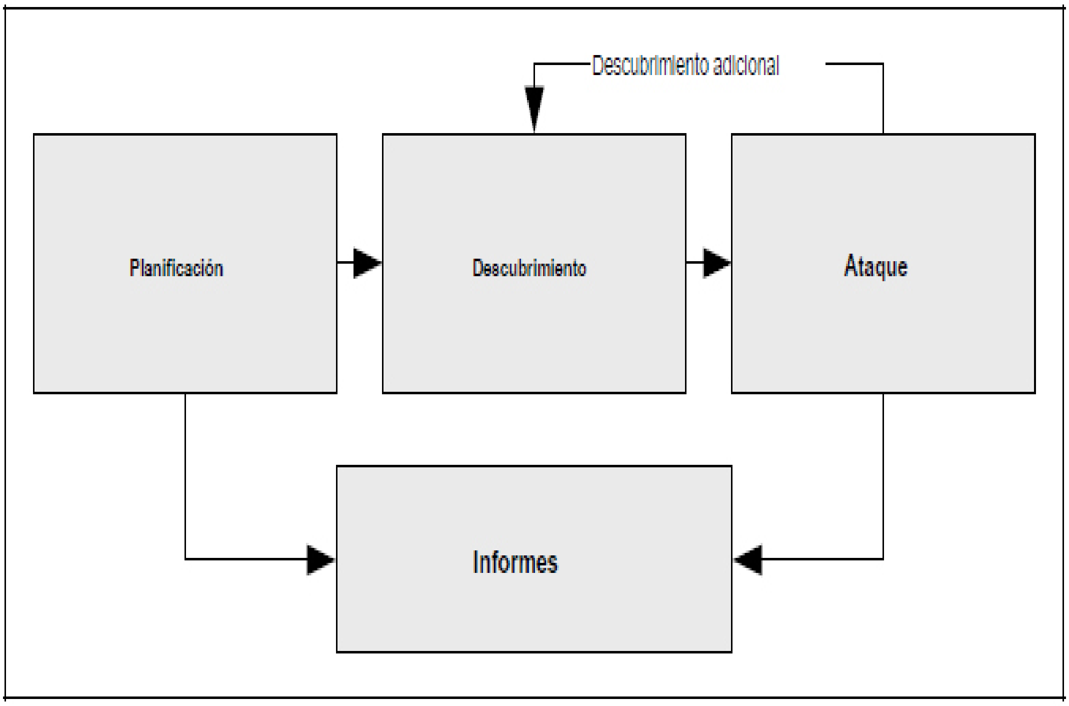


Figura 1.4: Metodología de prueba de penetración
Fuente: [19]

- Ingeniería social

La ingeniería social es un intento de engañar a alguien para que revele información que pueda usarse para atacar sistemas o redes. Se utiliza para probar el elemento humano y la conciencia del usuario sobre la seguridad, y puede revelar debilidades en el comportamiento del usuario, como no seguir los procedimientos estándar. La ingeniería social se puede realizar a través de muchos medios, incluidos los analógicos (conversaciones realizadas en persona o por teléfono) y digitales (correo electrónico, mensajería instantánea). Una forma de ingeniería social digital se conoce como suplantación de identidad, donde los atacantes intentan robar información como números de tarjetas de crédito, números de seguro social, identificaciones de usuario y contraseñas. El phishing utiliza correos electrónicos de aspecto auténtico para solicitar información o dirigir a los usuarios a un sitio web falso para recopilar información. Otros ejemplos de ingeniería social digital incluyen la elaboración de correos electrónicos fraudulentos y el envío de archivos adjuntos que podrían imitar la actividad de gusanos [19].

1.4. Objetivos

Objetivo General

- Analizar la seguridad de la información aplicando las metodologías NIST SP 800-30 y NIST SP 800-115 para la empresa Textiles Jhonatex.

Objetivos Específicos

- Conocer la situación actual referente a la Seguridad de la Información dentro de la empresa.
- Determinar los elementos necesarios de la metodología NIST SP 800-30 para la aplicación en la empresa Textiles Jhonatex.
- Proponer un proceso de Gestión de Vulnerabilidades basado en el estándar de Seguridad NIST SP 800-115.

CAPÍTULO II

METODOLOGÍA

2.1. Materiales

2.1.1. Humanos

- Docente tutor de Tesis de la Universidad Técnica de Ambato.
- Departamento de sistemas.
- Departamento administrativo.
- Investigador.

2.1.2. Institucionales

- La empresa Textiles Jhonatex.
- Biblioteca Virtual de la Universidad Técnica de Ambato.
- Acceso a internet.

2.1.3. Otros

No.	Detalle	Unidad	Cantidad	Valor Unitario	Valor Total
1	Internet	Horas	200	0,80	160,00
2	Resma de papel	c/u	2	5,00	10,00
3	Anillados	c/u	2	5,00	10,00
4	Carpetas	c/u	2	0,35	0,70
5	Impresiones	c/u	500	0,02	10,00
6	Lápiz	c/u	1	0,40	0,40
7	Esfero	c/u	1	0,40	0,40
8	Laptop	c/u	1	900,00	900,00
9	Copias	c/u	500	0,02	10,00
10	Transporte	c/u	100	0,30	30,00
				Sumatoria Parcial	1121,50
				Imprevisto (10 %)	127,15
				Total	1248,65

2.2. Métodología

2.2.1. Modalidad de la Investigación

Investigación Bibliográfica

La investigación será bibliográfica debido a que se tomará como apoyo a la investigación el uso de libros, documentos técnicos, tesis del área informática, revistas, artículos y leyes existentes.

Investigación de Campo

La investigación será también de campo debido a que se buscará obtener información correspondiente a los procesos y mecanismos de gestión a la seguridad de la empresa con el personal involucrado en el tema.

Investigación Descriptiva

La investigación será descriptiva porque se realizará un análisis para llegar a determinar las inseguridades que existe en la empresa.

2.2.2. Población y muestra

2.2.2.1. Población

Esta investigación está dirigida al Gerente General, y a los departamentos como son: Sistemas, Administración, Cobros, Compras, Producción, y Sistema de gestión de seguridad y salud en el trabajo (SST) de la empresa Textiles Jhonatex.

Tabla 2.1: Poblaciones

Población	**Frecuencia**	**Porcentaje**
Departamento de sistemas	1	7,14
Gerente	1	7,14
Administrativos	3	21,43
Ventas	2	14,29
Cobros	2	14,29
Compras	1	7,14
Producción	3	21,43
SST	1	7,14
Total	14	100,00

Fuente: Elaboración Propia

2.2.2.2. Muestra

En virtud de que ninguna de la población a ser investigadas pasa de cien elementos se trabajará con la totalidad del universo sin que sea necesario sacar muestras representativas.

2.2.3. Recolección de información

Para desarrollar el análisis de seguridad de la información se utilizará los siguientes mecanismos de recolección de información.

- Encuestas.
- Entrevistas.
- Observación.
- Revisión de documentos.

Para la elaboración de las encuestas se usará Google Form, debido a que permite recopilar información de manera fácil y eficiente, además la interfaz es muy intuitiva lo cual es fácil de manejar. Cualquier usuario con conocimiento promedio de la computación puede crear formularios y desplegarlo.

2.2.4. Procesamiento y Análisis de Datos

Se podrá utilizar el siguiente criterio:

- Levantamiento de información.
- Clasificación de la información.
- Análisis de la información.

El proceso de los datos obtenidos se lo realizará con Excel que es una herramienta ofimática de Microsoft, lo cual permitirá clasificar los datos más relevantes que se usarán en el proyecto de investigación.

2.2.5. Planificación de entrevistas y encuestas

Con la finalidad de alcanzar resultados reales de la situación actual de la empresa referente a la Seguridad de Información, se realizó 2 entrevistas, una al Gerente propietario y la otra al Jefe de Sistemas, cabe recalcar que la empresa tiene solo un Ingeniero en Sistemas, asimismo se realizó 11 encuestas al persona dentro de las diferentes áreas las cuales son: Administración, Ventas, Compras, Cobros, Producción, SST las entrevistas y encuestas se las realizó en 2 semanas debido al difícil acceso a la empresa por la situación actual que vive el planeta.

Cabe señalar que se considera de vital importancia el criterio de la persona entrevistada, debido a que posee el nivel de conocimiento de la forma en cómo se maneja la Seguridad de la Información, de igual manera las encuestas proveerán una mejor visión en la forma de la organización trata el tema anteriormente mencionado.

2.2.6. Análisis e interpretación de la información obtenida mediante encuestas y entrevistas

Información obtenida en las encuestas

Conforme al plan de recolección de información mediante el uso de encuestas. Se obtuvo los siguientes resultados, de esta manera se refleja el nivel de gestión de seguridad de la información en las diferentes áreas ajenas al área de sistemas.

A continuación, se describe las preguntas que se utilizaron en la encuesta.

Pregunta 1

¿Conoce de qué se trata el tema de seguridad de la información?

Tabla 2.2: Valoración sobre el conocimiento en el tema de seguridad de la información

Detalle	Frecuencia	Porcentaje
Si	8	72,72
No	1	9,09
Desconoce	2	18,18

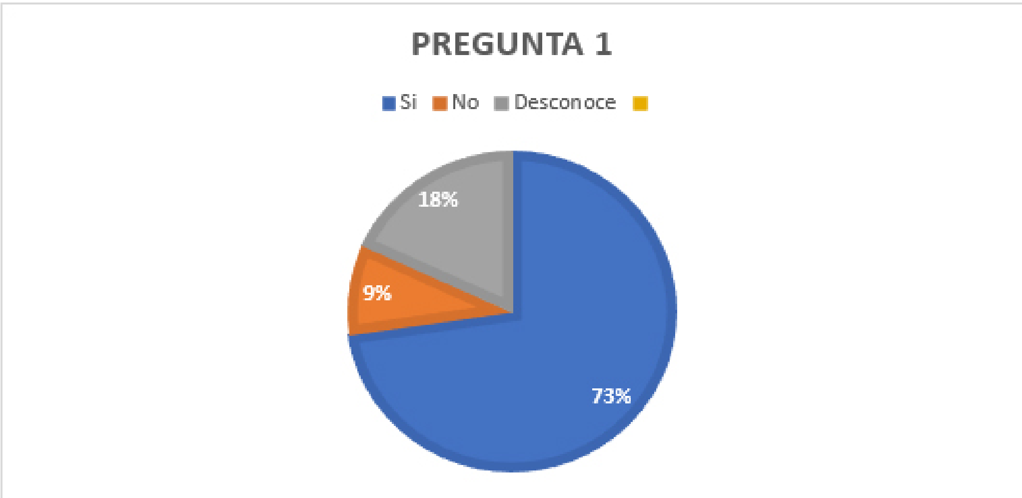


Figura 2.1: Respuestas obtenidas de los empleados acerca del tema de seguridad de la información.
Fuente: Elaboración propia

Análisis e interpretación

El 79 % de los empleados conocen acerca del tema de Seguridad de la Información, el 14 % desconoce acerca del tema, mientras el 7 % dice no conocer acerca del tema.

Existe un porcentaje de menor de la mitad de los empleados, que no saben o desconocen sobre el tema de seguridad de la información, lo que se traduce en una falencia en la empresa, debido a que es un punto vulnerable que podría ser explotado, ya sea externa o internamente.

Pregunta 2

¿Conoce si en la empresa hay un área o persona encargada de la seguridad de la información?

Tabla 2.3: Valoración sobre la existencia del responsable de la seguridad de la información

Detalle	**Frecuencia**	**Porcentaje**
Si	8	72,72
No	0	0
Desconoce	3	27,27

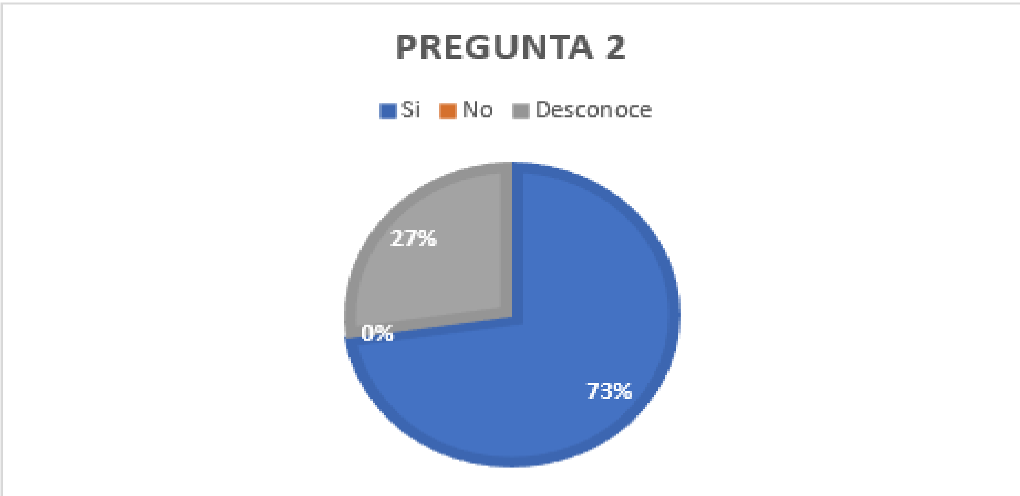


Figura 2.2: Respuestas obtenidas de los empleados sobre la existencia de un responsable de seguridad de la información.
Fuente: Elaboración propia

Análisis e interpretación

El 73 % de los empleados conocen acerca de la existencia de un encargado o área de la seguridad de la información mientras que el 27 % desconoce la existencia de un responsable o área.

Lo que se logra apreciar es que existe una figura responsable de la seguridad de la información de forma parcial debido a que no está establecido correctamente sus funciones.

Pregunta 3

¿Cuál área considera que debe ser responsable de la seguridad de la información?

Tabla 2.4: Valoración de pertenencia de responsabilidad sobre la seguridad de la información

Detalle	**Frecuencia**	**Porcentaje**
Sistemas	8	72,72
Administración	2	18,18
Todas las áreas	3	27,27
Otras	0	0

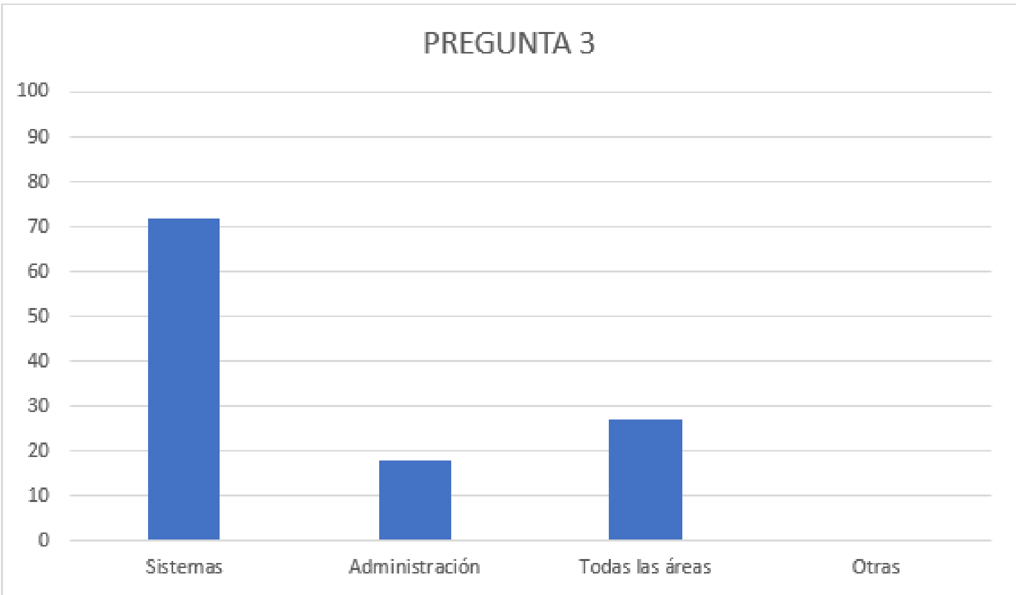


Figura 2.3: Respuestas obtenidas de los empleados acerca de quien consideran como responsable de la seguridad de la información.
Fuente: Elaboración Propia

Análisis e interpretación

Más del 70 % de los empleados sugieren que el área de Sistemas debería ser el encargado de la Seguridad de la Información, mientras que un 15 % indico que la Administración debería ser la encargada de la Seguridad de la Información y el 23 % señalo además que todas las áreas deberían hacerse cargo en la gestión de la Seguridad de la Información.

Se puede entender, que la mayoría de los empleados conocen que el área de sistemas realiza ciertas actividades referentes la seguridad de la información, sin embargo algunos no conocen que área es responsable.

Pregunta 4

¿Cuántas capacitaciones ha recibido acerca de seguridad de la información en el último año?

Tabla 2.5: Capacitaciones recibidas a los empleados sobre temas de seguridad de la información

Detalle	**Frecuencia**	**Porcentaje**
Más de 5	0	0
Menos de 5	3	72,72
Nunca ha recibido	8	27,27

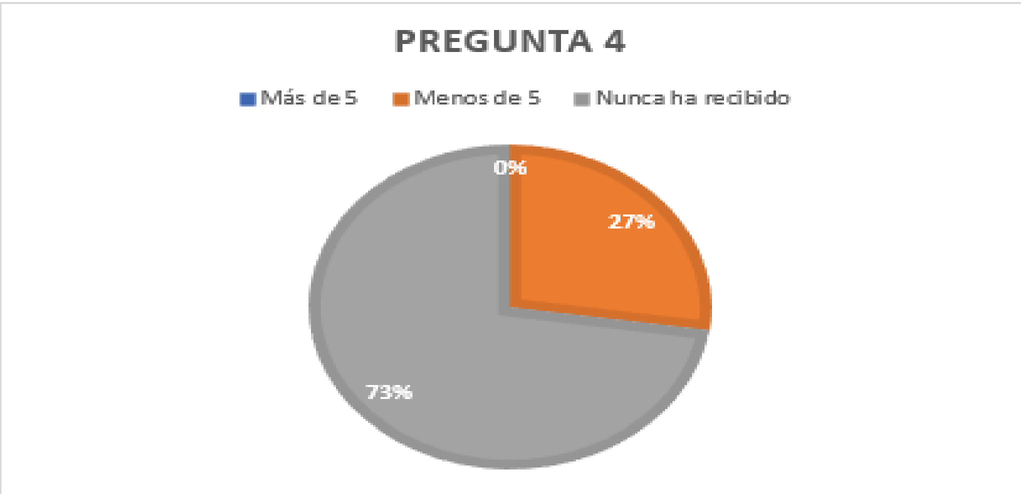


Figura 2.4: Respuestas obtenidas de los empleados referente a las capacitaciones recibidas en temas relacionados con la seguridad de la información.
Fuente: Elaboración propia

Análisis e interpretación

El 73 % de los empleados mencionan no haber recibido capacitaciones y el 27' % señalan haber recibido al menos una capacitación referente al tema de Seguridad de la Información.

Lo que se logra apreciar, es que existe una grave falencia con respecto a capacitaciones a los empleados sobre el tema de seguridad de la información, lo cual podría provocar incidentes de seguridad.

Pregunta 5

¿Las contraseñas que usa tiene combinación de números, letras y es de más de 10 caracteres?

Tabla 2.6: Seguridad en las contraseñas usadas por los empleados

Detalle	Frecuencia	Porcentaje
Solo números y más de 10 caracteres	1	9,09
Solo letras más de 10 caracteres	1	9,09
Números y letras, más de 10 caracteres	5	45,45
Otras	4	36,36

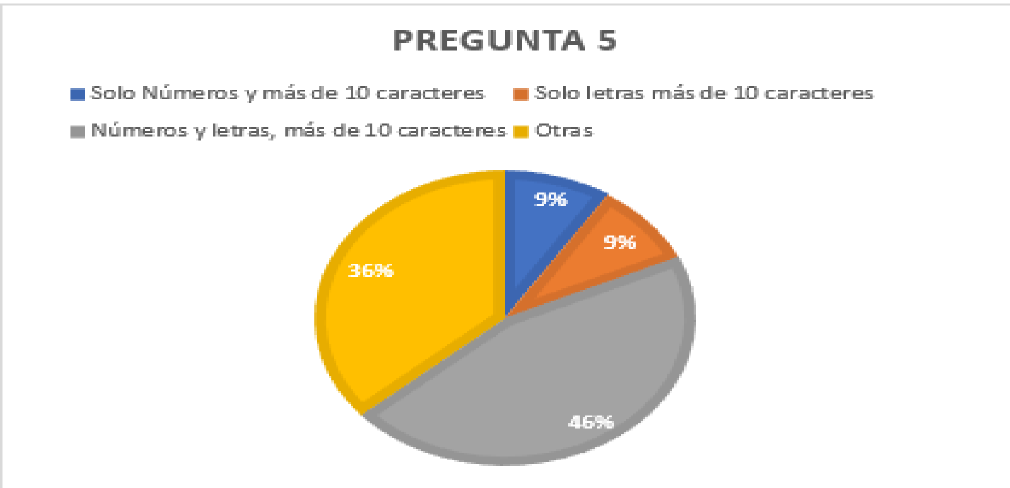


Figura 2.5: Respuestas obtenidas por los empleados referente a las contraseñas utilizadas en los sistemas de procesamiento de la información.
Fuente: Elaboración propia

Análisis e interpretación

El 9 % de los empleados opta por utilizar letras o números y más de 10 caracteres, el 46 % optan por una combinación de números y letras con más de 10 caracteres, mientras que el 36 % utiliza una contraseña con longitud variable la cual puede contener letras, números o solo letras.

Lo que se logra apreciar, la gestión llevada a cabo por el área de sistemas sobre la manera en que los empleados se autentifican en los diferentes sistemas de procesamiento de información no lleva un proceso estricto ni homogénea para los mismos.

Pregunta 6

¿Las contraseñas que utiliza las guarda en un medio físico para no olvidarse?

Tabla 2.7: Valoración sobre la gestión de las contraseñas otrogadas por el departamento de sistemas a los empleados

Detalle	Frecuencia	Porcentaje
Si	8	72,72
No	3	27,27

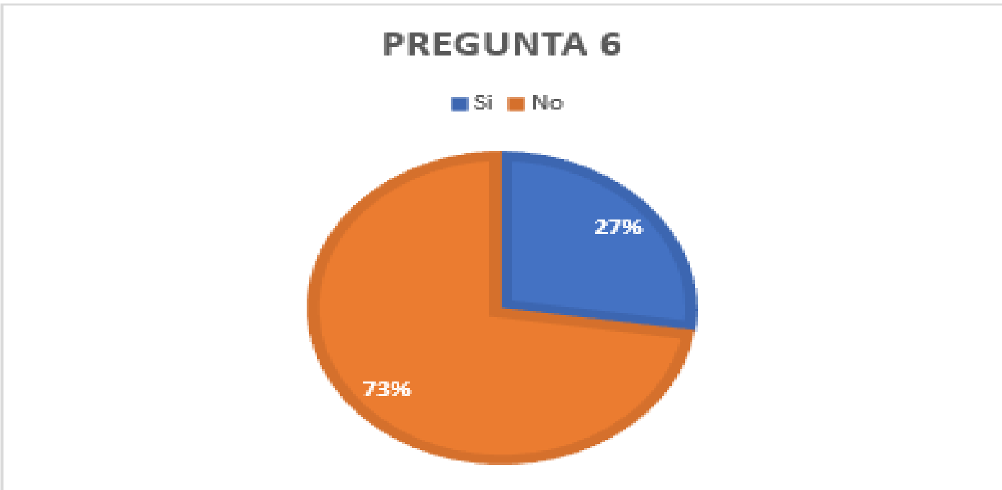


Figura 2.6: Respuestas obtenidas por los empleados respecto a forma en que se autentifican en los sistemas de procesamiento.
Fuente: Elaboración Propia

Análisis e interpretación

El 73 % de los empleados señalan que las contraseñas que manejan para los sistemas de procesamiento no la guardan en algún medio físico, sin embargo, el 27 % señala que si los guarda en un medio físico.

Esto demuestra la carencia de controles de seguridad, debido a que menos de la mitad de los empleados no son conscientes de las consecuencias que presentaría que roben sus credenciales de autentificación.

Pregunta 7

¿Ha ocurrido algún incidente de seguridad en su puesto de trabajo en el último año?

Tabla 2.8: Valoración sobre incidentes de seguridad en el último año

Detalle	Frecuencia	Porcentaje
Si	0	0
No	11	100
Desconoce	0	0

Figura 2.7: Respuestas obtenidas por los empleados referente a incidentes de seguridad reportadas
Fuente: Elaboración propia

Análisis e interpretación

El 100 % de los empleados señalan que no han experimenta algún tipo de incidente de seguridad.

Se logra apreciar, que en su totalidad ninguno de los empleados ha reportado incidentes de seguridad en sus puestos de trabajo.

Pregunta 8

¿Se le bloquea automáticamente su computadora cuando no la está utilizando?

Tabla 2.9: Valoración bloqueo automático de pc

Detalle	Frecuencia	Porcentaje
Si	0	0
No	11	100
Desconoce	0	0

Figura 2.8: Respuestas obtenidas por lo empleados referente al bloqueo automático de sus estaciones de trabajo
Fuente: Elaboración propia

Análisis e interpretación

El 100 % de los empleados señalan que sus estaciones de trabajo no se bloquean automáticamente.

Se da a entender, que existe una grave falencia en la seguridad, puesto que alguien ajeno al equipo de cómputo, puede acceder a información confidencial y manipular la misma.

Pregunta 9

¿Cuándo tiene algún incidente de seguridad (pérdida de información, falla de equipos) a quién lo notifica?

Tabla 2.10: Notificaciones de los empleados a quien consideran responsable de la seguridad

Detalle	Frecuencia	Porcentaje
Sistemas	8	72,72
Jefe Inmediato	6	54,54
Altos Directivos	3	27,27
No notifica	0	0
Otra	0	0

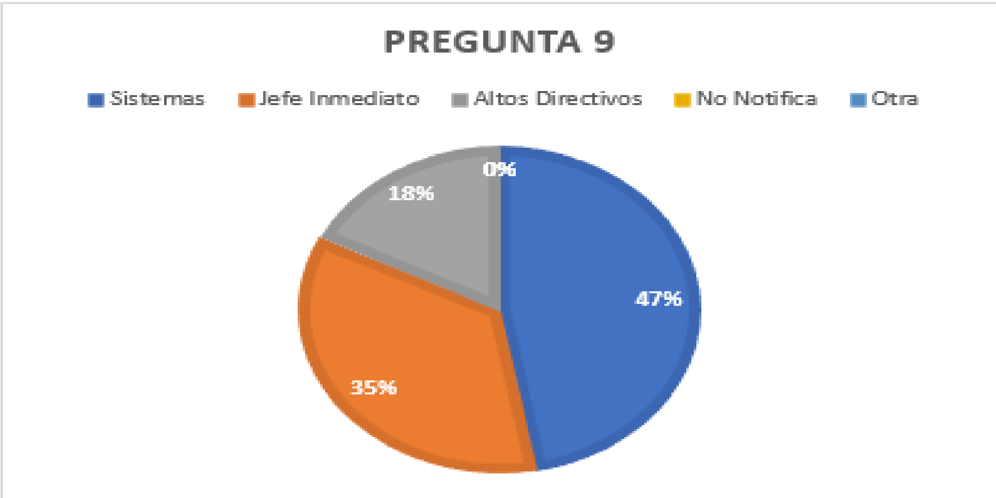


Figura 2.9: Notificaciones de los empleados acerca de incidentes ocurridos en sus estaciones de trabajo y a quien consideran como responsable
Fuente: Elaboración propia

Análisis e interpretación

El 47 % señalo que notifica al área de sistemas, mientras que el 35 % notifica a su Jefe Inmediato y el 18 % señalo que notifica a los Altos directivos.

Lo que se entiende, no existe una determinada figura que sea responsable de la seguridad, al cual los empleados puedan recurrir cuando se presente algún tipo de incidente, para de esta manera obtener una ayuda oportuna.

Pregunta 10

¿Algunos mensajes de correo electrónico usualmente contienen link para abrir otras páginas web, usted abre esos links sin una previa revisión de la fuente del mensaje?

Tabla 2.11: Valoración sobre la forma de actuar, al momento de recibir un correo electrónico

Detalle	Frecuencia	Porcentaje
Si	1	9,09
No	7	63,63
A veces	3	27,27

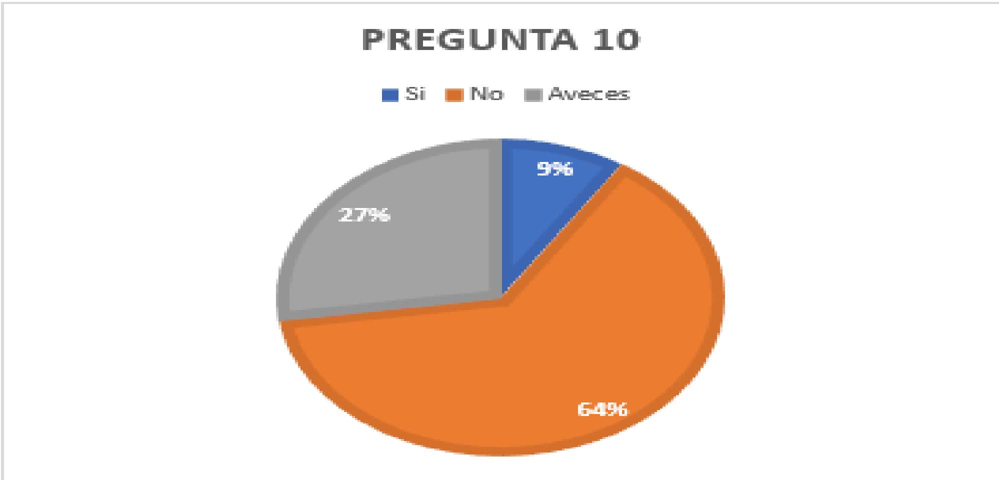


Figura 2.10: Respuestas obtenidas por los empleados referente a la forma de actuar al recibir un correo electrónico.
Fuente: Elaboración propia

Análisis e interpretación

El 64 % señalo que al recibir un correo electrónico donde su contenido tenga un link que le redirigiera a otra página web ellos no abren estos tipos de mensajes, mientras que el 27 % señalo que en ocasiones abre estos tipos de mensajes, asimismo el 9 % señalo que si lo hace sin revisar la fuente del mensaje.

Se logra apreciar que menos de la mitad de los empleados, han abierto algún tipo de correo electrónico sin hacer una previa revisión de la fuente del mensaje, de esta manera estarían abriendo una puerta a sufrir algún tipo de incidente de seguridad.

Información obtenida en las entrevistas

Conforme a las respuestas obtenidas a través de las entrevistas, se pudo determinar los siguientes criterios referentes a la seguridad de la información dentro de la empresa.

Políticas de seguridad

La empresa Textiles Jhonatex hasta la actualidad no posee de un manual de políticas de seguridad de la información, sin embargo, tiene implementados algunos controles que permiten limitar el acceso no autorizado a la información, pero estos no se encuentran debidamente documentados.

Organización de la seguridad de la información

No existe un Comité de Gestión de Seguridad de la Información que explícitamente se encargue en la toma de decisiones con respecto a implementaciones de controles y herramientas que ayuden a mejorar la seguridad de la información.

Al hablar del tema de Seguridad de la Información con los altos funcionarios, ellos piensan que se está refiriendo a la Seguridad Informática de la empresa, no se evidencia el conocimiento necesario, que ayude a distinguir entre los dos conceptos.

Al no existir un área o persona que se dedique únicamente a gestionar el tema acerca de la Seguridad de la Información no se sostiene contacto con empresas o grupos que aporten conocimientos referentes al tema.

Los controles implementados no son continuamente monitoreados, mientras no se reporte ningún mal funcionamiento, se asume que funciona bien, caso contrario se soluciona en ese mismo instante.

Gestión de Activos

El área de Sistemas cuenta con inventarios de equipos tecnológicos, los cuales son actualizados únicamente cada fin año.

El área de Sistemas carece de un documento formal donde se especifique los usuarios y los activos asociados con los medios de procesamiento de información.

Seguridad de los Recursos Humanos

Desde los empleados hasta las máximas autoridades no poseen conocimientos concisos acerca de temas relacionados a la seguridad de la información, además no conocen que tipos de controles de seguridad están implementados para mitigar algún incidente de seguridad. Puesto que nunca han recibido capacitaciones acerca del tema, de esta manera se abriría una puerta para posibles ataques.

Al terminar el contrato laboral de los empleados de la empresa, el jefe inmediato es quien se encarga de examinar que el empleado haga la respectiva entrega de la información utilizada y generadas durante presto su servicio a la empresa.

El proceso de contratación del nuevo personal este sigue un proceso exhaustivo, debido a que se pretende que la empresa no sea perjudica, de preferencia para una nueva contratación se toma como criterio principal contratar a los familiares del personal que demuestre compromiso con la empresa.

Seguridad Física

La empresa posee un sistema de cámaras, el cual es manejado por el guardia, el jefe de Sistemas, y los altos directivos.

El Rack de comunicaciones, así como el UPS se encuentra dentro del área de Sistemas, las llaves las tiene únicamente el jefe se Sistemas.

El área donde se encuentra el Rack y UPS no cuenta con la debida señalización para su fácil identificación.

Cuenta únicamente con un UPS que permite tener energía eléctrica por 2 horas cuando existe alguna interrupción de la energía, lo que les da el tiempo necesario para tomar medidas adecuadas, de esta manera se evita daños a los equipos tecnológicos y posible pérdida de la información.

Para limitar el acceso no autorizado a personas ajenas a la empresa, todos los equipos informáticos se encuentran ubicados dentro de las áreas.

Los mantenimientos en los equipos de procesamiento de información y de los equipos informáticos se los realiza cada 4 meses, pero si no es posible se lo realiza cada 6 meses, pero carece de documentación donde se describa que tipos de mantenimiento se realizaron.

Para sacar equipos fuera de las instalaciones de la empresa, esta debe ser debidamente autorizada por los altos directivos.

Control de acceso

Posee un mecanismo que permite bloquear automáticamente las estaciones de trabajo cuando se encuentran desentendidas.

La única forma de ingresar a la red de la empresa, es a través de los equipos tecnológicos de la empresa, debido a que no se les permite ingresar cualquier equipo externo que no sea de la misma.

A los equipos informáticos se les restringe el ancho de banda a solo 2 MB, para evitar la saturación en la red.

Gestión de incidentes en la seguridad de la información

Al no existir un procedimiento formal para el tratamiento de incidentes de seguridad, no se puede llevar a cabo acciones al momento de presentarse algún incidente de seguridad grave y/o menor, pues al ocurrir algún tipo de incidente de seguridad el Gerente de Sistemas es el encargado de indicar las acciones que se deben tomar.

Con respecto al incidente de seguridad en el último año se registró un posible ataque de denegación de servicio (DDoS), lo cual no fue de gran importancia. Sin embargo, hace aproximadamente 2 años la empresa sufrió un ataque que perjudico a la empresa, debido a que se robó información valiosa, pues los respaldos de información en esa época no se los realizaba diariamente como actualmente se lo realiza, el perjuicio a la empresa fue alrededor de 8.000 dólares, sin embargo, se logró identificar el causante del perjuicio pues era el mismo que estaba encargado en esa época del área de Sistemas.

No se encuentran registros las acciones correctivas que se tomaron después de tener el incidente.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

Para mejorar la seguridad de la información en la empresa Textiles Jhonatex se hará uso de dos metodologías, el propósito de cada una de estas se describe a continuación.

Las evaluaciones de seguridad, se las realiza con el objetivo de encontrar vulnerabilidades potenciales que pueden ser comprometidas mediante el acceso de un agente no autorizado, generalmente las evaluaciones de seguridad se realizan con una fecha de inicio y finalización. Estas una vez identificadas, son detalladas mediante un informe el cual proporciona recomendaciones para sus correcciones [20].

Sin embargo, la gestión de vulnerabilidades, va más allá que solo una simple evaluación de seguridad, ya que es un proceso integral continuo, con el objetivo de administrar las vulnerabilidades a largo plazo en una organización. Teniendo en cuenta estos dos conceptos, se realizará un proceso de gestión de vulnerabilidades basado en la metodología NIST 800-155, puesto que se especializa en evaluaciones de seguridad técnicas, el cual ofrece pautas que debe considerar antes y después de realizar la evaluación.

Este proceso ayudará a mejor la seguridad informática en la empresa Textiles Jhonatex, no obstante, para mejorar los niveles de protección, se necesita conocer los riesgos a los que se puede encontrar la misma, puesto que al desconocer estos riesgos provocaría impactos adversos como: divulgación, modificación no autorizadas de información, pérdida de información o la disponibilidad del sistema de información, generadas por debilidades en los controles internos, procedimiento de seguridad del sistema o el sistema de información.

Los sistemas de información generalmente están compuestos de los siguientes recursos como se muestra en la figura 3.1.

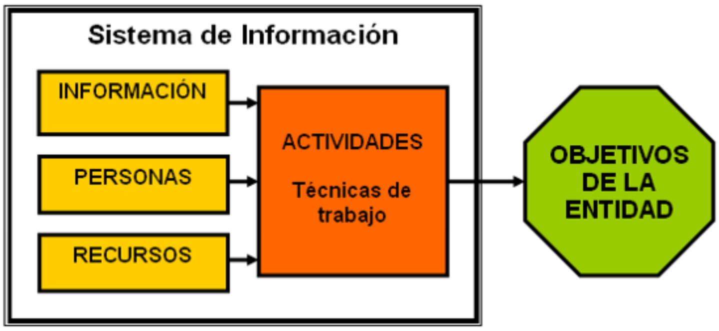


Figura 3.1: Componentes básicos de un Sistema de Información
Fuente: [21]

Por tal motivo, se necesita una metodología de evaluación de riesgos que permita identificar las vulnerabilidades que pueden ser explotadas por una o varias fuentes de amenazas, con el objetivo de evaluar los riesgos y realizar recomendaciones de mitigación, haciendo uso de la metodología NIST 800-30, se cumplirá con este objetivo

A continuación, se hace una breve descripción de estas dos metodologías.

NIST SP 800-115

En esta metodología describe de forma estructurada, cómo debe realizarse el proceso de evaluación de seguridad de la información en una organización. Los elementos más sobresalientes de esta metodología son:

- Ofrece una visión general sobre el enfoque de las evaluaciones de seguridad que los evaluadores deben tomar encuentra antes de realizar la evaluación, esto se logra apreciar en la figura 3.2.

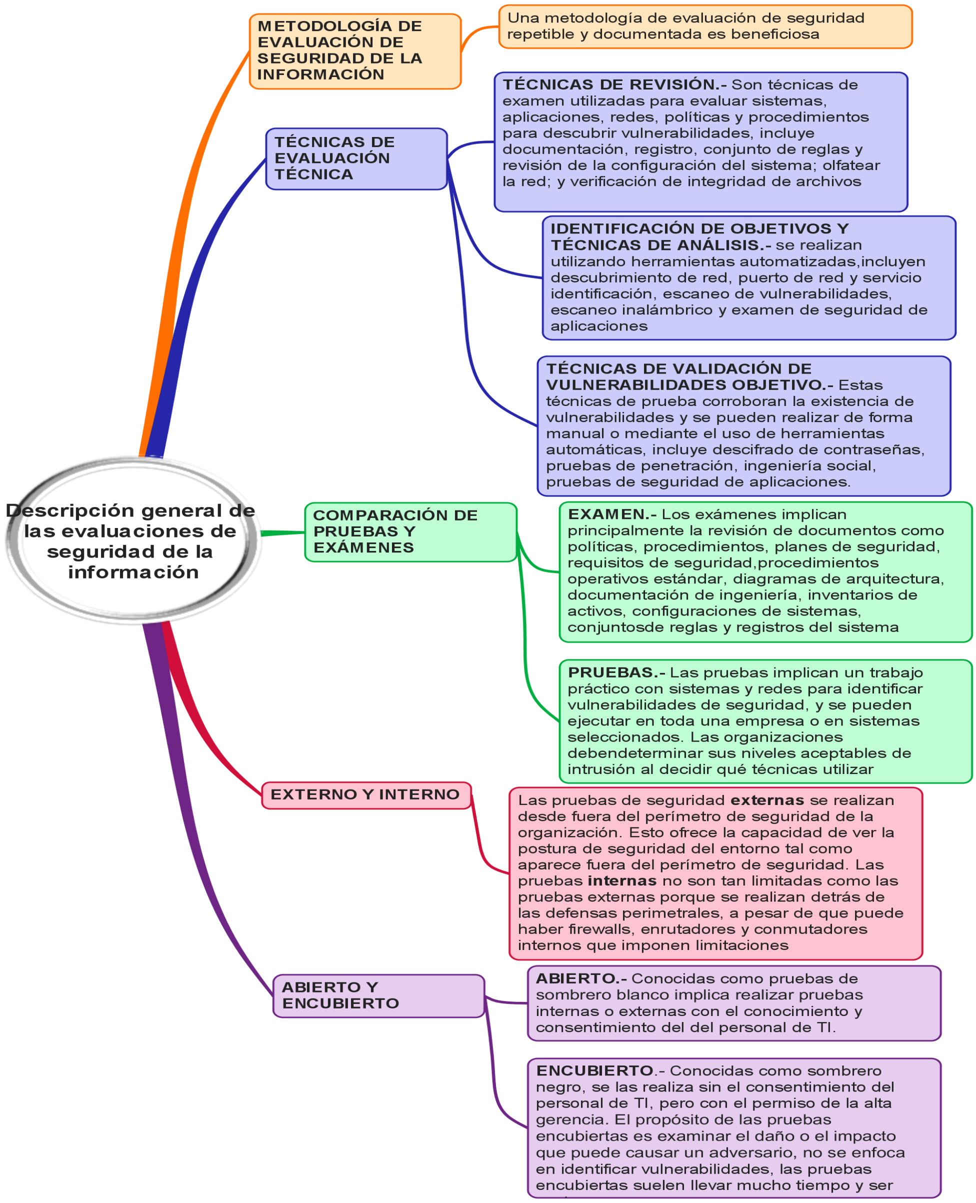


Figura 3.2: Descripción de las evaluaciones de seguridad
Fuente: Elaboración propia a partir de [17]

- Presenta técnicas de evaluación que una organización podría usar como parte de la evaluación que utilizan generalmente los atacantes reales, ofreciendo información adicional sobre los conocimientos mínimos en informática que deben tener los evaluadores antes de realizar una evaluación de seguridad, de esta manera evitar un impacto adverso en la organización, como se muestra en la figura 3.3.

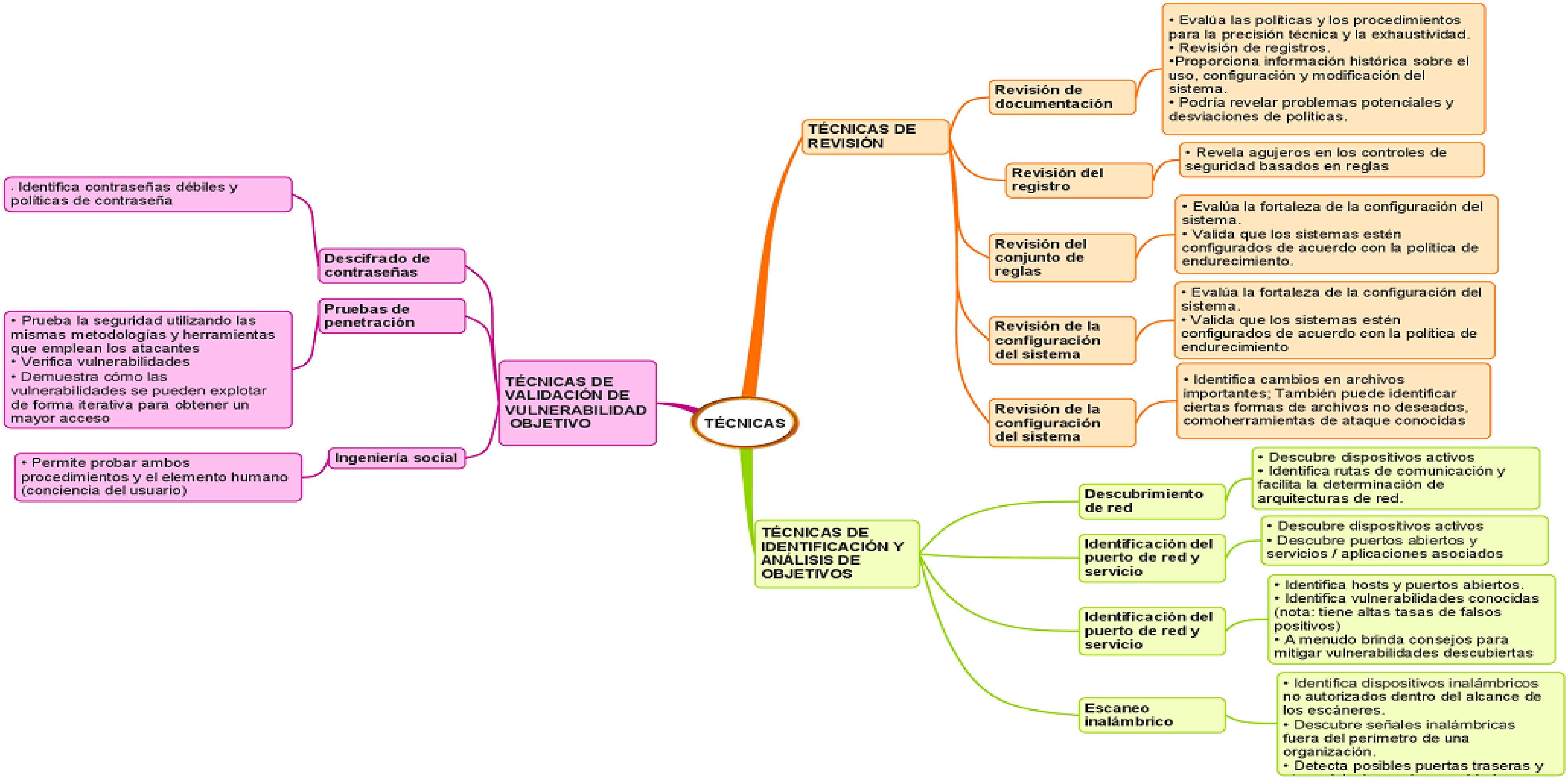


Figura 3.3: Tipos de técnicas de evaluación
Fuente: Elaboración propia a partir de [19]

- Determina el proceso de evaluación con puntos tales como: objetivos, alcances, limitaciones, roles, involucrados, resultados, mecanismos de mitigación, entre otros, como se muestra en la figura 3.4.

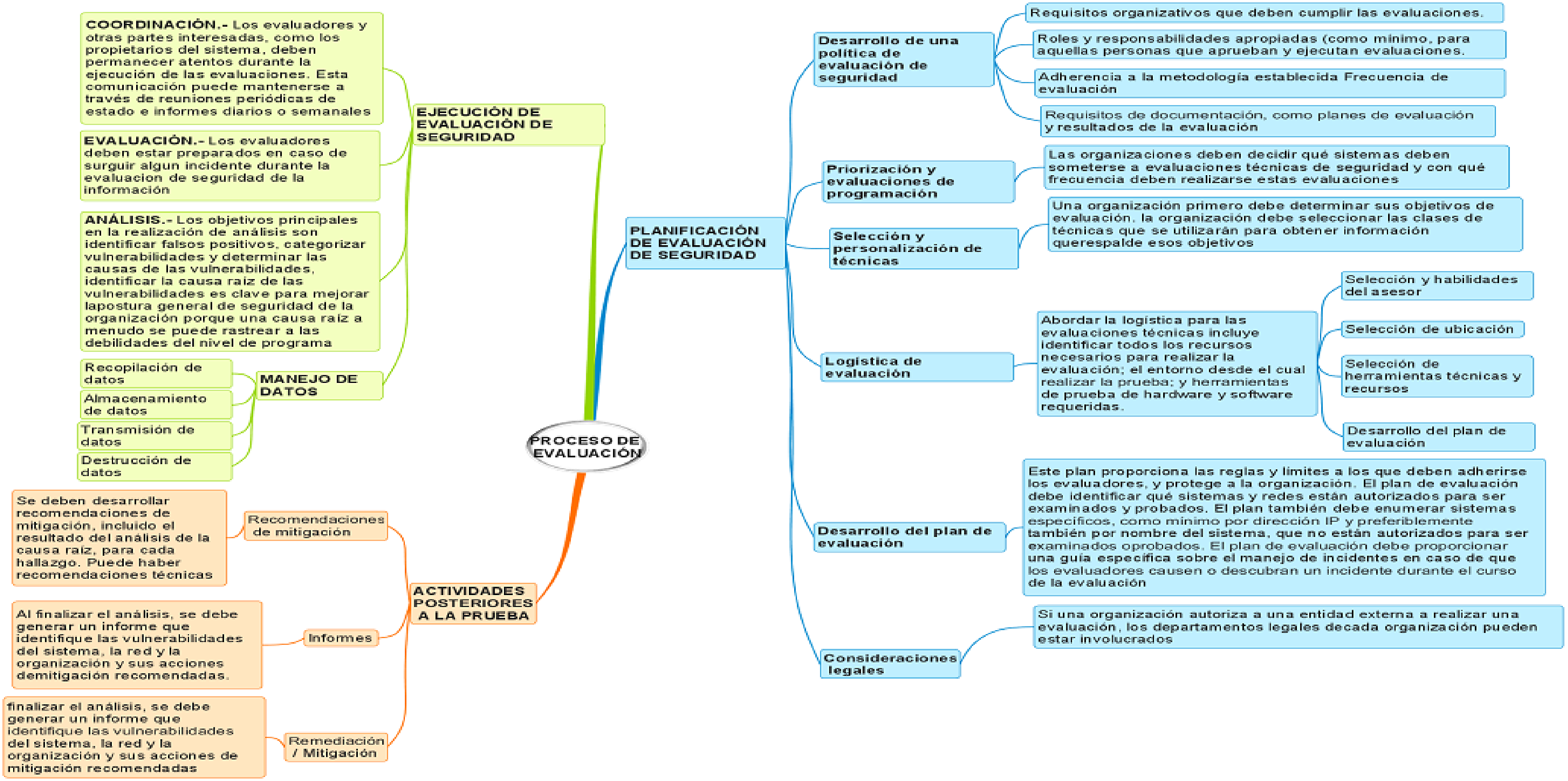


Figura 3.4: Proceso de la evaluación de seguridad
Fuente: Elaboración propia a partir de [19]

NIST SP 800-30

Es una guía de gestión de riesgo para sistemas de tecnología de la información, propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información. Además, los conceptos y principios relacionados con los procesos y métodos de evaluación de riesgos proporcionada en esta guía se pretenden que sean consistentes y parecidos con los procesos y enfoques descritos en la Organización Internacional de Normalización (ISO) y la Internacional Comisión Electrotécnica Internacional (IEC).

Según NIST, la evaluación de riesgos se define como el proceso de identificar, estimar y priorizar los riesgos de seguridad de la información, mientras que el riesgo se expresa en función de la probabilidad de que ocurra un evento de amenaza y el impacto adverso potencial, si el evento ocurre.

El método de evaluación de riesgos adoptado por el NIST 800-30 incluye:

1. Un modelo de riesgo explícito
2. Un enfoque de evaluación
3. Un enfoque de análisis
4. Un proceso de evaluación de riesgos

1. Modelo de riesgo

Un modelo de riesgo define los factores de riesgo a evaluar y las relaciones entre esos factores. Se define cinco factores de riesgo en la NIST 800-30, los cuales se describe a continuación:

- Amenaza: Es cualquier evento que pueda tener un impacto adverso en los activos organizacionales, operacionales, individuos, de un sistema de información.
- Vulnerabilidad: Es una debilidad en un sistema de información, controles internos, procedimiento de seguridad del sistema, que puede ser explotados por una fuente de amenaza.
- Condición predisponente: Es una condición que existe en sistema de información, controles internos, procedimiento de seguridad del sistema, que

afecta o disminuye la probabilidad de que los eventos de amenaza, tengan un impacto adverso en la organización.

- Probabilidad: Se basada en un análisis de la probabilidad de que una amenaza sea capaz de explotar una vulnerabilidad o conjunto de vulnerabilidades.
- Impacto: Es la magnitud del daño que puede resultar de las consecuencias de la divulgación, modificación no autorizadas de información, o la pérdida de información o disponibilidad del sistema de información.

2. Enfoque de evaluación

Se analizan tres enfoques en NIST 800-30 para evaluar el riesgo: cuantitativo, cualitativo y semicuantitativo.

- Cuantitativa: Se emplea haciendo uso de conjunto de métodos, principios o reglas basadas en el uso de números.
- Cualitativa: Se emplea un conjunto de métodos, principios o reglas basadas niveles no numéricos (bajo, medio, alto).
- Semicuantitativa: Se emplea un conjunto de métodos, principios o reglas que utilizan escalas o números representativos (0-15, 16-35, 36-70,71-85, 86-100).

3. Enfoque de análisis

El enfoque de análisis difiere con respecto a la orientación o punto de partida de la evaluación de riesgos, asimismo su nivel de detalle. El enfoque de análisis discutido en la metodología es tres:

- Orientado a amenazas.
- Orientado a activos / impacto.
- Orientado a la vulnerabilidad.

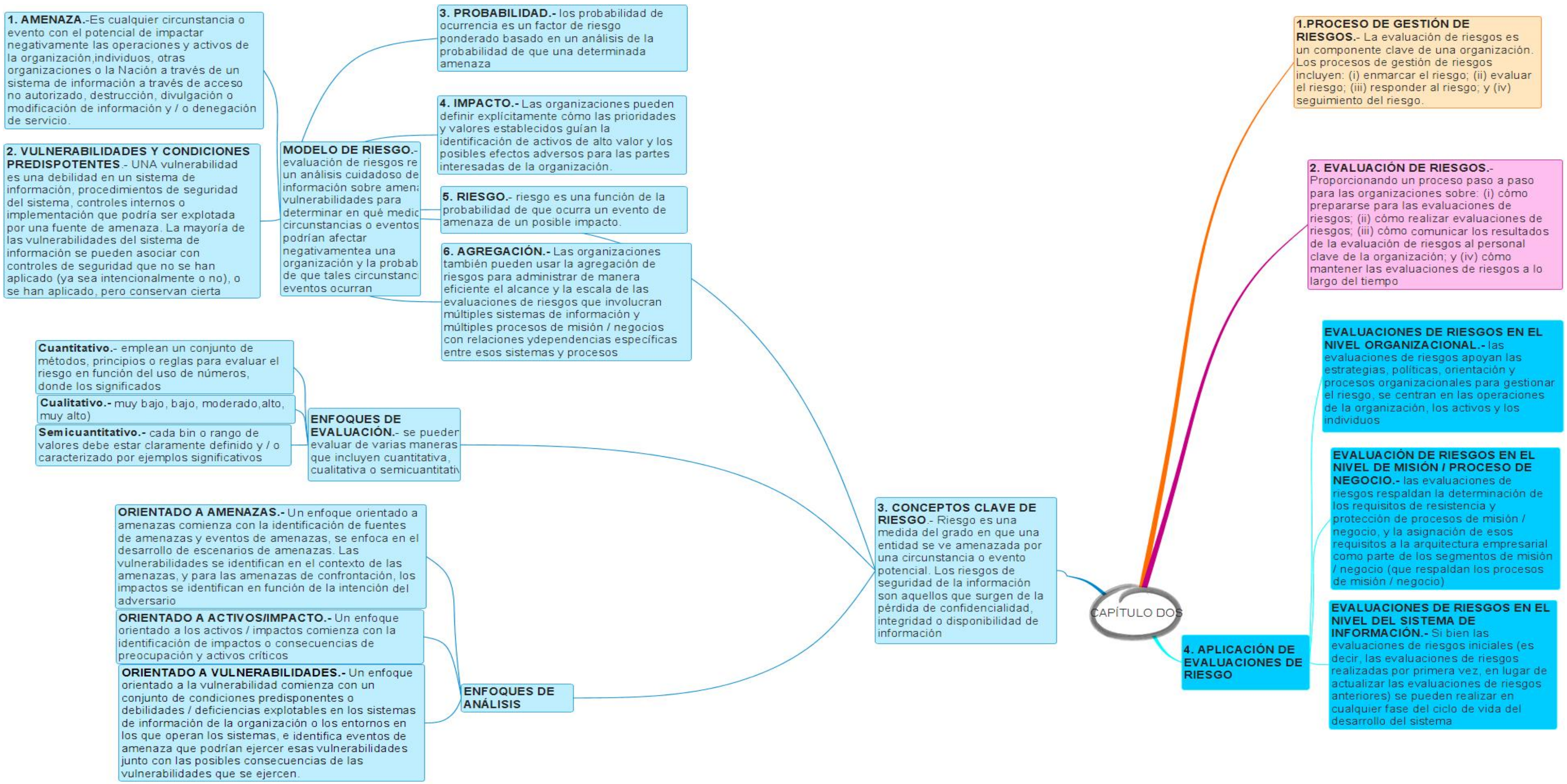


Figura 3.5: Método de evaluación de riesgo
Fuente: Elaboración propia a partir de [17]

4. Proceso de evaluación de riesgos

El proceso de evaluación de riesgos se compone de cuatro pasos. Cada uno de estos se encuentra divididos en un conjunto de tareas. Además, el proceso permite a las organizaciones utilizar el resultado de una evaluación como entrada útil para la respuesta al riesgo o aspecto de tratamiento del proceso de gestión de riesgos, esto se evidencia en la figura 3.6.

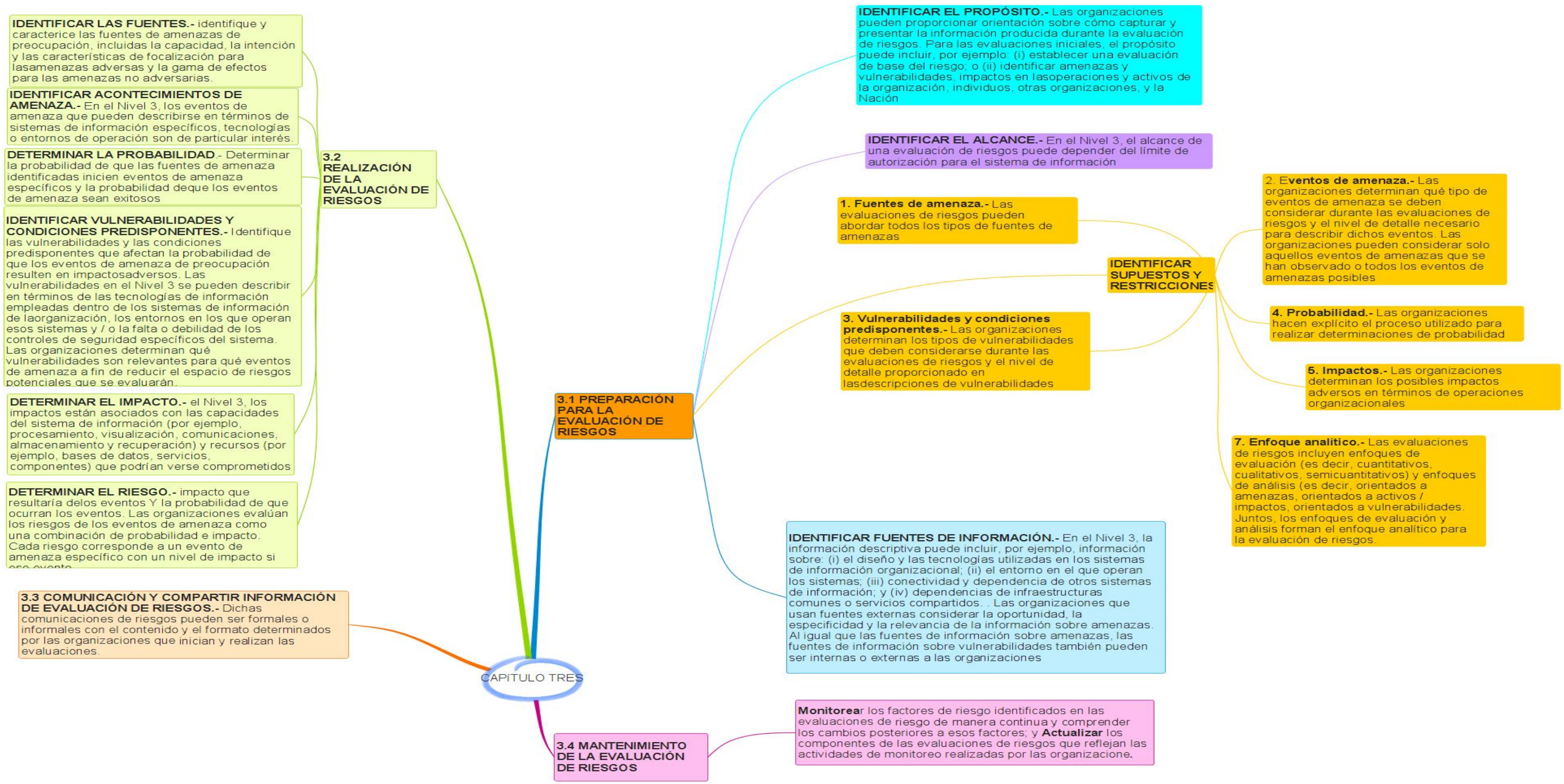


Figura 3.6: Proceso de evaluación de riesgo
Fuente: Elaboración propia a partir de [17]

3.1. Inventario de Textiles Jhonatex

Como primer paso, se realizará un inventario de los activos de información de la empresa Textiles Jhonatex, de esta manera, permite conocer que activos que se encuentran asociados a los procesos de la información.

Los activos de información para una organización son todos aquellos componentes que permiten el funcionamiento de la organización, estos pueden ser equipos tecnológicos, comunicación entre diferentes sistemas, recurso humano.

A continuación, se describe de forma general los activos de la empresa Textiles Jhonatex en la tabla 3.1.

Tabla 3.1: Resumen general de lista de activos de la empresa

Activos de la empresa Textiles Jhonatex	
Tipo de activo	Descripción
Hardware	Equipos de oficina (computadoras de escritorio, laptops).
Software	Aplicaciones instaladas en los equipos informáticos (antivirus, ofimática, entre otros).
Sitio Web	Servicio.
Comunicación	Red de área local e inalámbrica, telefonía ip

Fuente: Elaboración propia a partir del inventario de la empresa

3.1.1. Hardware

El inventario de hardware permite detallar los activos informáticos que integran la red empresarial. Para el caso de la empresa Textiles Jhonatex, estos se describen a continuación.

La empresa se encuentra divido en las siguientes áreas, en los cuales se encuentran los siguientes equipos de escritorio, como se describe en la tabla 3.2.

Tabla 3.2: Listado de equipos de computación por cada área de la empresa

Departamentos	Esquipos
Gerencia	2
Sistemas	1
Compras	2
Cobros	1
Financiero	1
Contabilidad	1
Seguridad industrial	1
Producción tela terminado	1
TTHH/Administración,	1
Diseño de cuellos/bodega	1
Laboratorio	1
Bodega	2
Dabotex	1
Gematex	1

Fuente: Elaboración propia a partir del inventario de la empresa

Asimismo, en el departamento de sistemas se encuentran los siguientes equipos tecnológicos, como se puede apreciar en la tabla 3.3.

Tabla 3.3: Listado de equipos tecnológicos del departamento de sistemas

Equipo tecnológico	Modelo
Servidor primario	HP DL380
Router ap	Tplink 3 antenas
Dvr	Dh-dvr2116h
Central telefónica	Panasonic kx-tem824
Router frontera	2 mikrotick 750gr
Miniordenador	Tx3mini
Miniordenador	Acepc
Ups	Tripplite 1kva
Rack	Next 30 u
Switch	24p dlink
Switch	24p nexxt no gestionable
Rack	Pared 12 u con regleta energia
Central telefonica	Panasonic kx-ns500
Dvr	32 canales hcvr4232an
Router	Mikrotick 951u
Router ap	Tplink 3 antenas

Fuente: Elaboración propia a partir del inventario de la empresa

3.1.2. Software

ElEl inventario de software permite detallar las aplicaciones que se encuentran instaladas en los equipos informáticos la empresa. Esto se detalla a continuación en la tabla 3.4.

Tabla 3.4: Listado de software que utiliza la empresa

Software	Función
Microplus	Sistema contable usado en las siguientes áreas: gestión de bodega e inventarios, contabilidad, cobros, costos, tthh y facturación.
Software sin nombre para el área de laboratorio	Programado por terceros, destinado a la creación de mezclas y composiciones químicas destinadas a la tintura de productos.
Datacolor tools	Sistema de gestión y control de datos adquiridos por espectrofotómetros para obtener las coloraciones y calidad la calidad producto.
Software sin nombre para el departamento de TTHH	Sistema de almacenamiento y gestión de registros mediante el uso de la tecnología biométrica. Este sistema reportes diarios y mensualidades de asistencias del personal.
Office 2013 con licencia	Permite automatizar y perfeccionar las actividades habituales del área administrativa.

Fuente: Elaboración propia a partir del inventario de la empresa

3.1.3. Servidores

La empresa Textiles Jhonatex posee un servidor físico como servidor principal, y un servidor secundario que se encuentra virtualizado en el servidor principal, con la tecnología Hiper-V. A continuación, se describe las características
de los servidores tanto del hardware como el software, como se muestra en la tabla 3.5, 3.6.

Tabla 3.5: Características de hardware y software del servidor principal

Servidor Principal	
Hardware	Software
• Compatible con la segunda generación de la familia de procesadores escalables Intel® Xeon®, 2 x NVIDIA Quadro P4000 Graphics Accelerator. • 64 GB (4 x 16 GB) DDR4 2666 Registered Smart Memory Kit • Montaje en rack de 2U y 19"	• Windows Server 2012 R2 • Microplus SQL Server

Fuente: Elaboración propia a partir del inventario de la empresa

Tabla 3.6: Características de software del servidor secundario

Servidor Secundario	
Hardware	Software
No se dispone de esta información	• Windows Server 2008 R2 • Microplus SQL Client • XAMPP 7.3.23 para el software biométrico • Servicio de escritorio remoto (RDS),

Fuente: Elaboración propia a partir del inventario de la empresa

3.1.4. Servicios

La empresa Textiles Jhonatex, muestra su cartera de servicios mediante la una página web, esta se muestra en la figura 3.7.

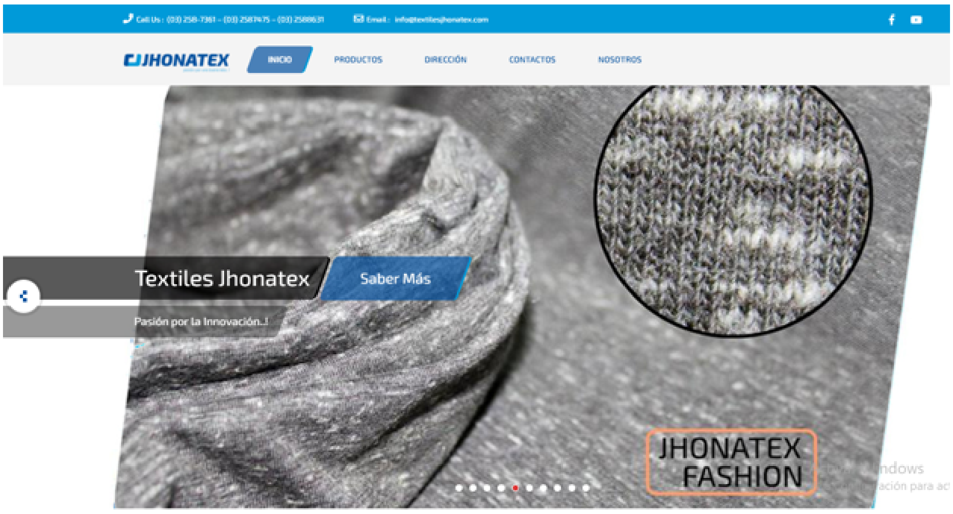


Figura 3.7: Portal web de la empresa Textiles Jhonatex
Fuente: Textiles Jhonatex

3.2. Evaluación de seguridad de la información

En el proceso de la evaluación de riesgo, para la parte de identificación de vulnerabilidades, la metodología NIST 800-30 sugiere la identificación de estas, mediante documentos de auditorías, evaluaciones de riesgos, evaluaciones de seguridad, que se hayan realizado anteriormente, por tal motivo se realizara esta evaluación, puesto que no se evidencia estos tipos de información en la empresa Textiles Jhonatex.

A continuación, se detalla el proceso de la evaluación de seguridad de la información.

3.3. Planificación

Es necesario identificar que activos formaran parte de la evaluación de seguridad, para después identificar que herramientas se usaran en los mismos, para posteriormente ser tratadas, esto se detalla a continuación.

3.3.1. Especificación de recursos que formaran parte de la evaluación

Se necesita conocer que activos se les considera con mayor grado de criticidad, los cuales formaran parte este proceso. Para la empresa Textiles Jhonatex estos recursos son: servidor principal, servidor secundario y también es considerado la estación de trabajo, es importante mencionar que, para evitar algún tipo de impacto adverso en la organización, se la realizara en un ambiente simulado, virtualizando estos recursos.

De igual forma se necesita conocer las características de hardware y de software de estos recursos, para esto se hará uso de la tabla 3.5 y 3.6 del inventario de la empresa, donde se encuentran descritas estas características de cada servidor de la empresa.

La estación de trabajo hace referencia al equipo de computación que usa el Gerente de Sistemas para administrar los servidores, igualmente se describirá las características de hardware y de software, para la parte del hardware se detallará los requisitos mínimos que deben contener estos para que funcionen las aplicaciones instaladas en estas. A continuación, se describe las características en la tabla 3.7.

Tabla 3.7: Características de hardware y software de la estación de trabajo

Estación de trabajo	
Hardware	Software
• Procesador de 32 bits (x86) o 64 bits (x64); a 2.0 gigahercio (GHz) o más. • Memoria RAM de 2 Gigabytes (GB) (32 bits) o memoria RAM de 4 GB (64 bits). • Soporte para gráficos DirectX 9 con 128 MB de memoria. • Tarjeta de red Fast Ethernet o Puerto USB.	• Windows 7 Professional • Terminal Remota

Fuente: Elaboración propia a partir del inventario de la empresa

A continuación, se describe el proceso para la creación del ambiente simulado.

Instalación de Windows Server 2012 R2 en el servidor principal

Las características del hardware del servidor físico, que formará parte de este ambiente simulado, en el cual se instalará el sistema operativo (S.O) Windows Server 2012 R2, se muestra en la tabla 3.8.

Tabla 3.8: Características del hardware del servidor para el ambiente simulado

Características
Nombre: TEXTILES_JHONATEX_BD
Procesador: Core i5
Memoria RAM: 8 GB
Disco duro: 500 GB

Fuente: Elaboración propia

La instalación de este S.O es similar de cualquier otra distribución de Windows, por tal motivo no se detallará la instalación de la misma. Una vez finalizado el proceso de instalación, iniciará automáticamente el administrador del servidor, como se muestra en la figura 3.8.

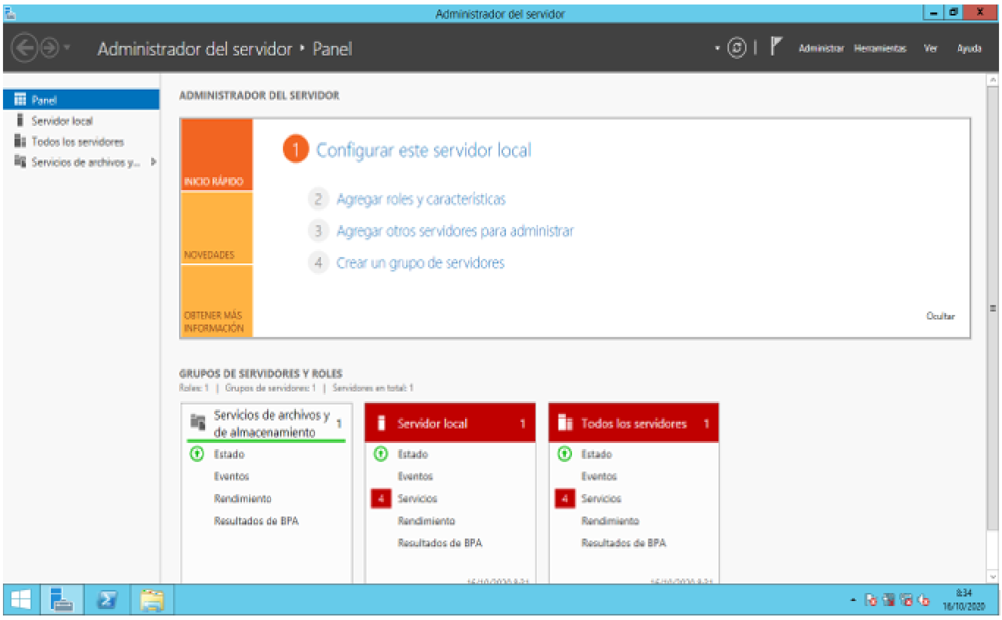


Figura 3.8: Interfaz gráfica de inicio del administrador de servicio
Fuente: Windows Server 2012 R2

Es importante mencionar que la empresa usa el sistema contable Microplus SQL Server para el lado del servidor y Microplus SQL Client para la parte del cliente, al no existir una versión de prueba de este sistema, debido a que el sistema se lo entrega personalmente a la empresa solicitante una vez realizada la compra de este software, por tal motivo queda fuera del alcance de este ambiente simulado. La figura 3.9, muestra los módulos que contiene el sistema contable Microplus.

Figura 3.9: Interfaz gráfica del sistema contable Microplus
Fuente: [22]

Sin embargo, este sistema contable Microplus usa el gestor de base de datos Sybase SQL Anywhere, perteneciente a la empresa SAP, el cual ofrece una gama de productos y servicios, en los siguientes ámbitos: manejo o administración de Información, desarrollo e integración, soluciones móviles, soluciones para la industria y soluciones verticales.

La versión Sybase de SQL Anywhere que se encuentra instalado en la empresa es la versión 12.0, por lo que se usará la misma versión, el cual se instalará en el servidor principal de este ambiente simulado, como originalmente se encuentra instalado en el servidor principal de la empresa Textiles Jhonatex.

En la figura 3.10, se muestra este gestor de base de datos iniciado correctamente en el servidor principal.

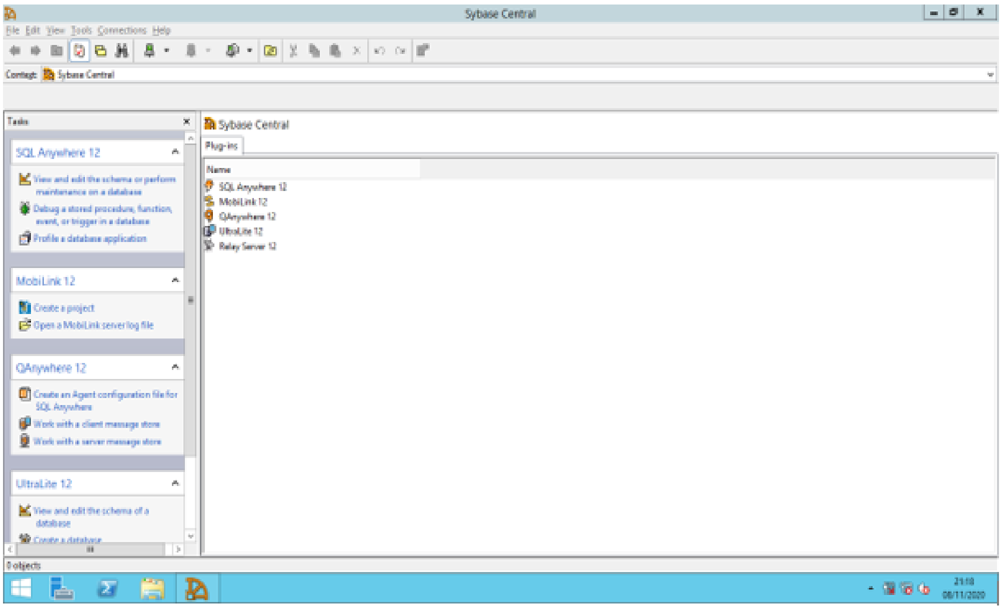


Figura 3.10: Interfaz gráfica Sybase de SQL Anywhere 12.0
Fuente: Sybase de SQL Anywhere

Activación de Hyper-V en el servidor principal

Para la virtualización del servidor secundario, la empresa usa la tecnología de virtualización Hyper-V, para este paso primero se debe activar la virtualización de Hyper-V que es una característica propia de Windows, para esto primero se debe hacer clic en la opción Administrar, que se encuentra en la parte superior derecha del administrador de servicio, luego agregar roles y características, aparece el siguiente cuadro de diálogo, donde se debe seleccionar roles de servidor y marcar la opción Hyper-V, como se muestra en la figura 3.11.

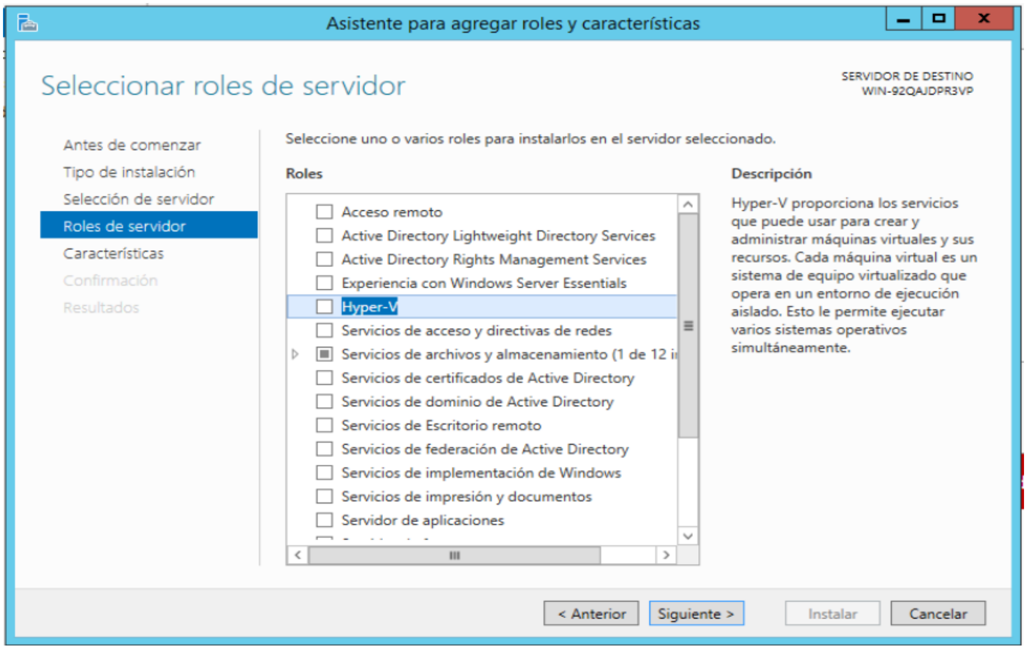


Figura 3.11: Interfaz gráfica del asistente para agregar roles y características
Fuente: Windows Server 2012 R2

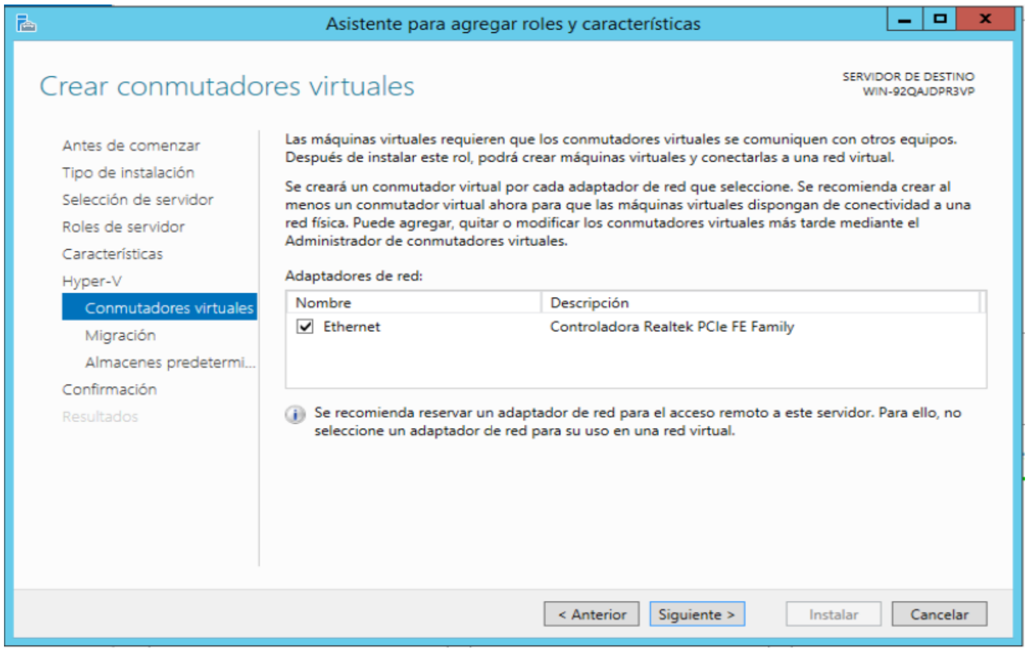


Figura 3.12: Interfaz gráfica de creación de conmutadores virtuales para máquinas virtuales
Fuente: Windows Server 2012 R2

En la figura 3.12, se muestra la creación del conmutador virtual, donde se debe especificar que adaptador de red se va a usar, en este caso solo está habilitado la tarjeta red Ethernet, esto permitirá que la máquina virtual creada en Hyper-

V, logre comunicarse con otros equipos en la red, en este caso con el servidor primario y la estación de trabajo.

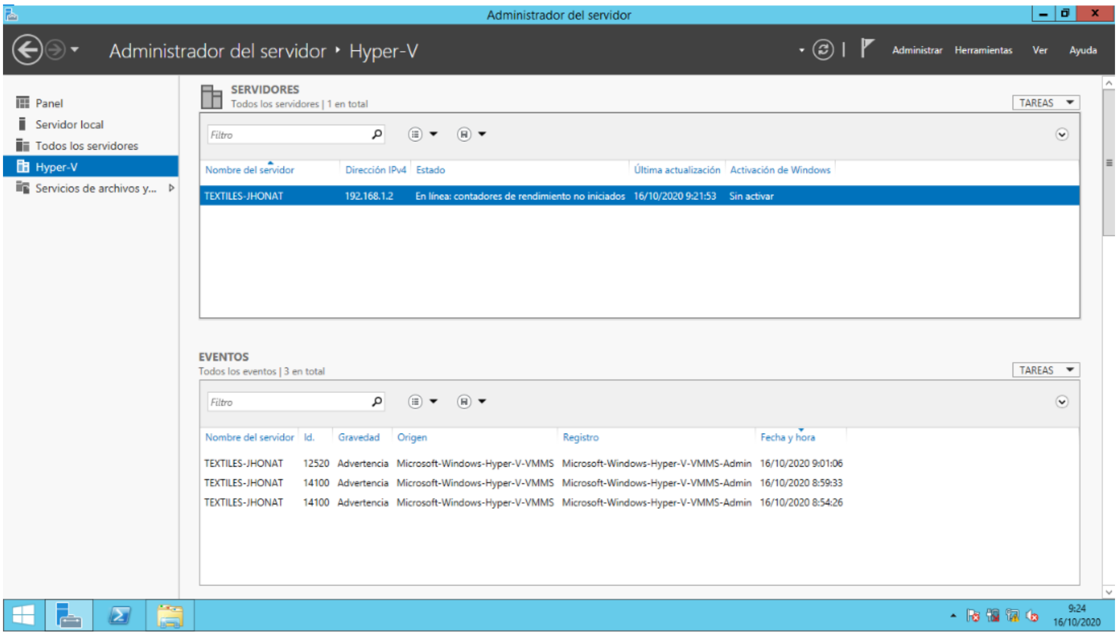


Figura 3.13: Interfaz gráfica la activación de Hyper-V
Fuente: Windows Server 2012 R2

En la figura 3.13, muestra que Hyper-V se encuentra correctamente instalado en el servidor y está listo para la virtualización.

Virtualización del servidor secundario

Para la virtualización del servidor secundario, primero se necesita ingresar al administrador del Hyper-V, se procede a crear la máquina virtual con el nombre TEXTILES_JHONATEX-CLIENTE, como se muestra en la figura 3.14.

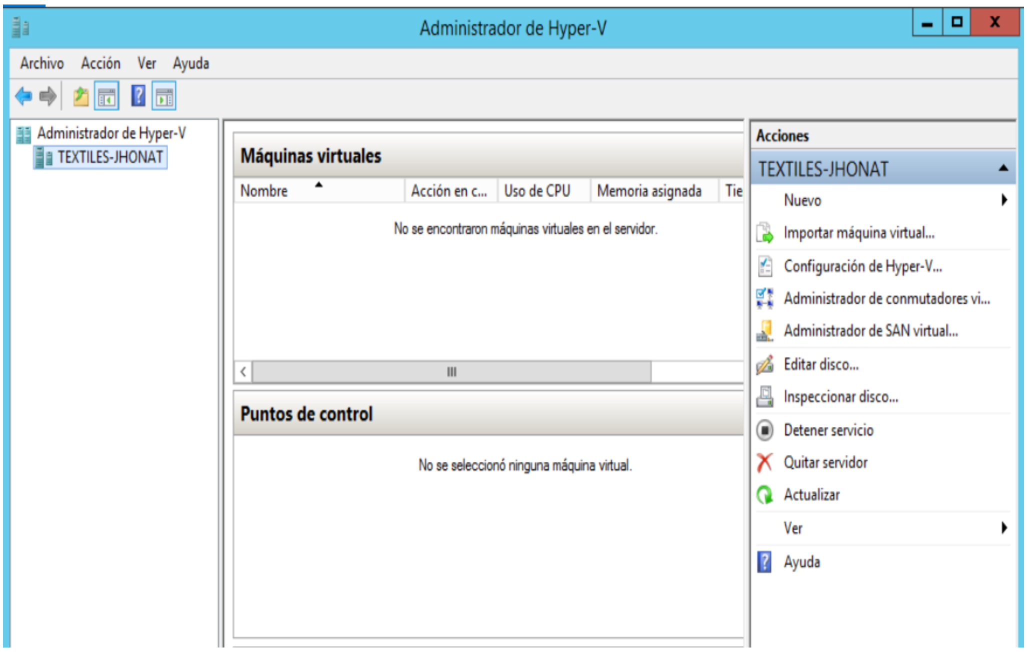


Figura 3.14: Interfaz gráfica del administrador de Hyper-V
Fuente: Windows Server 2012 R2

Para la creación de la máquina virtual, primero se debe dar clic derecho en el nombre del servidor físico, (TEXTILES_JHONATEX-BD), después se da clic en las opciones: Nuevo>Máquina virtual, como se muestra en la figura 3.15.

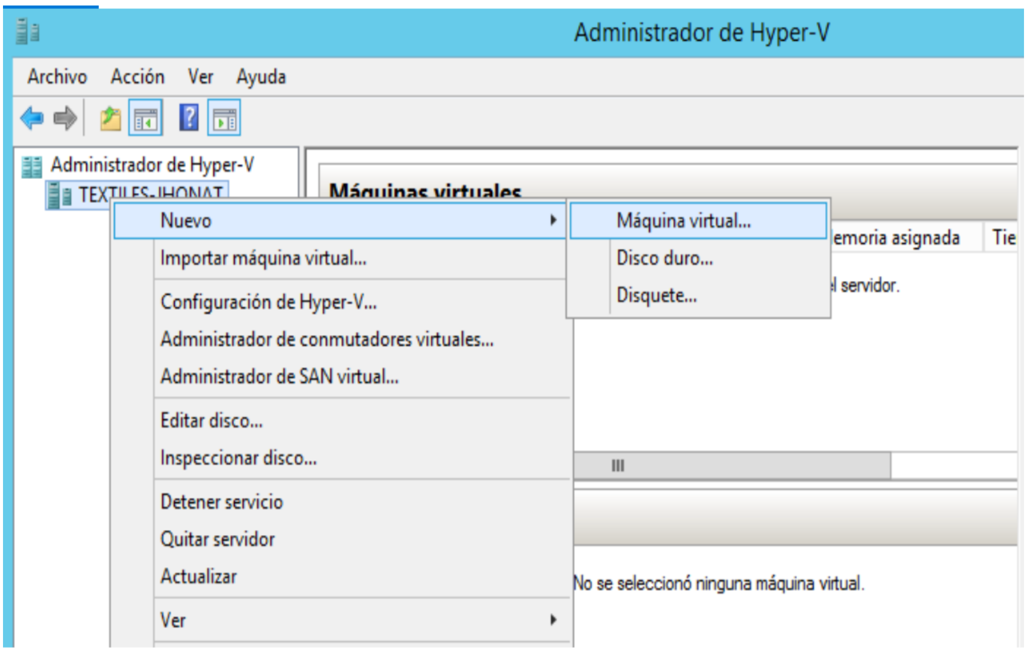


Figura 3.15: Interfaz gráfica de la creación de una máquina virtual
Fuente: Windows Server 2012 R2

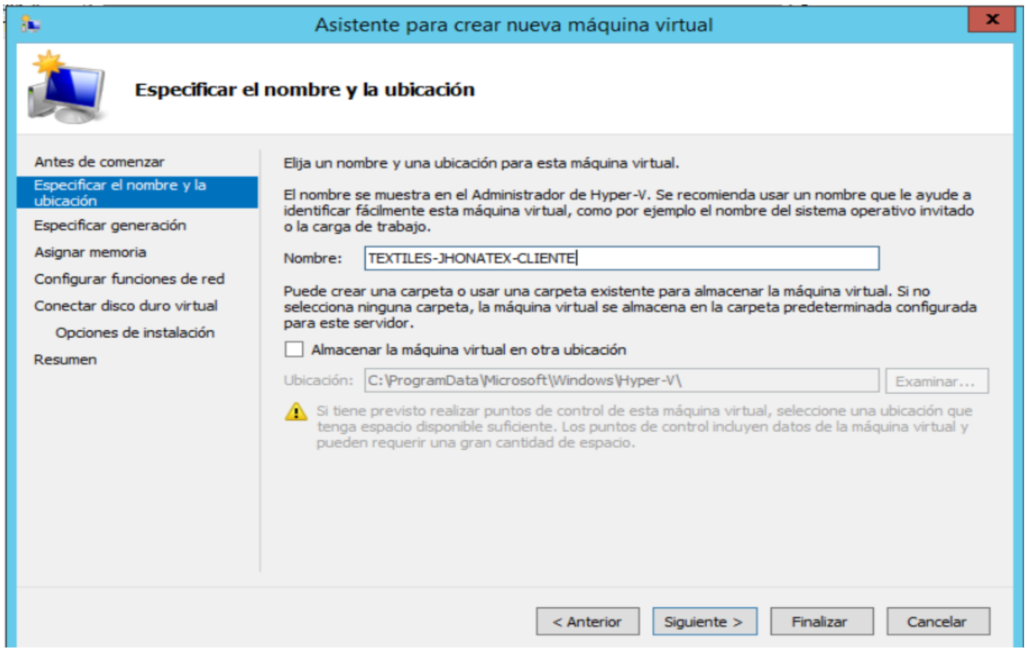


Figura 3.16: Interfaz gráfica del asistente para crear nueva máquina virtual
Fuente: Windows Server 2012 R2

En la figura 3.16, se muestra el cuadro de diálogo para la asignación de las características de hardware de la nueva máquina virtual, a continuación, se las describe en la tabla 3.9.

Tabla 3.9: Características de hardware de la nueva máquina virtual

Características
Nombre: TEXTILES_JHONATEX_CLIENTE
Memoria RAM: 3 GB
Tarjeta de red: Controladora Realtek PCIe FE Family – Virtual Switch
Disco duro: 100 GB

Fuente: Elaboración propia a partir del administrador de Hyper-V

Una vez terminado el proceso de asignación, se creará la nueva máquina virtual con estas especificaciones, como se muestra en la figura 3.17.

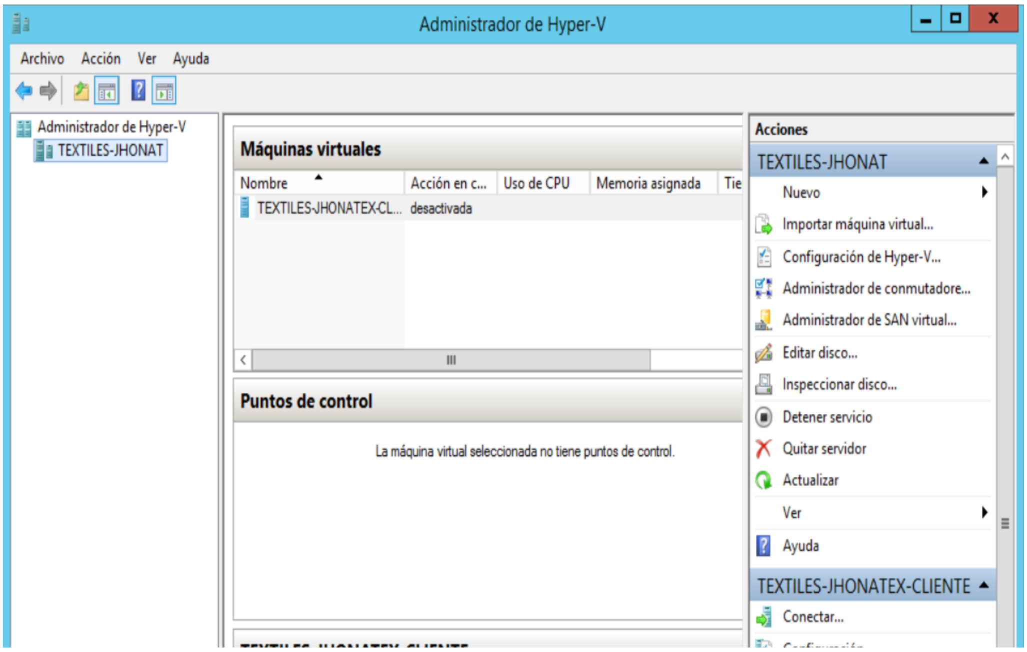


Figura 3.17: Interfaz gráfica de la nueva máquina virtual creada
Fuente: Windows Server 2012 R2

Instalación del sistema operativo Windows Server 2008 en el servidor secundario

Ahora se procede con la instalación de Windows Server 2008, para esto primero se debe iniciar la misma, como se muestra en la figura 3.18, una vez iniciado este proceso, se debe especificar la ruta de la imagen iso del sistema operativo a instalar, después se inicia el proceso de instalación como una distribución normal de Windows. Una vez terminado el proceso, se iniciará automáticamente el administrador de servicios de Windows Server 2008, como se puede apreciar en la figura 3.19.

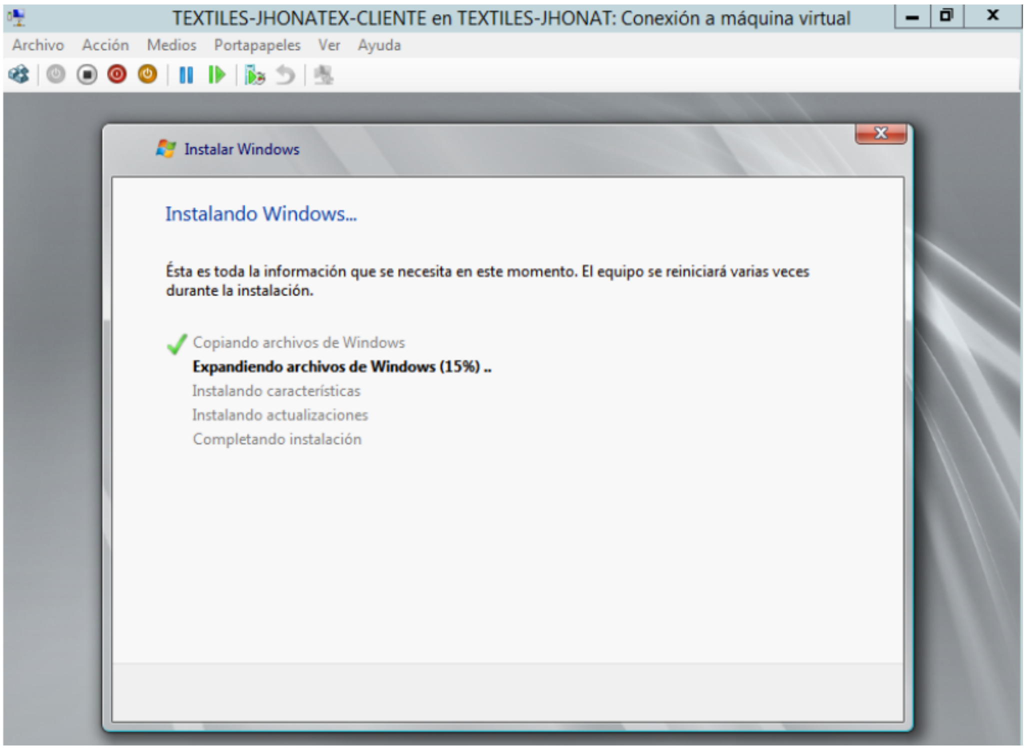


Figura 3.18: Interfaz gráfica del administrador de Hyper-V
Fuente: Windows Server 2012 R2

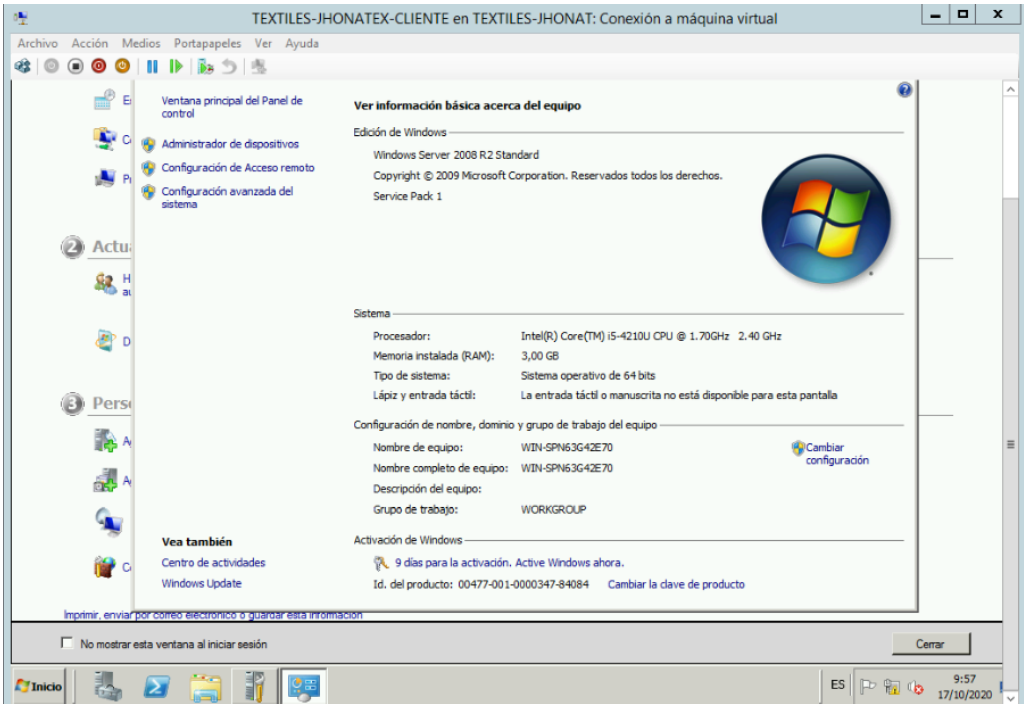


Figura 3.19: Interfaz gráfica del administrador del servicio
Fuente: Windows Server 2008

Una vez finalizado la instalación de Windows Server 2012 R2 en el servidor, y la virtualización del servidor secundario, este cuenta con los siguientes servicios anteriormente mencionados: servicio RDS, y servidor XAMPP 7.3.23, a continuación, se describe la instalación de estos servicios.

Activación de servicio RDS en el servidor secundario

Para activar el acceso remoto en el cliente, el cual permitirá el acceso de la estación de trabajo, el cual debe encontrarse dentro de la misma red, de igual manera este se conectará mediante las credenciales del usuario de acceso remoto, el cual será creado en el cliente.

Como primer paso se iniciará con la creación del usuario de acceso remoto en el cliente, se debe ir las siguientes opciones: Inicio > Herramientas administrativas > Administrador de equipos, como se muestra en la figura 3.20.

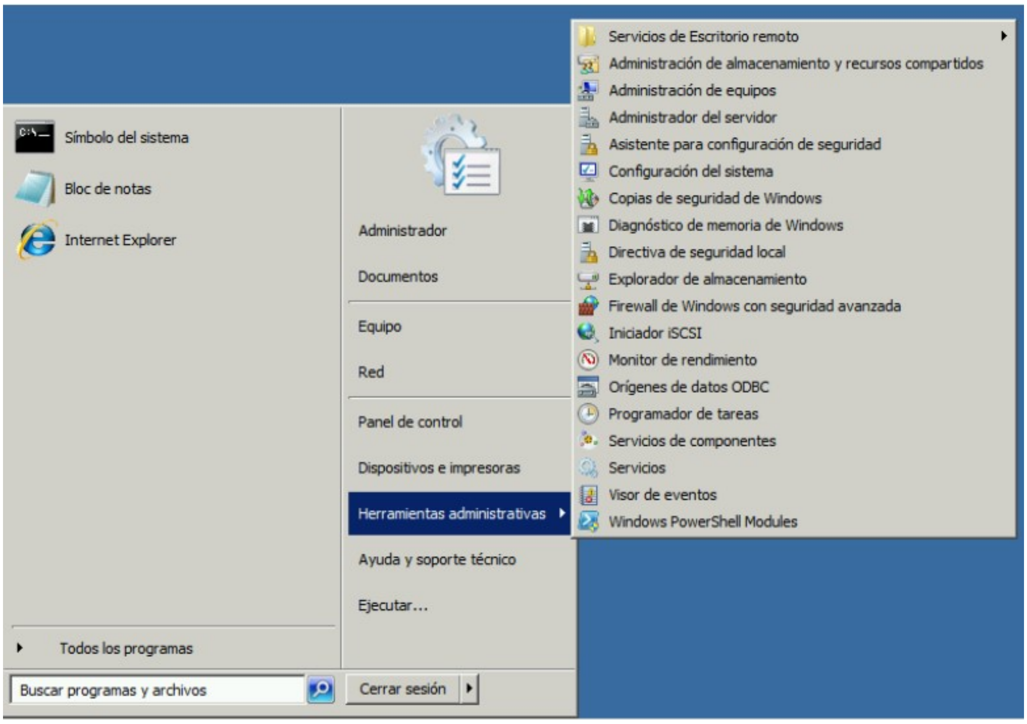


Figura 3.20: Interfaz gráfica del menú inicio de Windows Server 2008
Fuente: Windows Server 2008

Una vez ahí, se debe seleccionar la opción Usuarios y Grupos Locales, después doble clic izquierdo en usuarios, y clic derecho usuario como se muestra en la figura 3.21.

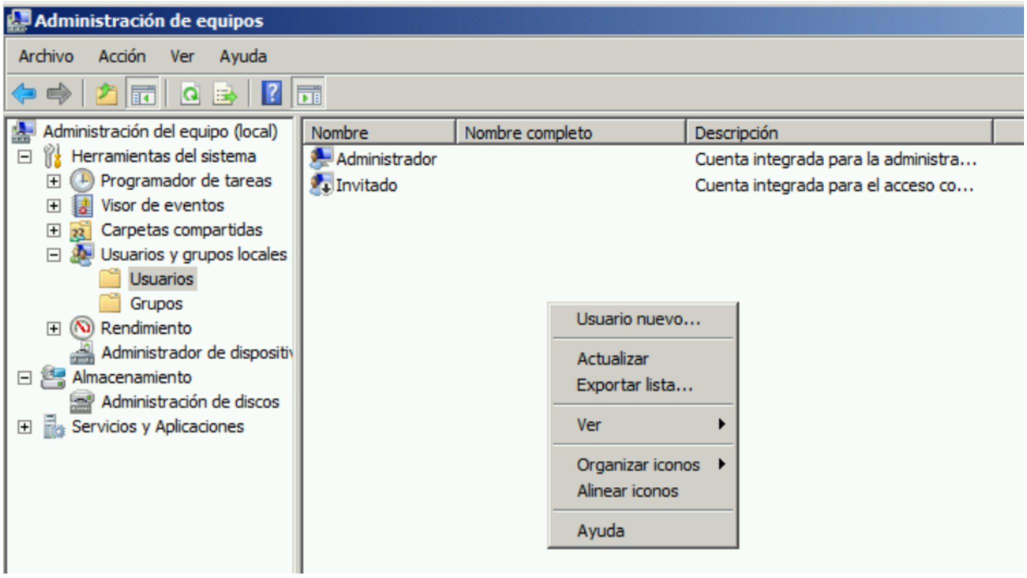


Figura 3.21: Interfaz gráfica de administrador de equipos
Fuente: Windows Server 2008

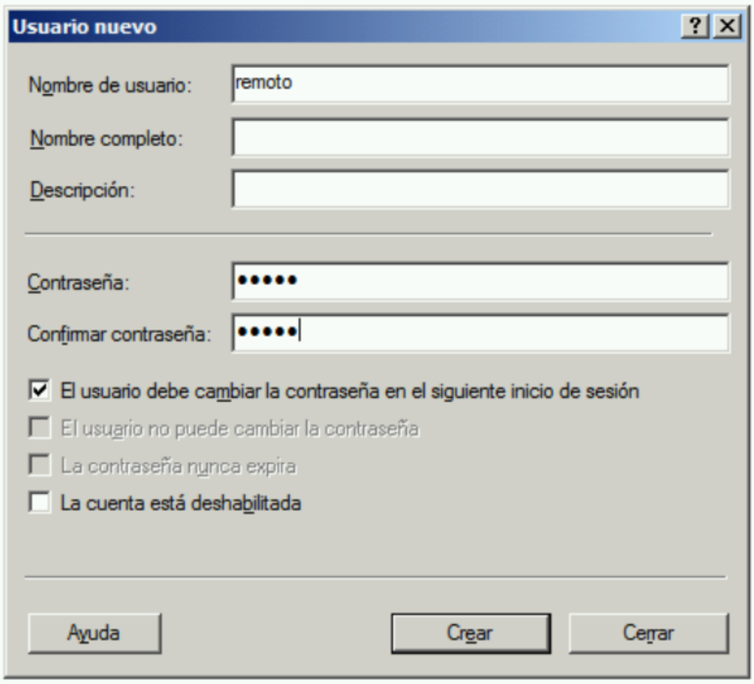


Figura 3.22: Interfaz gráfica usuario nuevo de
Fuente: Windows Server 2008

En la figura 3.22, se muestra la creación del nuevo usuario que será parte de usuario de acceso remoto, donde se le asignará un nombre y una contraseña, asimismo en la figura 3.23, una vez ya creado el usuario se lo asignará como usuario de acceso remoto, para esto se hará doble clic derecho en propiedades del usuario en este caso al usuario remoto.

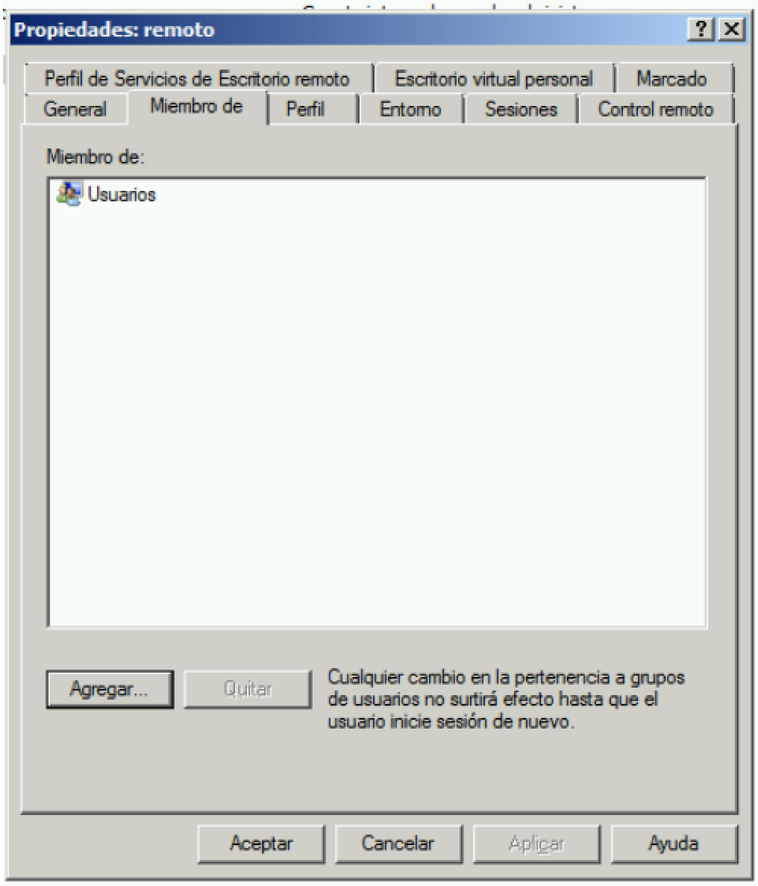


Figura 3.23: Interfaz gráfica de propiedades de usuario
Fuente: Windows Server 2008

Ahora se debe asignar al usuario remoto como Usuarios de acceso remoto, para esto se debe hacer clic en las siguientes opciones: Agregar > Opciones Avanzadas > Buscar ahora, aparecerá el siguiente cuadro de diálogo como muestra la figura 3.24, donde se debe seleccionar Usuarios de acceso remoto, para después aceptar y aplicar los cambios.

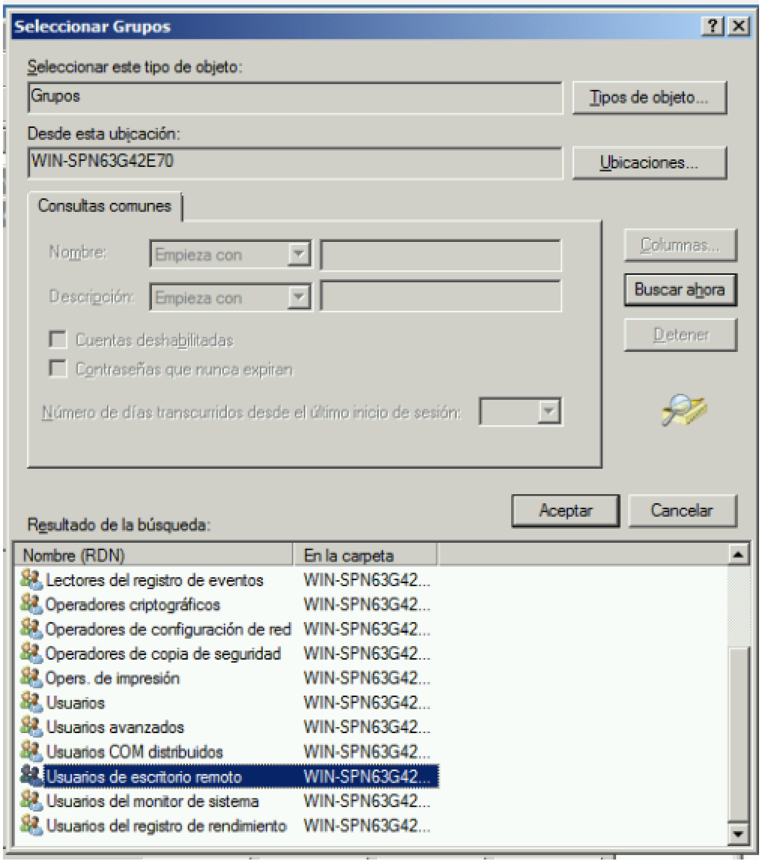


Figura 3.24: Interfaz gráfica de selección de grupos para el usuario remoto
Fuente: Windows Server 2008

Por último, se debe habilitar las conexiones de acceso, para esto se debe ir al menú inicio y dar clic derecho en Equipo, y seleccionar Propiedades, como se muestra en la figura 3.25.

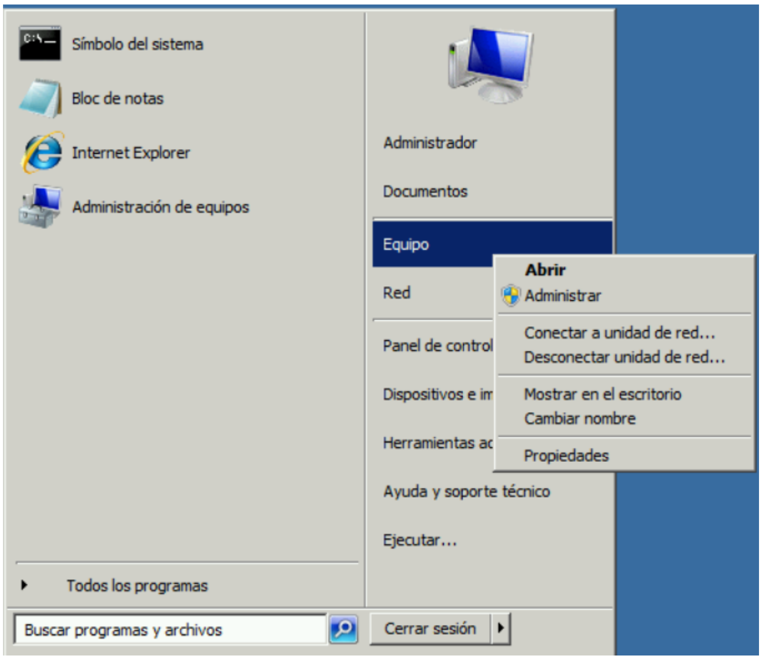


Figura 3.25: Interfaz gráfica menú inicio
Fuente: Windows Server 2008

Ahora se debe hacer clic la opción Configuración de acceso remoto como se muestra en la figura 3.26, el cual desplegara el cuadro de diálogo de las Propiedades del sistema, donde se debe escoger la opción Acceso remoto y seleccionar la tercera opción, y aceptar los cambios, como se muestra en la figura 3.27.

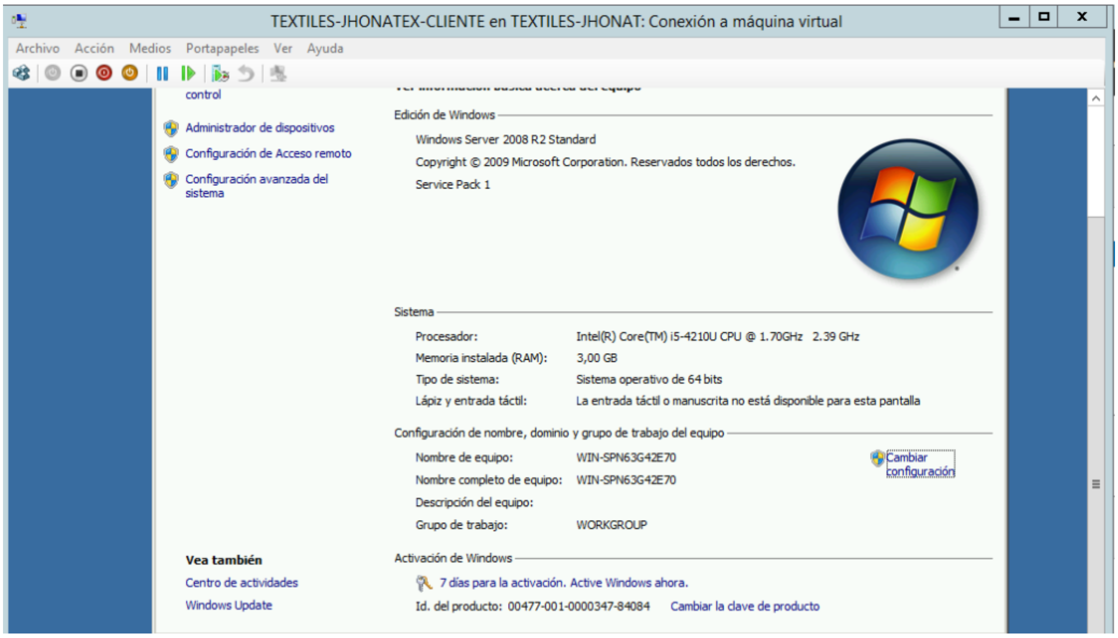


Figura 3.26: Interfaz gráfica de información del sistema
Fuente: Windows Server 2008

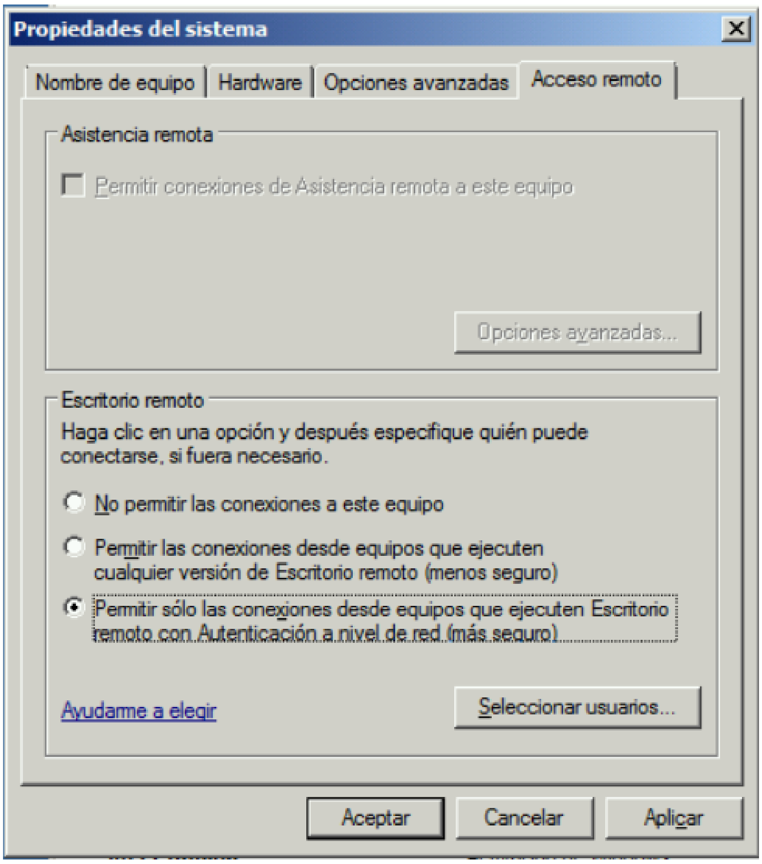


Figura 3.27: Interfaz gráfica de propiedades del sistema
Fuente: Windows Server 2008

Instalación de XAMPP 7.3.23

XAMPP es un servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl [22].

Una vez iniciado el proceso de instalación, aparecerá el siguiente cuadro de diálogo, como se muestra en la figura 3.28, en la sección de Servidor solo se marcará la opción MYSQL, que es un sistema de gestión de bases de datos, puesto que la empresa solo usa este servicio de XAMPP, para guardar la información de registro diario de entrada y salida del personal mediante un software biométrico.

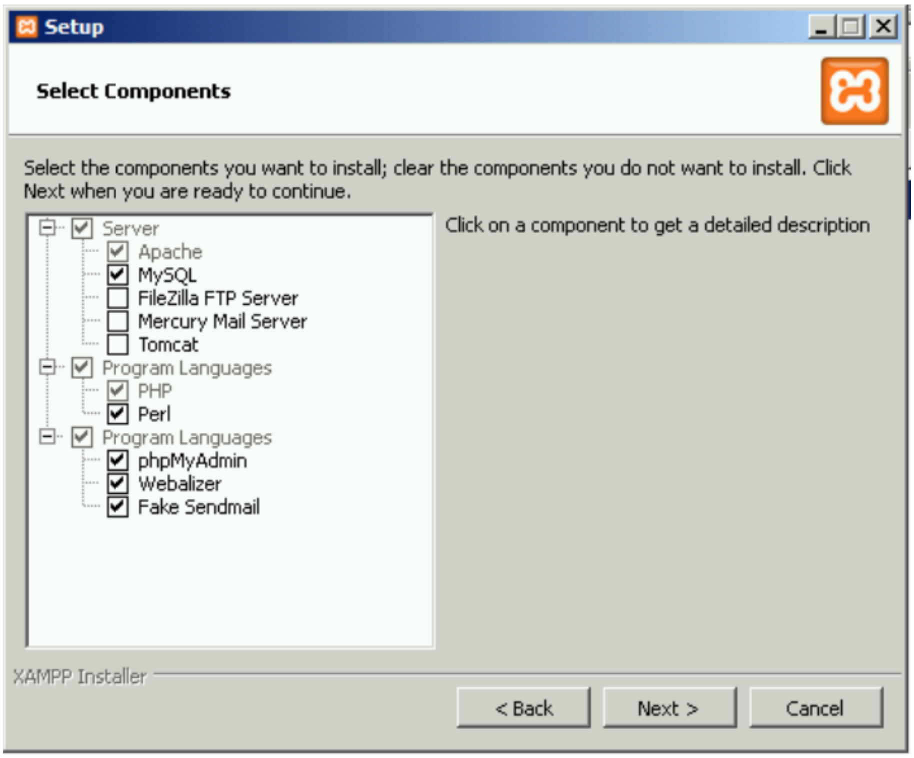


Figura 3.28: Interfaz gráfica de selección de componentes a instalar
Fuente: XAMPP 7.3.23

Al terminar el proceso de instalación aparecerá un cuadro de diálogo, el cual preguntará si quiere iniciar el panel de control de XAMPP, donde se le dirá que sí, de esta manera poder activar el servicio MYSQL, para probar que el servicio está funcionando correctamente, se abre cualquier navegador y se escribe la dirección 127.0.0.0 que es la dirección IP de localhost, como se muestra en la figura 3.29.

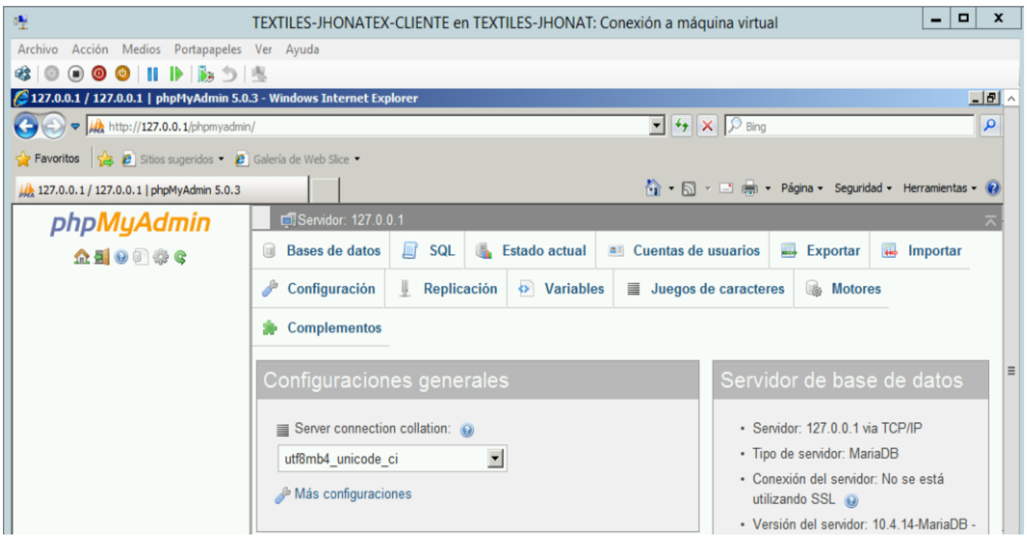


Figura 3.29: Interfaz gráfica de phpMyAdmin
Fuente: XAMPP 7.3.23

Estacion de trabajo

El equipo de cómputo utiliza el sistema operativo (S.O) Windows 7 Ultimate, a continuación, se describe las características del hardware del equipo de cómputo que simulara a una estación de trabajo de la empresa, como se muestra en la tabla 3.10.

Tabla 3.10: Características del hardware de estación de trabajo

Características
Procesador: Intel Core Duo
Memoria RAM: 4 GB
Disco duro: 500 GB

Fuente: Elaboración propia

Igualmente, la instalación de Windows 7 Ultimate, es como cualquier otra distribución de Windows, por consiguiente, no se detallará su instalación.

Una vez terminado el proceso de instalación, iniciará automáticamente como se muestra en la figura 3.30.

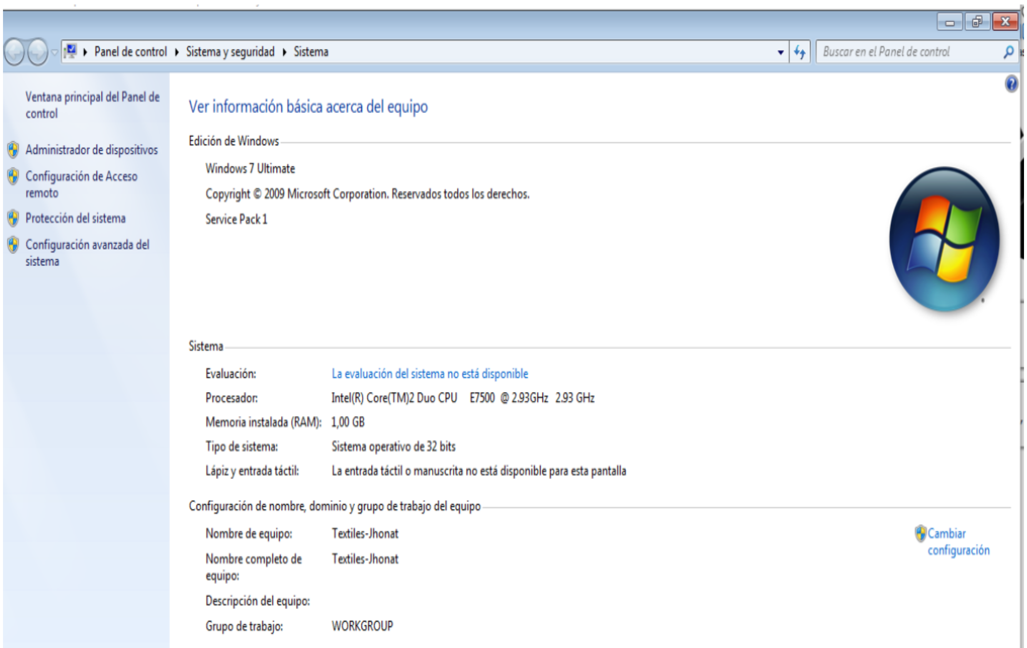


Figura 3.30: Interfaz gráfica de información del sistema
Fuente: Windows 7 Ultimate

Finalizado el proceso del ambiente simulado de la empresa Textiles Jhonatex, se observa en la figura 3.31, el entorno en el cual se realizará la evaluación de seguridad de la información, para las técnicas de descubrimiento de red y escaneo de vulnerabilidades.

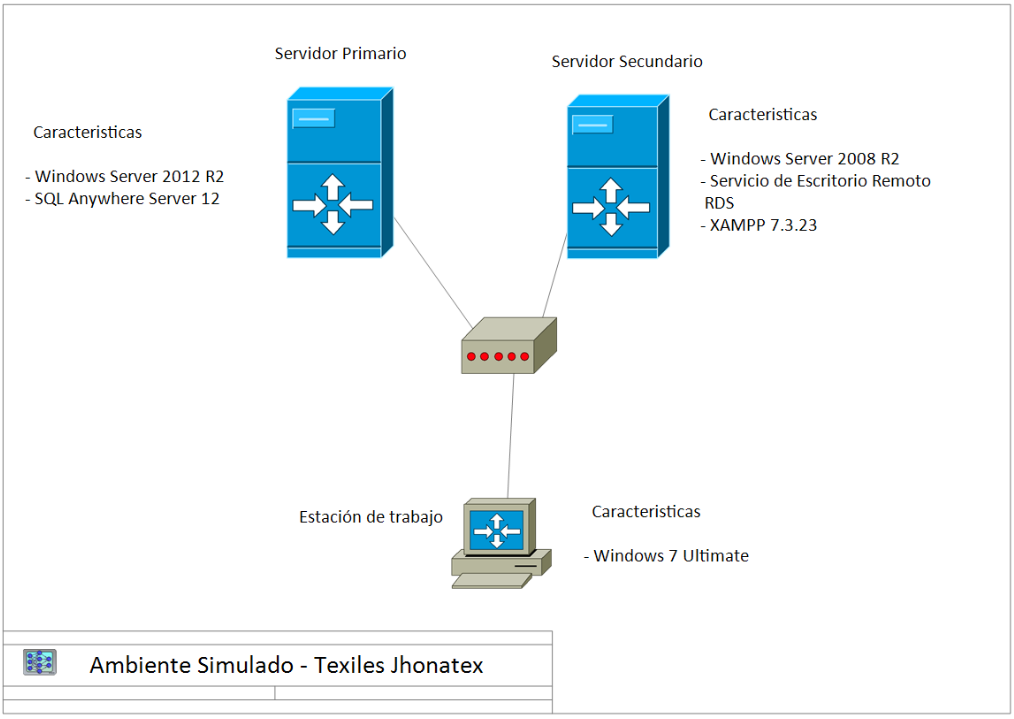


Figura 3.31: Ambiente simulado Textiles Jhonatex
Fuente: Elaboración propia

3.3.1.1. Herramienta para la identificación de vulnerabilidades

Las herramientas a utilizar se instalarán sobre el S.O Kali Linux. Estas herramientas son: Nmap, Openvas y Nessus, que se especializan en la identificación de vulnerabilidades. A continuación, se describe cada una de estas herramientas.

Kali Linux

Kali Linux fue desarrollado con el propósito de realizar pruebas de penetración y análisis forense digital, fue lanzado en 2013 por la organización Offensive Security. Se puede decir que uno de los aspectos principales de Kali Linux es su conjunto de herramientas preinstaladas con el propósito de ser utilizadas en la ciberseguridad, incluidas las pruebas de penetración y la explotación [23].

Nmap

Es una herramienta que permite realizar de manera general el análisis de red. Permitiendo diferentes tipos de análisis de puertos: las opciones incluyen análisis

SYN, FIN y ACK con ambos TCP y UDP, asimismo como escaneo ICMP [24].

Nessus

Nessus es un software comercial desarrollado y mantenido por Tenable, utilizado principalmente para evaluaciones de seguridad en la red, con el objetivo de encontrar vulnerabilidades. Ofrece diferentes licencias, una es la licencia gratuita sin embargo está limitado en el número de destinos simultáneos que se pueden escanear [25].

OpenVas

Sistema Abierto de Evaluación de Vulnerabilidades (OpenVAS) utilizado principalmente para escanear un host de destino o muchos hosts de destino en el mismo tiempo para encontrar principalmente vulnerabilidades en la red [26].

3.3.2. Ejecución y análisis

3.3.2.1. Nmap

Nmap se encuentra ya instalado en Kali Linux versión 2019.4, por lo que no es necesario la instalación del mismo. Como primer paso es necesario identificar los equipos que se encuentran en la red, se necesita la dirección de red y mascara de subred, de esta manera conocer cuántos dispositivos se encuentran en la red, la dirección de red de este ambiente simulado es la 192.168.1.0 y la máscara de subred es la 255.255.255.240, una vez identificado estos dos parámetros se usa el comando nmap -sn -v 192.168.1.0/28, como se muestra en la figura 3.32.

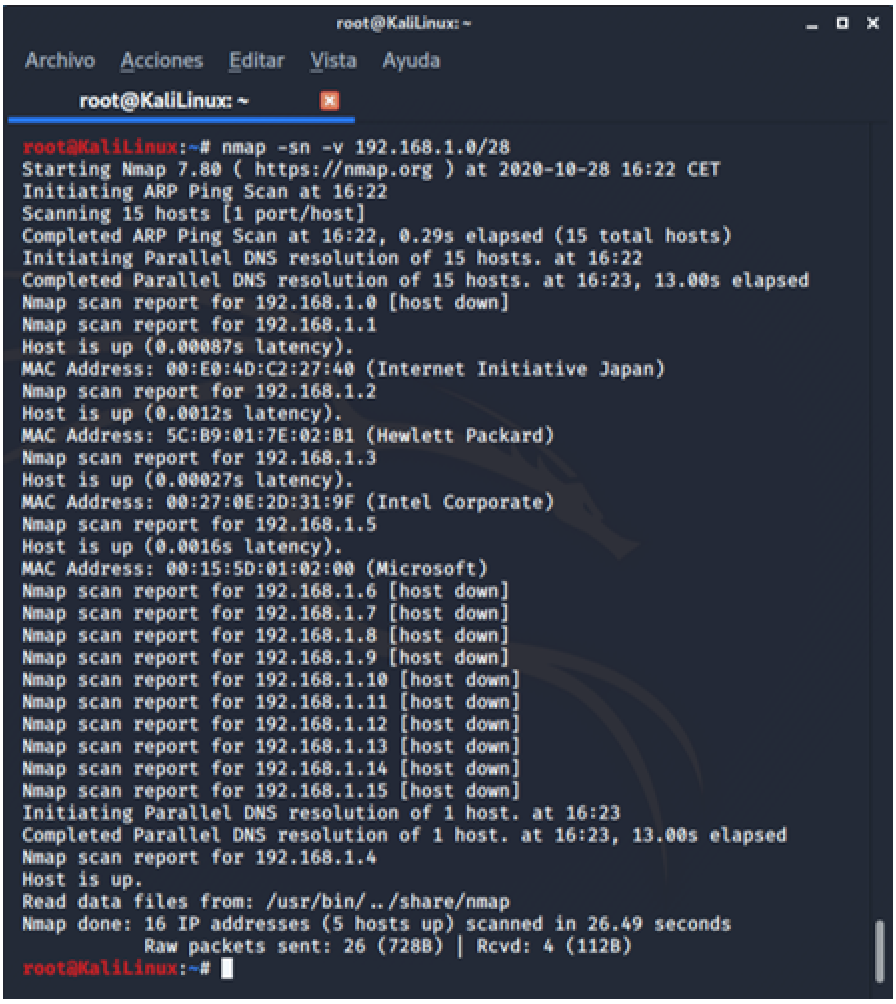


Figura 3.32: Interfaz gráfica escaneo de totalidad de host en la red
Fuente: Nmap

Tabla 3.11: Direcciones IP en la red

No	Dirección
1	192.169.1.2
2	192.168.1.5
3	192.168.1.5

Fuente: Elaboración propia a partir de Nmap

En la tabla 3.11, se muestra las 3 direcciones IP, que formaran parte de la evaluación.

Una vez identificado la IP que pertenece a cada dispositivo que se encuentra conectada a la red. Se empieza por el escaneo individual de cada IP, es importante mencionar que por defecto Nmap escanea solo los puertos del 1 al 10000, pero con la opción -p escanea todos los puertos, acompañado del 1 al 65535. Se tomará como ejemplo la primera IP identificada que es la 192.168.1.2 con el siguiente comando nmap –p 1-65535 –T4 –A –v 192.168.1.2, se realiza un escaneo del host, como se puede apreciar en la figura 3.33.

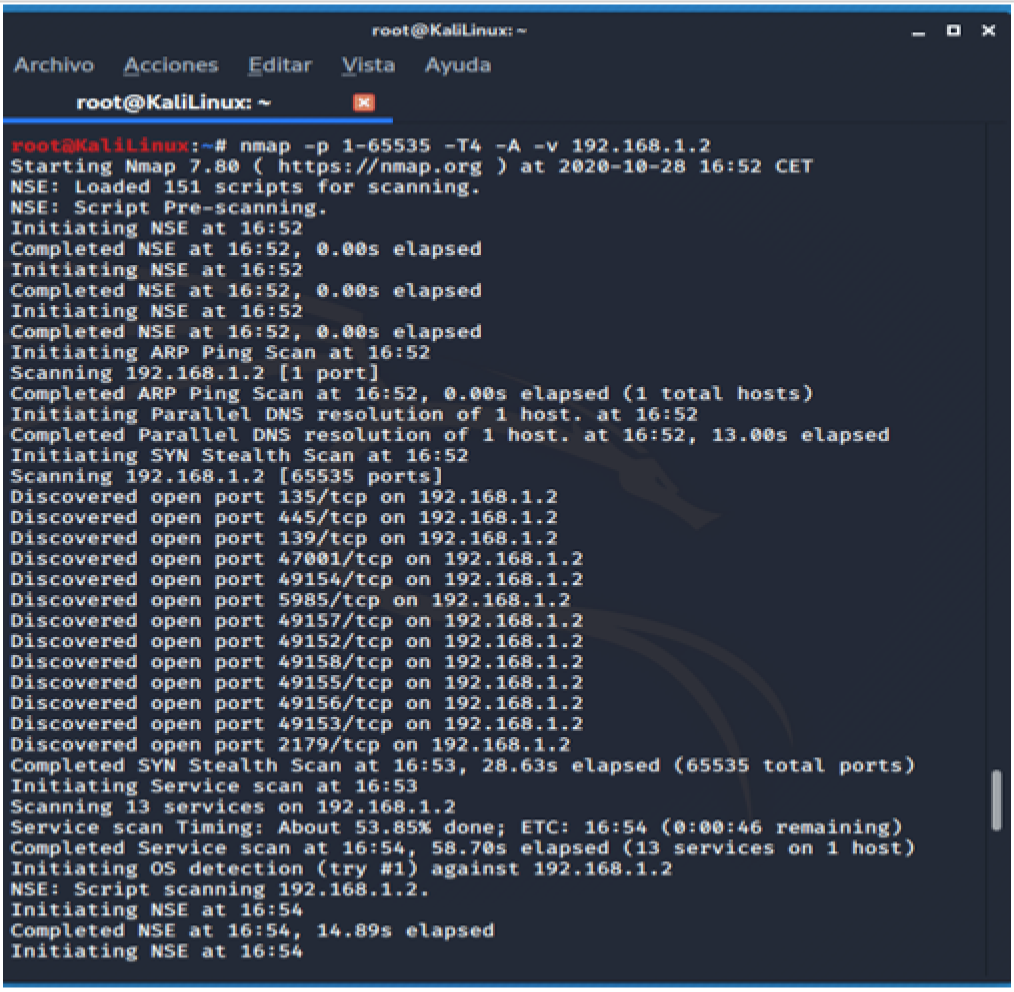


Figura 3.33: Interfaz gráfica descripción de un host en la red
Fuente: Nmap

Una vez terminado el escaneo de estos dispositivos en la red, a continuación, se describe los resultados obtenidos por cada host en la tabla 3.12, 3.13, 3.14 respectivamente.

Tabla 3.12: Listado de puertos y servicios del host 192.168.1.2

Puerto	Protocolo	Servicio	Versión
135	tcp	msrpc	Microsoft Windows RCP
139	tcp	msrpc	Microsoft Windows RCP
445	tcp	netbios-ssn	Microsoft Windows netbios-ssn
2179	tcp	microsoft-ds	Windows Server 2012 R2 – 2012 microsoft-ds
5985	tcp	vmrdp	----------
47001	tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152	tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49153	tcp	msrpc	Microsoft Windows RPC
49154	tcp	msrpc	Microsoft Windows RPC
49155	tcp	msrpc	Microsoft Windows RPC
49156	tcp	msrpc	Microsoft Windows RPC
40157	tcp	msrpc	Microsoft Windows RPC
49158	tcp	msrpc	Microsoft Windows RPC

Fuente: Elaboración propia a partir de Nmap

Tabla 3.13: Listado de puertos y servicios del host 192.168.1.5

Puerto	Protocolo	Servicio	Versión
80	tcp	http	Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.
135	tcp	msrpc	-------------
139	tcp	Netbios-ssn	-------------
443	tcp	https	Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.
445	tcp	Microsoft-ds	Microsoft Windows Server 2008 R2 - 20
3306	tcp	Mysql	-------------
3389	tcp	Ms-wbt-server	Microsoft Terminal Services
47001	tcp	Winrm	Microsoft Windows RPC
49152	tcp	msrpc	Microsoft Windows RPC
49153	tcp	msrpc	Microsoft Windows RPC
49154	tcp	msrpc	Microsoft Windows RPC
40155	tcp	msrpc	Microsoft Windows RPC
49156	tcp	msrpc	Microsoft Windows RPC

Fuente: Elaboración propia a partir de Nmap

La tabla 3.13, muestra la información de los puertos y servicios: Microsoft Windows netbios, este provee la interfaz de programación de NetBIOS sobre el protocolo TCP/IP y el Microsoft-ds es un protocolo para compartir archivos.

Tabla 3.14: Listado de puertos y servicios del host 192.168.1.6

Puerto	Protocolo	Servicio	Versión
135	tcp	msrpc	Microsoft Windows netbios-ssn
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	microsoft-ds	Windows 7 Ultimate 7061 Service Pack 1microsoft
2869	tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357	tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Fuente: Elaboración propia a partir de Nmap

La tabla 3.14, muestra la información de los puertos y servicios: Microsoft HTTPAPI httpd, es un servicio propio de Windows que implementa el protocolo Simple Service Discovery Protocol (SSDP), para administrar el recibo de los anuncios de presencia de dispositivos, y actualización del caché.

3.3.2.2. Nessus

Nessus ofrece una variedad de opciones para realizar el escaneo de vulnerabilidades, sin embargo, casi todas están bloqueadas, y solo se puede utilizar en la versión de paga, asimismo están habilitadas tres opciones de escaneo, que es la básica, la avanzada y malwares. Como se muestra en la figura 3.34.

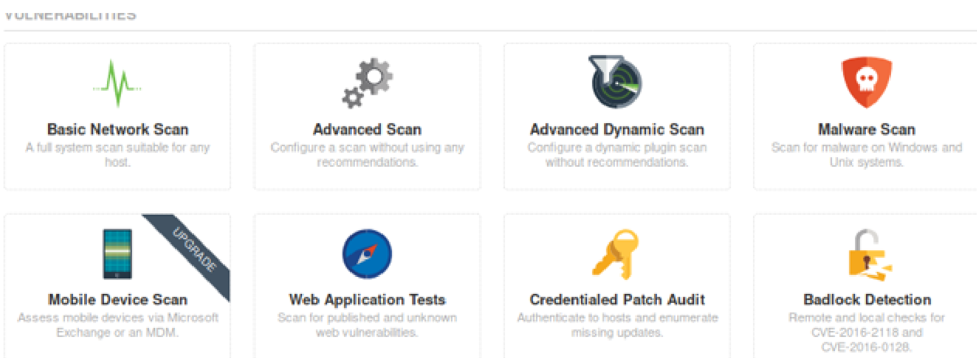


Figura 3.34: Interfaz gráfica tipos de escaneo
Fuente: Nessus

Para analizar las vulnerabilidades de la red, se realiza un escaneo avanzado, para esto se debe ingresar el nombre de la evaluación, asimismo se puede poner el detalle de la misma y escoger en que carpeta se guardara esta evaluación, y lo más importante especificar el rango de direcciones que serán escaneadas o especificar manualmente las direcciones IP, en este caso ya se identificó anteriormente las direcciones IP de los dispositivos en la red con la herramienta Nmap.

Después se guarda esta información, y se abrirá otra interfaz mostrando los escaneos ejecutados o por ejecutar, se ejecutará el escaneo anteriormente descrito, como se muestra en la figura 3.35.

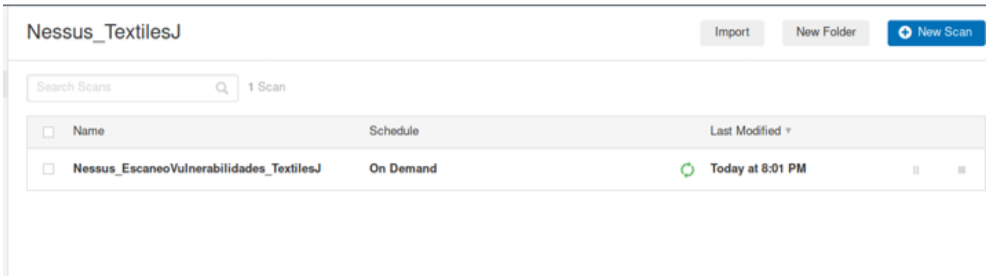


Figura 3.35: Interfaz gráfica listado de los escaneos ejecutados o por ejecutar
Fuente: Nessus

Una vez finalizado el escáner, muestra una lista con las direcciones IP conectadas a la red, asimismo muestra un gráfico de barras especificando que vulnerabilidades se encontró por cada dirección IP, las cuales se dividen en críticas, altas, medias y bajas, de igual manera muestra los resultados de forma general la totalidad de las vulnerabilidades encontradas mediante un gráfico de anillo. Como se muestra en la figura 3.36.

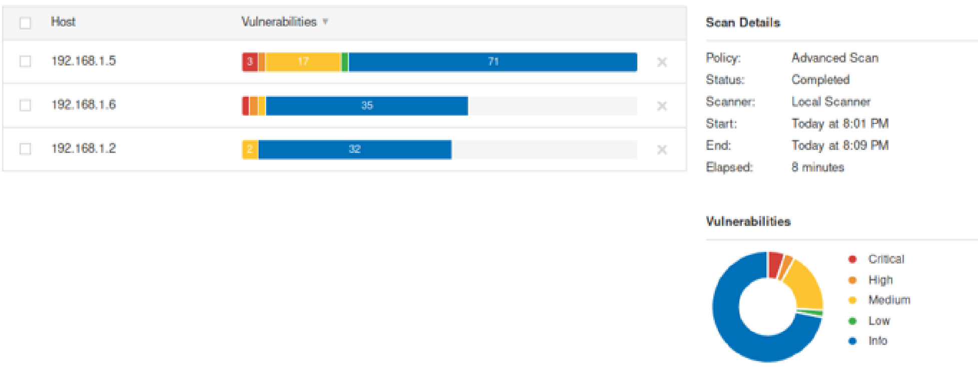


Figura 3.36: Interfaz gráfica resultado de vulnerabilidades
Fuente: Nessus

A continuación, en las tablas 3.15, 3.16, 3.17 se describe las vulnerabilidades encontradas, y las remediaciones de las mismas.

Tabla 3.15: Vulnerabilidades encontradas en el servidor principal IP: 192.168.1.2

Riesgo	Servicio	Vulnerabilidad	Descripción	Solución
Medio	Msrpc	Actualización de seguridad para protocolos remotos SAM y LSAD	El host de Windows remoto se ve afectado por una vulnerabilidad de elevación de privilegios en el Administrador de cuentas de seguridad (SAM) y protocolos de autoridad de seguridad local.	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.
Medio	Microsoft-ds	No se requiere firma SMB	No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques man-in-the-middle contra el servidor SMB.	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de política 'Microsoft servidor de red: Firmar digitalmente las comunicaciones (siempre) '. En Samba, la configuración se llama 'firma del servidor'. Ver el 'ver también' enlaces para más detalles.

Fuente: Elaboración propia a partir de los resultados obtenidos de Nessus

Tabla 3.16: Vulnerabilidades encontradas en el servidor secundario IP: 192.168.1.5

Riesgo	Servicio	Vulnerabilidad	Descripción	Solución
Critico	domain	Una vulnerabilidad en la resolución de DNS podría permitir la ejecución remota de código (2509553) (control remoto)	Una falla en la forma en que el cliente DNS de Windows instalado procesa la resolución de nombres de multidifusión local de enlaces (LLMNR). Se puede explotar de forma remota.	Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.
Critico	tcpwrappef	Una vulnerabilidad en Schannel podría permitir la ejecución remota de código	El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución remota de código debido a un procesamiento incorrecto de paquetes por el paquete de seguridad Secure Channel (Schannel).	Microsoft ha lanzado un conjunto de parches para Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1 y 2012 R2.
Critico	tcpwrappef	Windows no compatible (remoto)	A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible.	Actualice a un paquete de servicio o sistema operativo compatible
Alto	Microsoft-ds	Actualización de seguridad para Microsoft Windows SMB Server	Existen varias vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a manejo inadecuado de determinadas solicitudes.	Microsoft ha lanzado parches de emergencia para los sistemas operativos Windows que ya no compatible, incluidos Windows XP, 2003 y 8.

Medio	Apache/2.4.46	Falta HSTS en el servidor HTTPS	La falta de HSTS permite ataques de degradación, ataques man-in-the-middle de eliminación de SSL y debilita el secuestro de cookies protecciones.	Configure el servidor web remoto para usar HSTS.
Medio	Apache/2.4.46	Métodos HTTP TRACE / TRACK permitidos	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.	Deshabilite estos métodos HTTP. Consulte la salida del complemento para obtener más información.
Medio	Msrpc	Actualización de seguridad para protocolos remotos SAM y LSAD (3148527) (Badlock) (cheque sin credencial)	Las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM pueden explotar esto para forzar el nivel de autenticación.	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

Fuente: Elaboración propia a partir de los resultados obtenidos de Nessus

Tabla 3.17: Vulnerabilidades encontradas en la estación de trabajo IP: 192.168.1.6

Riesgo	Servicio	Vulnerabilidad	Descripción	Solución
Critico	Msrpc	Vulnerabilidad Sistema operativo Windows no compatible (remoto)	A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.	Actualice a un paquete de servicio o sistema operativo compatible.
Alta	Microsoft-ds	Varias vulnerabilidades de Microsoft Windows SMBv1	El host de Windows es vulnerable si el host está ejecutando una versión posterior de Windows (es decir, Windows 8.1, 10, 2012, 2012 R2, y 2016)	Aplique la actualización de seguridad de Windows 7: KB4019264
Medio	Microsoft-ds	No se requiere firma SMB	No es necesario firmar en el servidores SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques man-in-the-middle contra el servidor SMB.	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de política 'Microsoft servidor de red: Firmar digitalmente las comunicaciones (siempre) '. En Samba, la configuración se llama 'firma del servidor'.

Fuente: Elaboración propia a partir de los resultados obtenidos de Nessus

3.3.2.3. OpenVas

Se usará la versión web de esta herramienta, que es el Asistente de Seguridad Greenbone (GSA), primero se debe crear un Target(objetivo), que es la IP del host al que se realizará el escaneo, como se muestra en la figura 3.37 de la tarea creada para analizar en servidor principal, posteriormente se realiza este proceso para los otros dispositivos.

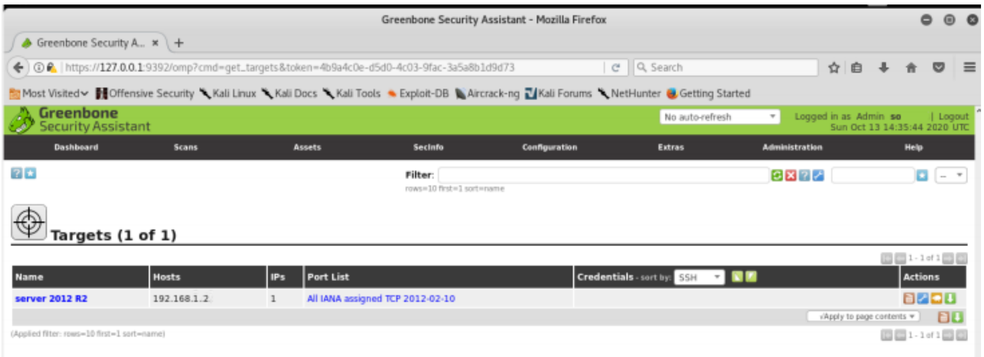


Figura 3.37: Interfaz gráfica listado de los escaneos ejecutados o por ejecutar
Fuente: Elaboración propia a partir de OpenVas

A continuación, se detalla las vulnerabilidades detectadas con OpenVas en las tablas 3.18, 3.19 y 3.20.

Tabla 3.18: Vulnerabilidades encontradas en la sercidor primario IP: 192.168.1.2

Riesgo	Servicio	Vulnerabilidad	Descripción	Solución
Medio	tcpwrapped	Se ha firmado un certificado SSL en la cadena de certificados mediante un algoritmo hash débil.	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado mediante un algoritmo hash criptográficamente débil	Pongase en contacto con una autoridad de certificación para que se vuelva a emitir el certificado.
Medio	tcpwrapped	Los servicios de Terminal Server remotos no utilizan únicamente la autenticación de nivel de red.	Los servicios de Terminal Server remotos no están configurados para utilizar únicamente la autenticación de nivel de red (NLA)	Habilitar la autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto generalmente se hace en la pestaña 'Remoto' de la configuración del 'Sistema' en Windows.

Fuente: Elaboración propia a partir de los resultados obtenidos de Openvas

Tabla 3.19: Vulnerabilidades encontradas en la sercidor secundario IP: 192.168.1.5

Riesgo	Servicio	Vulnerabilidad	Descripción	Solución
Medio	Apache/2.4.46	Métodos HTTP TRACE / TRACK permitidos	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.	Se recomiendan que los sistemas que están conectados a Internet tengan una cantidad mínima de puertos expuestos. En este caso, los puertos LLMNR deben bloquearse de Internet.
Medio	Msrpc	Los servicios de Terminal Server remotos no utilizan únicamente la autenticación de nivel de red.	Los servicios de Terminal Server remotos no están configurados para utilizar únicamente la autenticación de nivel de red (NLA). NLA utiliza el protocolo Credential Security Support Provider (CredSSP) para realizar una sólida autenticación del servidor a través de TLS / SSL o mecanismos Kerberos, que protegen contra ataques de intermediarios.	Se recomienda habilitar la autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto generalmente se hace en la pestaña 'Remoto' de la configuración del 'Sistema' en Windows.
Medio	Msrpc	El servicio remoto cifra el tráfico con una versión anterior de TLS.	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de defectos criptográficos de diseño.	Se recomienda habilitar la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.

Medio	Apache/2.4.46	Suites de cifrado de intensidad media SSL admitidas (SWEET32)	El host remoto admite el uso de cifrados SSL que ofrecen un cifrado de nivel medio Es fácil eludir el cifrado de nivel medio si el atacante esta en la misma red.	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

Fuente: Elaboración propia a partir de los resultados obtenidos de Openvas

Tabla 3.20: Vulnerabilidades encontradas en la estación de trabajo IP: 192.168.1.6

Riesgo	Servicio	Vulnerabilidad	Descripción	Solución
Critico	Msrpc	Las vulnerabilidades en el escritorio remoto podrían permitir la ejecución remota de código	La más grave de estas vulnerabilidades podría permitir la ejecución remota de código si un atacante envía una secuencia de paquetes RDP especialmente diseñados a un sistema afectado.	La mayoría de los clientes tienen habilitada la actualización automática y no necesitarán realizar ninguna acción porque esta actualización de seguridad se descargará e instalará automáticamente. Los clientes que no han habilitado la actualización automática deben buscar actualizaciones e instalar esta actualización manualmente
Critico	Microsoft-ds	Varias vulnerabilidades de Microsoft SMBv1	Existen varias vulnerabilidades de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de los paquetes SMBv1.	Aplique la actualización de seguridad de Windows 7: KB4019264

Fuente: Elaboración propia a partir de Openvas

El escaneo realizado a los tres hosts con Nessus y Openvas se determinó lo siguiente:

En el servidor secundario, el cual se encuentra instalado el servidor web Apache/2.4.46 se encontraron vulnerabilidades como HTTP TRACE/TRACK son métodos HTTP que se utilizan para la depuración de las entradas de los usuarios, mediante este se pueden realizar un ataque web del tipo XSS, permitiendo acciones como:

- Robo de sesiones
- Robo de información sensible
- Control del ordenador
- Cambio de la apariencia visual

Se evidenció que las versiones de Microsoft SMB, requieren ser actualización, debido a que ya no son compatibles con las características del servidor.

3.4. Evaluación de riesgos basado en la metodología NIST 800-30

3.4.1. Introducción

La evaluación de riesgos se la puede llevar a cabo de diferentes maneras y con cierto grado de detalle, esto depende de la metodología escogida como de los activos que formaran parte de evaluación y su valor dentro de la empresa.

En esta parte se realizará la evaluación de riesgos y para lo cual se necesita los controles que tiene implementado dentro de la organización, asimismo se identificara, estimara y se evaluara los activos, con el objetivo de identificar las amenazas y vulnerabilidades existentes dentro de la empresa Textiles Jhonatex, para finalmente determinar controles que se debería implementar para mitigar los riesgos.

Mediante el análisis que se obtuvo de la situación actual de la empresa referente a la seguridad de la información y la evaluación de seguridad de la información previamente realizada, se puede establecer criterios que se utilizaran en el proceso de la evaluación de riesgos para tomar decisiones, principalmente para determinar los controles que deberían ser implementados.

3.4.2. Alcance y límites

El análisis de riesgo que se presentará posteriormente comprende los activos del departamento de sistemas, los cuales son de mayor prioridad, puesto que almacenan y administran información de vital importancia para la empresa, por tal motivo es esencial salvaguardar estos activos de información mediante salvaguardias que permitan mitigar el riesgo para su correcto funcionamiento.

EL análisis se lo realiza con el propósito de identificar que activos son de vital importancia dentro de la empresa, de igual manera conocer que vulnerabilidades y amenazas estos se encuentran expuestos.

3.4.3. Enfoques de evaluación

Los enfoques de evaluación hacen referencia a la estimación del riesgo, se lo puede realizar de manera cualitativa, cuantitativa o la combinación de estas dos, dependiendo del grado de detalle que se desea analizar, asimismo de la información que se disponga.

El enfoque de evaluación será de manera cualitativa haciendo referencia con base en los niveles para determinar la probabilidad y la magnitud del impacto en calificativos como, por ejemplo: Alto, Medio, Bajo.

La ventaja de este enfoque es su facilidad de comprensión sobre lo que se está realizando.

3.4.4. Análisis de riesgo

El objetivo del análisis de riesgos es identificar los activos que hacen funcionar a la empresa en sus labores diarias e identificar que amenazas atentan con el funcionamiento normal de estas, además de evaluar el nivel impacto que podría causar, y las salvaguardias que se deben tomar para eliminar o mitigar el impacto de los riesgos existentes.

Como primer paso se necesita determinar los activos que proporcionan servicios a través de la red de datos de la empresa Textiles Jhonatex, hacia los empleados de las diferentes áreas de la misma, siendo internos y/o externos, de igual forma a que amenazas se encuentran expuesto y las vulnerabilidades que podrían explotar causando impactos adversos si no se cuenta con salvaguardias adecuadas.

3.4.4.1. Identificación de Activos

La identificación de activos de la empresa es la parte crucial que permitirá catalogar la criticidad de los mismos.

La identificación de activos ya se lo realizó anteriormente en el paso de inventario de la empresa de Textiles Jhonatex, sin embargo, esto se lo realizó de toda la organización, en la tabla 3.21, se muestra los activos que corresponde al departamento de sistemas.

Tabla 3.21: Inventario del departamento de sistemas

Categoría	Descripción	Herramientas
Hardware	Se refiere a los dispositivos que brinda soporte informático.	Servidor principal Windows server 2012 R2
		Servidor secundario Windows server 2008
		Pc Windows 7
Software	Son aquellos programas, que permiten la administración de los datos.	Sistema de gestión del personal sin nombre
		Sistema contable Microplus
Red	Se refiere a los dispositivos que permiten la interconexión con otros dispositivos, en un sistema de información.	Central telefónica
		Router ap (Access Point)
		Router frontera
		Switch
		Dvr
Personal	Todas las personas que pertenecen al departamento de sistemas	Gerente de Sistemas

Fuente: Elaboración propia a partir del inventario de la empresa

Criticidad activos

Una vez identificado estos activos, se necesita la valoración de estos por su nivel de impacto en la organización, para esto se hará uso de la valoración de dimensiones que se divide en la disponibilidad, integridad y confidencialidad, con el propósito de generar criterios de valoración como se muestra a continuación.

Dimensiones de valoración

Al hablar de las dimensiones de valoración se debe considerar la disponibilidad, confidencialidad y la integridad que son características esenciales de un activo valioso dentro de una organización, para esto se hará uso de la metodología Magerit, puesto que la metodología NIST 800-30 no establece estas dimensiones.

[D] Disponibilidad

La disponibilidad de los activos hace referencia a la importancia que tiene el activo, si no se encontrara disponible causado por una fuente de amenaza.

[I] Integridad

Esta propiedad consiste en conocer el valor de importancia si los datos fueran modificados de manera no autorizada, teniendo en cuenta las consecuencias que conllevaría.

[C] Confidencialidad

Esta característica consiste en identificar la importancia de la información, si esta se divulga a individuos o entidades no autorizadas, causando daños graves a la organización o por lo contrario estos carecen de un valor si fueran revelados [27].

Criterios de valoración

Teniendo en cuenta las dimensiones de valoraciones para estos activos, se debe seguir con los criterios de valoración, para esto se usará la valoración de bajo, medio y alto, puesto que el enfoque de evaluación es de manera cualitativa, evitando confusiones a la hora de la valoración.

La tabla 3.22, se muestra a continuación, ayudará a tener más claros criterios de valoración para los activos.

Tabla 3.22: Criterios de Valoración

Valoración	Criterio de Valoración
Alto	El daño sería muy grave, probablemente ocasionando que la empresa deje de funcionar por un tiempo considerable.
Medio	El daño sería importante, probablemente ocasionaría que la empresa deje de funcionar por un corto periodo de tiempo.
Bajo	El daño sería menor, probablemente ocasionaría molestias menores en las funciones normales de la empresa.

Fuente: Elaboración propia a partir de [27]

Una vez realizado este análisis, se procede a la valoración de los activos que pertenecen al departamento de sistemas, para medir el grado de criticidad de los activos se lo realizará mediante la guía de gestión y clasificación de activos de la información, publicada por Mintic, para esto se hará uso de las dimensiones anteriormente descritas.

La tabla 3.23, que se muestra a continuación determinara como calcular el valor del activo.

Tabla 3.23: Criterios de Valoración

Alto	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
Medio	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
Bajo	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Elaboración propia a partir de [28]

A continuación, en la tabla 3.24, se muestra la valoración de criticidad de los activos.

Tabla 3.24: Valoración de activos críticos

	[D]	[I]	[C]	Nivel de criticidad
Servidor principal Windows server 2012 R2	Alto	Alto	Medio	Alto
Servidor secundario Windows server 2008	Medio	Medio	Alto	Medio
PC Windows 7	Medio	Bajo	Bajo	Medio
Sistema de gestión del personal sin nombre	Medio	Alto	Medio	Medio
Sistema contable Microplus	Medio	Alto	Medio	Medio
Router ap	Medio	Bajo	Bajo	Medio
Central telefónica	Medio	Bajo	Bajo	Medio
Router ap (Access Point)	Bajo	Bajo	Bajo	Bajo
Router frontera	Medio	Bajo	Medio	Medio
Switch	Medio	Medio	Medio	Medio
Dvr	Medio	Bajo	Bajo	Bajo
Gerente de Sistemas	Medio	Bajo	Bajo	Medio

Especificación de fuentes de amenaza

El NIST define una amenaza como "el potencial de una fuente de amenaza para ejercer (activar accidentalmente o explotar intencionalmente) una vulnerabilidad específica". Además, establece que una fuente de amenaza “ya sea (1) la intención y el método dirigido a la explotación intencional de una vulnerabilidad o (2) una situación y un método que puede desencadenar accidentalmente una vulnerabilidad”.

NIST SP 800-30, ofrece una taxonomía de fuentes de amenaza que pueden aplicarse a la empresa, asimismo, agrupados por el tipo la amenaza.

Aplicabilidad de fuentes de amenaza adversa

Una fuente de amenaza adversa está relacionada directamente con individuos, grupos, organizaciones o la nación, que buscan explotar la dependencia de la organización de los recursos cibernéticos (es decir, información en forma electrónica, tecnologías de información y comunicaciones, las capacidades de comunicación y manejo de información proporcionadas por esas tecnologías). A continuación, se presenta en la tabla 3.25, la aplicabilidad de las fuentes de amenaza adversa, relevantes para la empresa Textiles Jhonatex [17].

Tabla 3.25: Amenazas adversas

Subtipo	Fuente de amenaza	Aplica
Individuos	Agente externo	Si
	Agente interno	Si
Grupo	Ad hoc	No
	Establecido	No
Organización	Competidor	No
	Proveedor	No
	Socio	No
	Cliente	No

Fuente: Elaboración propia a partir de [17]

Aplicabilidad de fuentes de amenaza accidental

Una fuente de amenaza accidental se relaciona de forma directa con acciones erróneas tomadas por individuos en el curso de la ejecución de sus responsabilidades cotidianas. A continuación, se presenta en la tabla 3.26, la aplicabilidad de las fuentes de amenaza accidental.

Tabla 3.26: Amenazas accidentales

Subtipo	Fuente de amenaza	Aplica
Humana	Usuario	No
	Administrador	Si

Fuente: Elaboración propia a partir de [17]

Aplicabilidad de fuentes de amenaza estructural

Una fuente de amenaza estructural se relaciona de forma directa con las fallas de equipos, controles ambientales o software debido al envejecimiento, agotamiento de recursos u otras circunstancias que exceden los parámetros operativos esperados. A continuación, se presenta en la tabla 3.27, la aplicabilidad de las fuentes de amenaza accidental.

Tabla 3.27: Amenazas estructurales

Subtipo	Fuente de amenaza	Aplica
Tecnología	Equipos de tecnología de la información	Si
Controles ambientales	Controles de temperatura / humedad	Si
	Fuente de alimentación	No
Software	Sistema operativo	Si
	Redes	Si
	Aplicación de uso general	Si

Fuente: Elaboración propia a partir de [17]

Aplicabilidad de fuentes de amenaza organizacionales

Una fuente de amenaza organizacional se relaciona de forma directa con las políticas, controles, planes que se encuentren incompletos, desactualizados o carezcan de los mismos, como se muestra en la tabla 3.28.

Tabla 3.28: Amenazas estructurales

<table>
<tr><td>Subtipo</td><td>Fuente de amenaza</td><td>Aplica</td></tr>
<tr><td rowspan="2">Regulaciones</td><td>Planes de contingencia</td><td>Si</td></tr>
<tr><td>Políticas de seguridad</td><td>Si</td></tr>
</table>

Fuente: Elaboración propia a partir de [17]

Aplicabilidad de fuentes de amenaza natural

Una fuente de amenaza natural se relaciona de forma directa con los desastres naturales y fallas de las infraestructuras críticas de las que depende la organización, pero que están fuera del control de la organización. A continuación, se presenta en la tabla 3.29, la aplicabilidad de las fuentes de amenaza natural.

Tabla 3.29: Amenazas naturales

<table>
<tr><td>Subtipo</td><td>Fuente de amenaza</td><td>Aplica</td></tr>
<tr><td rowspan="5">Desastres naturales o provocados por el hombre</td><td>Fuego</td><td>No</td></tr>
<tr><td>Inundación / Tsunami</td><td>No</td></tr>
<tr><td>Tormenta de viento / Tornado</td><td>No</td></tr>
<tr><td>Huracán</td><td>No</td></tr>
<tr><td>Terremoto</td><td>No</td></tr>
<tr><td rowspan="3">Evento natural</td><td>Falla / corte de infraestructura</td><td>No</td></tr>
<tr><td>Telecomunicaciones</td><td>No</td></tr>
<tr><td>Energía eléctrica</td><td>No</td></tr>
</table>

Fuente: Elaboración propia a partir de [17]

Especificación de eventos de amenaza con sus fuentes de amenaza

Los eventos de amenaza son originados por fuentes de amenaza. Una amenaza se caracteriza como una situación o evento con la capacidad de impactar de forma adversa los activos de la organización, procesos, personal, o a los sistemas de información por medio del acceso no autorizado, alteración, destrucción de información o el más común “denegación de servicio” o por una situación y un método que puede desencadenar accidentalmente una vulnerabilidad. Basado en los criterios definidos por la metodología NIST SP 800-30, se define los posibles eventos de amenaza. Se muestra en la tabla 3.30, 3.31, 3.32, 3.33 respectivamente por el tipo de fuente se amenaza anteriormente descrito [17].

Tabla 3.30: Eventos de amenaza adversa

Fuentes de amenaza	Eventos de amenazas
Agente externo	Realice reconocimiento / escaneo de red perimetral
	Realice el rastreo de la red de redes expuestas.
	Realizar reconocimiento y vigilancia de organizaciones específicas.
	Recopile información utilizando el descubrimiento de código abierto de información organizacional.
	Ataques de phishing.
	Ataques basados específicamente en el entorno de tecnología de información implementada.
	Elaboración de certificados de seguridad falsos.
	Obtener información confidencial a través del rastreo de redes externas.
	Crear sitio web falsificado / falso.
	Causar pérdida de integridad al crear, eliminar y / o modificar datos en sistemas de información de acceso público.
	Causar pérdida de integridad al contaminar o corromper los datos críticos.
Agente Interno	Realice reconocimiento / escaneo de red perimetral.
	Causar el deterioro / destrucción de los componentes y funciones críticos del sistema de información.
	Obtener información robando o eliminando de manera oportunista sistemas / componentes de información.
	Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados.
	Causar el deterioro / destrucción de los componentes y funciones críticos del sistema de información.
	Obtenga información robando o eliminando de manera oportunista sistemas / componentes de información.

Fuente: Elaboración propia a partir de [17]

Tabla 3.31: Eventos de amenaza accidentales

Fuente de amenaza	Eventos de amenaza
Administrador	Derrame información sensible.
	Mal manejo de información crítica y / o sensible.
	Ingeniería Social.
	Configuración de privilegios incorrecta.
	Introducción de vulnerabilidades en productos de software.

Fuente: Elaboración propia a partir de [17]

Tabla 3.32: Eventos de amenaza accidentales estructurales

Fuente de amenaza	Eventos de amenaza
Equipos tecnológicos	Deterioro total o parcial de equipos tecnológicos.
	Errores de componentes.
	Perdida de total o parcial.
Controles Ambientales	Falla en su función provocando el sobrecalentamiento del equipo.
Sistema Operativo	Perdida de la integridad de la información.
	Fallos en el sistema.
Red	Inoperatividad en los procesos de la empresa por falta de comunicación entre los equipos tecnológicos.
	Falla del servicio de Internet.

Fuente: Elaboración propia a partir de [17]

Tabla 3.33: Eventos de amenaza accidentales organizacional

Fuente de amenaza	Eventos de amenaza
Regulaciones	Gastos monetarios considerables.
	Mayor tiempo empleados para la recuperación ante una eventualidad de carácter adverso.

Fuente: Elaboración propia a partir de [17]

Identificación de vulnerabilidades

NIST define la vulnerabilidad como "Una falla o debilidad en los procedimientos de seguridad del sistema, el diseño, la implementación o los controles internos que podrían ser ejercitados (activados accidentalmente o explotados intencionalmente) y resultar en una brecha de seguridad o una violación en las políticas de seguridad" [17]. Para este paso se puede hacer uso de resultados de auditorías, evaluaciones de seguridad, evaluaciones de riesgos anteriormente realizadas.

Mediante entrevistas y la evaluación de seguridad técnica anteriormente realizada, se obtuvo las siguientes vulnerabilidades que pueden ser explotadas por una o varias fuentes de amenaza, como se muestra en la tabla 3.34.

Tabla 3.34: Vulnerabilidades/amenazas

Categoría	Código	Vulnerabilidad	Fuentes de amenaza
Hardware	V01	Falta de revisión y monitoreo de los servidores.	Equipos Tecnológicos
	V02	Calentamiento en los servidores por falta de un sistema de ventilación.	Controles Ambientales
Software	V03	Para la implementación de un nuevo servicio, no se evidencia un previo análisis.	Agente externo, Administrador
	V04	Desconocimiento de las vulnerabilidades actuales en las aplicaciones.	Sistema Operativo, Aplicaciones de uso general, Agente externo
Red	V05	No se evidencia monitoreos continuos en la red.	Agente externo
Personal	V06	Insuficiente capacitación referente al tema de seguridad de la información.	Administrador, Agente externo
	V07	Los respaldos que se realizan de su sistema Microplus no se realizan de manera formal.	Regulaciones
	V08	No se evidencia bitácoras.	Regulaciones

Fuente: Elaboración propia

Análisis de controles

Este paso se lo realiza para analizar los controles implementados en la organización, con el objetivo de mitigar o eliminar la probabilidad de que una o varias fuentes de amenaza explote una vulnerabilidad en los sistemas de información.

El departamento de sistemas la empresa Textiles Jhonatex, actualmente no tiene establecidas políticas de seguridad que garanticen la seguridad de la información dentro de la empresa, existen algunos controles que están implementados como parte de la seguridad, los cuales deberían estar dentro de una política estructurada para la seguridad de la información.

A continuación, se detalla los controles implementados por la empresa, para los equipos, manejo de información y control físico, en la tabla 3.35, 3.36 y 3.37 respectivamente.

Tabla 3.35: Controles para los equipos de Textiles Jhonatex

Código	Controles de los Equipos de Textiles Jhonatex
C01	Los equipos que forman parte de la red Textiles Jhonatex, independientemente del área al que pertenezca, tendrá asignado un NOMBRE DE EQUIPO y pertenecerá a un GRUPO DE TRABAJO.
C02	Cada estación de trabajo es de uso exclusivo de la persona a la que se le asigno el equipo.
C03	Se prohíbe el uso redes sociales como Facebook, Messenger, WhatsApp, a excepción de las personas autorizadas.
C04	Prohibido descargar programas provenientes del internet.
C05	Se realiza el mantenimiento de los equipos de cómputo se lo realizan semestralmente, o mínimo una vez al año.
C06	El daño total o parcial del equipo, causado por mal uso o negligencia, por parte del empleado de la empresa, deberá cubrir el monto económico del mismo.
C07	Prohibido usar memorias USB, no pertenecientes a la empresa.

Fuente : Elaboración propia a partir de los controles de la empresa

Tabla 3.36: Controles para el manejo de la información de Textiles Jhonatex

Código	Controles de los Equipos de Textiles Jhonatex
C08	Se prohíbe la divulgación intencionada de información que sea de carácter sensible de la empresa.
C09	El respaldo de la información generada diariamente por el sistema contable Microplus, se lo realiza manualmente, a través de un medio de almacenamiento extraíble.

Fuente: Elaboración propia a partir de los controles de la empresa

Tabla 3.37: Controles de seguridad física de Textiles Jhonatex

Código	Controles de los Equipos de Textiles Jhonatex
C10	No se permite el uso de celulares personales dentro de la empresa, solo se usan lo proporcionado por la misma, para las diferentes actividades del personal.
C11	La empresa se encuentra salvaguardada por un conjunto de cámaras, por todas las áreas que conforma la misma.
C12	Se permite el ingreso a las instalaciones, una vez identificada su identidad por el guardia de seguridad.

Fuente: Elaboración propia a partir de los controles de la empresa

3.4.5. Ejecución de la evaluación de riesgos

La evaluación de riesgos es "el proceso de identificar los riesgos para la seguridad del sistema y determinar la probabilidad de que sean explotadas por una fuente de amenaza, el impacto resultante y los controles adicionales que mitigarían o eliminarían ese impacto".

Determinación de probabilidad

La determinación de probabilidad tiene como objetivo determinar una calificación de probabilidad de que una vulnerabilidad pueda explotarse mediante una o varias amenazas asociadas a esta.

Para determinar la probabilidad se considera el siguiente punto tomado de NIS 800-30.

- Condiciones predisponentes

Condición predisponente. - Una condición predisponente es una condición que existe dentro de una organización, una misión o proceso de negocio, arquitectura empresarial, sistema de información o entorno de operación, que afecta (es decir, aumenta o disminuye) la probabilidad de que los eventos de amenaza, una vez iniciados, tengan un impacto adverso en las operaciones de la organización, activos o individuos [17].

Para calificar las vulnerabilidades con su probabilidad de ocurrencia, se los determina mediante el criterio de la NIST 800-30, como se muestra en la tabla 3.38.

Tabla 3.38: Criterio para determinar la probabilidad de una vulnerabilidad

Nivel de probabilidad	Definición de probabilidad
Alto	Las condiciones predisponentes no previenen que las vulnerabilidades sean explotadas.
Medio	Las condiciones predisponentes previenen que las vulnerabilidades sean explotadas.
Bajo	Las condiciones predisponentes impiden que las vulnerabilidades sean explotadas.

Fuente: Elaboración propia a partir de [17]

Probabilidad de las vulnerabilidades

Con el criterio de evaluación, mostrada en la tabla se inicia con el proceso de dar un nivel a la probabilidad de cada vulnerabilidad, anteriormente identificada.

VO1. Falta de revisión y monitoreo de los servidores.

Al no realizar revisiones y monitoreos continuos en los servidores pueden dañarse sus componentes de forma parcial o total, debido a su función pasan casi todo el tiempo de su vida útil encendidos., por lo que su probabilidad de ocurrencia es Medio.

VO2. Calentamiento en los servidores por falta de un sistema de ventilación.

El servidor se encuentra en el área de sistemas en un ambiente para mejorar el área de trabajo, sin embargo, este no posee un sistema de ventilación o un lugar adecuado, específico para el servidor, por tal motivo la probabilidad de ocurrencia es Medio.

V03. Para la implementación de un nuevo servicio, no se evidencia un previo análisis.

La implementación de un nuevo servicio sin un análisis previo, provocaría la incompatibilidad con los otros sistemas implementados en el servidor o vulnerabilidades dentro del mismo, por lo que la probabilidad de ocurrencia es: Alto.

V04. Desconocimiento de las vulnerabilidades actuales en las aplicaciones.

Generalmente las aplicaciones vienen con vulnerabilidades no descubiertas, puesto que, al no evidenciarse una planificación de las mismas en cuanto a gestión de vulnerabilidades, estas se encuentran latentes en las aplicaciones, por lo que la probabilidad de ocurrencia es: Alto.

VO5. No se evidencia monitoreos continuos en la red.

Este tipo de vulnerabilidad puede ser explotada por un agente externo, el encargado del departamento de sistemas lo ha realizado más por experiencia que por una política, de esta manera la probabilidad de ocurrencia es: Medio.

V06. Insuficiente capacitación referente al tema de seguridad de la información.

El encargado del área de sistemas podría ocasionar accidentalmente, la aparición de nuevas vulnerabilidades en los sistemas de información, divulgación de información sensible, ocasionado por no contar con capacidades necesarias, por tal motivo la probabilidad de que ocurra es: Medio.

V07. Los respaldos que se realizan de su sistema Microplus no se realizan de manera formal.

No se evidenció un proceso formal de respaldo de la información, sin embargo, existe el control C09, por lo que la probabilidad de que ocurra es: Bajo.

V08. No se evidencia bitácoras

AL no evidenciarse ningún tipo de bitácora en los activos del departamento de sistemas, no se conoce el estado en el que se encuentra los mismos, por lo que la probabilidad de ocurrencia es: Alto.

En la tabla 3.39, se visualiza el resumen de la valoración de la probabilidad de cada vulnerabilidad.

Tabla 3.39: Probabilidad de las vulnerabilidades

Categoría	*Vulnerabilidad*	*Probabilidad*
Hardware	*Falta de revisión y monitoreo de los servidores.*	*Medio*
	Calentamiento en los servidores por falta de un sistema de ventilación.	*Medio*
Software	*Para la implementación de un nuevo servicio, no se evidencia un previo análisis.*	*Alto*
	Desconocimiento de las vulnerabilidades actuales en las aplicaciones.	*Alto*
Red	*No se evidencia monitoreos continuos en la red.*	*Medio*
Personal	*Insuficiente capacitación referente al tema de seguridad de la información.*	*Medio*
	Los respaldos que se realizan de su sistema Microplus no se realizan de manera formal.	*Alto*
	No se evidencia bitácoras.	*Bajo*

Fuente : Elaboración propia

Determinación del Impacto

El nivel de impacto según la NIST 800-30, se la puede medir según el criterio de evaluación, como se muestra en la tabla 3.40.

Tabla 3.40: Criterio de valoración de la magnitud del impacto

Nivel de impacto	Definición
Alto	Las vulnerabilidades causan efectos adversos sobre las operaciones organizacionales, los activos organizacionales, o individuos, estos podrían ser: (i) pérdida de la capacidad de la misión en una medida y duración que la organización no puede realizar una o más de sus funciones principales; (ii) provocar daños importantes a los activos de la organización; (iii) resultar en una pérdida financiera importante.
Medio	Las vulnerabilidades causan efectos adversos sobre las operaciones organizacionales, los activos organizacionales, o individuos, estos podrían ser: (i) causar una degradación significativa en la capacidad de la misión en la medida y duración que la organización pueda realizar sus funciones principales, pero la efectividad de las funciones se reduce significativamente; (ii) provocar daños significativos a los activos de la organización; (iii) resultar en una pérdida financiera significativa.
Bajo	Las vulnerabilidades causan efectos adversos sobre las operaciones organizacionales, los activos organizacionales, o individuos, estos podrían ser: (i) causar una degradación en la capacidad de la misión en la medida en que la organización pueda realizar sus funciones principales, pero la efectividad de las funciones se reduzca notablemente; (ii) ocasionar daños menores a los activos de la organización; (iii) resultar en una pérdida financiera menor.

Fuente : Elaboración propia a partir de [17]

Una vez establecido estos criterios, y mediante el análisis previo de los activos críticos de la empresa, se calificará el impacto de estas vulnerabilidades en los mismos, como se muestra a continuación en la tabla 3.41.

Impacto de las vulnerabilidades

Tabla 3.41: Impacto de las vulnerabilidades

Categoría	Vulnerabilidad	Impacto
Hardware	Falta de revisión y monitoreo de los servidores.	Alto
	Calentamiento en los servidores por falta de un sistema de ventilación.	Alto
Software	Para la implementación de un nuevo servicio, no se evidencia un previo análisis.	Alto
	Desconocimiento de las vulnerabilidades actuales en las aplicaciones.	Medio
Red	No se evidencia monitoreos continuos en la red.	Medio
Personal	Insuficiente capacitación referente al tema de seguridad de la información.	Medio
	Los respaldos que se realizan de su sistema Microplus no se realizan de manera formal.	Medio
	No se evidencia bitácoras.	Medio

Fuente : Elaboración propia

Determinación de Riesgo

El objetivo es determinar el riesgo de estas vulnerabilidades en la empresa Textiles Jhonatex. Para conocer cuáles son las de mayor preocupación que deberían ser tratadas, a continuación, se determinara el nivel de riesgo haciendo uso de la tabla 3.42, propuesta por la NIST 800-30 para el cálculo del riesgo.

Tabla 3.42: Criterio de calificación para determinar el riesgo

Probabilidad	Impacto		
	Bajo (10)	Medio (50)	Alto (100)
Alto (1.0)	Baja 10 x 1.0 = 10	Medio 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Medio (0.5)	Baja 10 x 1.5 = 10	Medio 50 x 0.5 = 25	Media 100 x 0.5 = 50
Bajo (0.1)	Baja 10 x 0.1 = 1	Baja 50 x 1.0 = 5	Baja 100 x 1.0 = 10

Fuente : Elaboración propia a partir de [17]

A continuación, en la tabla 3.43, se muestra los riesgos, asociados con las vulnerabilidades y sus fuentes de amenaza, con la probabilidad de que estas fueran explotadas y el impacto que ocasionaría en la empresa.

Tabla 3.43: Valoración del Riesgo

Categoría	Vulnerabilidad	Probabilidad	Impacto	Riesgo
Hardware	Falta de revisión y monitoreo de los servidores.	Medio	Alto	Medio
	Calentamiento en los servidores por falta de un sistema de ventilación.	Medio	Alto	Medio
Software	Para la implementación de un nuevo servicio, no se evidencia un previo análisis.	Alto	Alto	Alto
	Desconocimiento de las vulnerabilidades actuales en las aplicaciones.	Alto	Medio	Medio
Red	No se evidencia monitoreos continuos en la red.	Medio	Medio	Medio
Personal	Insuficiente capacitación referente al tema de seguridad de la información.	Medio	Medio	Medio
	Los respaldos que se realizan de su sistema Microplus no se realizan de manera formal.	Alto	Medio	Medio
	No se evidencia bitácoras.	Bajo	Bajo	Bajo

Fuente: Elaboración propia

Recomendación de controles

Una vez identificado las vulnerabilidades con el nivel de riesgo, se inicia con el tratamiento de las mismas, las cuales se dará recomendaciones de mitigación, clasificándoles por el nivel de prioridad. A continuación, estas remediaciones se las describe en la tabla 3.44.

Tabla 3.44: Controles para mitigar las vulnerabilidades encontradas

Riesgo	Vulnerabilidad	Recomendación
Alto	Para la implementación de un nuevo servicio, no se evidencia un previo análisis.	Se recomienda realizar un análisis previo de servicios implementados en el departamento de sistemas, mediante el uso de un ambiente controlado, para conocer cómo sería el comportamiento de este en la empresa, mediante el uso de técnicas de evaluación y de esta manera, generar un reporte del impacto que ocasionaría el mismo.
Medio	Calentamiento en los servidores por falta de un sistema de ventilación.	Se sugiere un área específicamente para el servidor de la empresa, que cuente con un sistema de ventilación adecuado, dependiendo del tipo de servidor.
Medio	Falta de revisión y monitoreo de los servidores.	Crear una política de seguridad, especificando que persona debe estar a cargo del mismo y el tiempo que debe realizar las revisiones y monitoreo.
Medio	Insuficiente capacitación referente al tema de seguridad de la información.	Se recomienda realizar como mínimo una capacitación al o los empleados del área de sistemas referente a temas de seguridad de la información, con el propósito de mitigar el factor humano que es causante generalmente de las vulnerabilidades dentro de un sistema de información.

Medio	Desconocimiento de las vulnerabilidades actuales en las aplicaciones	Realizar evaluaciones de seguridad continua, para encontrar vulnerabilidades potenciales, usualmente se las encuentra mediante la utilización de las herramientas de Nessus y OpenVas, o muchos de las empresas de desarrollo del software lanzan parches de seguridad que deberían ser instalados y evitar estas vulnerabilidades.
Medio	No se evidencia monitoreos continuos en la red	Crear una política de seguridad, referente a evaluaciones de seguridad en la empresa, especificando cada que tiempo se las realizara, que activos informáticos formaran parte de esta evaluación, asimismo la persona a cargo de realizarlos, las herramientas a utilizar y el tipo de informe con los resultados que debe presentar a la Gerencia.
Medio	Los respaldos que se realizan de su sistema Microplus no se realizan de manera formal	Para que la información se encuentra segura, se recomienda la contratación de un backup online en función de la cantidad de información que se debe respaldar.
Bajo	No se evidencia bitácoras.	Mediante la herramienta de Excel se puede crear un documento que registre las actividades que se realiza en el host y dispositivos.

Fuente: Elaboración propia

3.5. Gestión de vulnerabilidades basado en la metodología NIST 800-115

3.5.1. Consideraciones importante

Antes de realizar el proceso de gestión de vulnerabilidades es importante realizar un inventario de los activos de información de la empresa. Como se describe a continuación.

3.5.1.1. Inventario

Se debe realizar un inventario de todos los recursos de TI, para determinar los componentes que forman parte del sistema de información, estos pueden ser: equipos de hardware, sistemas operativos y aplicaciones de software, que se utilizan dentro de la organización, de esta manera, agruparlos y priorizar esos recursos. De igual manera, se debe mantener un manual de inventario de los recursos de TI que no encuentren evidenciados en los inventarios comunes, como pueden ser políticas de seguridad, documentos de configuración de sistemas, entre otros, con el propósito de tener un sistema de inventario completo, lo que permitirá determinar que recursos estarán dentro del proceso de gestión de vulnerabilidades.

Antes de realizar el inventario, se debe determinar el nivel adecuado de abstracción, a continuación, se muestra una lista de elementos, que puede formar parte del inventario, sin embargo, no todos los elementos descritos, se aplicarán a todos los recursos que forman el sistema de información.

1. Nombre del sistema al que encuentra asociado.
2. Nombre del propietario del recurso (usuario).
3. Que función cumple el recurso.
4. Ubicación física.
5. Configuración del sistema (Sistema operativo y número de versión, Paquetes de software y números de versión, Servicios de red, Dirección de Protocolo de Internet (IP) (si es estática)).
6. Configuración de software instalado.
7. Características de hardware (Unidad Central de procesamiento (CPU), Memoria RAM, Espacio del disco, Direcciones Ethernet (tarjetas de red)).

Agrupación y priorización

Estos recursos de inventario una vez catalogados, deben agruparse y asignarse mediante niveles de prioridad que faciliten los esfuerzos de remedición. La agrupación de estos recursos y la priorización es fundamental para evaluar el riesgo, ayudando a identificar qué recursos requieren una atención especial en el proceso de gestión de vulnerabilidades. Por ejemplo, estos recursos se los podría agrupar por ubicación de red. Debido a que, pueden encontrarse expuestos al Internet.

3.5.1.2. Técnicas de evaluación

El objetivo principal del proceso de gestión de vulnerabilidades es proporcionar los tipos de evaluaciones técnicas que se realizarán periódicamente para identificar de manera proactiva las vulnerabilidades. Estos tipos de evaluaciones se describe a continuación.

Técnicas de revisión

Este tipo de técnicas examina pasivamente sistemas, aplicaciones, redes, políticas y procedimientos para descubrir vulnerabilidades de seguridad. También recopilan información para facilitar y optimizar otras técnicas de evaluación. A continuación, se describe estas técnicas.

Revisión de documentación determina si los aspectos técnicos de las políticas y los procedimientos son actuales y completos. Los documentos para revisar en cuanto a precisión técnica e integridad incluyen políticas de seguridad, arquitecturas y requisitos, estándar de procedimientos operativos; planes de seguridad del sistema y acuerdos de autorización, memorandos de entendimiento y acuerdo para las interconexiones del sistema, y planes de respuesta a incidentes.

Revisión del registro determina si los controles de seguridad están registrando la información adecuada, revelando problemas tales como servicios mal configurados y controles de seguridad, accesos no autorizados e intentos de intrusiones. Revela agujeros en los controles de seguridad basados en reglas. La persona que realice este tipo de técnica de evaluación debe tener conocimiento en formatos y estructuras de conjuntos de reglas, capacidad de correlacionar y analizar conjuntos de reglas desde una variedad de dispositivos.

Revisión de la configuración del sistema es el proceso de identificar debilidades en los controles de configuración de seguridad. Por ejemplo, este tipo de revisión revelará servicios y aplicaciones innecesarios, configuraciones de cuenta y contraseña de usuario inadecuadas, y configuraciones incorrectas de registro y respaldo. La persona que realice este tipo de técnica de evaluación debe tener conocimiento de la configuración segura del sistema, incluido el endurecimiento del sistema operativo y la configuración de la política de seguridad para una variedad de sistemas operativos, capacidad de usar herramientas de prueba de configuración de seguridad automatizadas.

Técnicas de identificación y análisis de objetivos

Este tipo de técnicas se centran en identificar dispositivos activos y sus puertos y servicios asociados, y posteriormente ser analizados para detectar posibles vulnerabilidades. A continuación, se describe estas técnicas.

Descubrimiento de red permite descubrir hosts activos y la manera en que responden en una red, asimismo identifica debilidades y permite aprender cómo funciona la red. La persona que realice este tipo de técnica de evaluación debe tener conocimientos generales de TCP / IP y redes; capacidad de usar herramientas de descubrimiento de redes. Las herramientas que se pueden utilizar para este propósito son: Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace y Umit.

Puerto de red e identificación del servicio permite identificar puertos y servicios de red que operan en hosts activos, como FTP y HTTP, y la aplicación que ejecuta cada servicio identificado. La persona que realice este tipo de técnica de evaluación debe tener conocimientos generales de TCP / IP y redes, puertos y protocolos para una variedad de sistemas operativos, capacidad de usar herramientas de escaneo de puertos y capacidad de interpretar resultados de herramientas. Las herramientas que se pueden utilizar para este propósito son: Amap, AutoScan, Netdiscover, Nmap, P0f, Umit y UnicornScan.

Escaneo inalámbrico permiten identificar dispositivos inalámbricos no autorizados, asimismo señales inalámbricas fuera del perímetro de la empresa. La persona que realice este tipo de técnica de evaluación debe tener conocimientos específicos en protocolos, servicios y arquitecturas de red inalámbricas, capacidad para utilizar herramientas de rastreo y exploración inalámbricas automatizadas. Las herramientas que se pueden utilizar para este propósito son: Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI LANguard, Kismet y WifiTAP.

Técnicas de validación de vulnerabilidad objetivo

Utilizan información producida a partir de la identificación y el análisis del objetivo para explorar más a fondo la existencia de vulnerabilidades potenciales. El objetivo es demostrar que existe una vulnerabilidad y las consecuencias de seguridad que ocurren cuando se explotan. A continuación, se describe estas técnicas.

Descifrado de contraseñas es el proceso de recuperar contraseñas de hashes de contraseñas almacenadas en un sistema informático o transmitidas a través de redes, permitiendo identificar contraseñas débiles y políticas de contraseña. La persona que realice este tipo de técnica de evaluación debe tener conocimiento en la composición segura de contraseñas y el almacenamiento de las mismas en los diferentes sistemas operativos, capacidad de usar herramientas de craqueo automatizadas. Las herramientas que se pueden utilizar para este propósito son: Hydra, John the Ripper, RainbowCrack, Rcrack, SIP-crack, SIPdump, TFTP-Brute, THC PPTP, VNCrack y WebCrack.

Pruebas de penetración permite realizar pruebas la seguridad utilizando las mismas metodologías y herramientas que emplean los atacantes, con el propósito de verificar vulnerabilidades y demostrando estas se pueden explotar de forma iterativa para obtener un mayor acceso. La persona que realice este tipo de técnica de evaluación debe tener conocimiento amplio en TCP / IP, redes y S.O, conocimiento avanzado de vulnerabilidades y vulnerabilidades de redes y sistemas, conocimiento de técnicas para evadir la detección de seguridad. Las herramientas que se pueden utilizar para este propósito son: Driftnet, Dsniff, Ettercap, Kismet, Metasploit, Nmap, Ntop, SinFP, SMB Sniffer y Wireshark.

3.5.1.3. Documentación

Los resultados de la evaluación de seguridad deben documentarse de forma técnica o ejecutivo dependiendo de a quien se le entregara el informe.

- Ejecutivo: Este tipo de informe se lo realiza con el propósito de orientar a los lectores no experimentados en el campo técnico, enfocándose en las consecuencias que podría ocasionar la explotación de las vulnerabilidades, haciendo un visón general de la seguridad de la información.

- Técnico: Este tipo de informes está orientado a lectores con un nivel de conocimiento técnico, específicamente a los profesionales encargados de llevar a cabo las soluciones en este documento. Es necesario que se muestre toda la información recopilada en la evaluación. Las partes más importantes de este informe son una lista de las vulnerabilidades y las acciones correctivas de estas.

3.5.2. Propósito

El propósito es proporcionar a la empresa Textiles Jhonatex un adecuado proceso de gestión de vulnerabilidades técnica de forma proactiva.

3.5.3. Alcance y objetivos

Este procedimiento determina el tipo de evaluación de seguridad técnica que puede realizar la empresa. Asimismo, los objetivos que se detallan a continuación.

- Establecer roles y responsabilidades en el proceso de gestión de vulnerabilidades.

- Establecer el ‘proceso de gestión de vulnerabilidades.

3.5.4. Responsabilidades

3.5.4.1. Responsabilidad del Gerente de Sistemas

Es responsable de las siguientes actividades que se describe a continuación:

- Garantizar una adecuada implementación de este proceso.

- Desarrollar una política de evaluación de seguridad con los siguientes aspectos.

  - Requisitos organizativos que deben cumplir las evaluaciones.

  - Requisitos de documentación y resultados de la misma.

  - La frecuencia de la evaluación.

- Una vez desarrollada y aprobada la política de evaluación de seguridad por Gerencia, esta debe difundirse a las partes involucradas.

- Desarrollar un plan de evaluación. El plan de evaluación debe contener las actividades planificadas para la evaluación e información relacionada de la misma, proporcionado reglas y los límites a los que debe adherirse el evaluador. El plan debe identificar los sistemas y redes que se evaluarán, el tipo y el nivel de prueba permitidos, el lugar desde donde se realizará evaluación, los requisitos de manejo de datos y la orientación para el manejo de incidentes.

- Garantizar la correcta selección y habilidades del evaluador.

- Debe garantizar que las herramientas que se usarán para el escaneo de vulnerabilidades o pruebas de penetración sean confiables, de igual manera, logren detectar vulnerabilidades actuales y que son de mayor riesgo, asimismo que se cubra todo el entorno que será monitoreado para la identificación de vulnerabilidades.

- Revisar todos los resultados obtenidos mediante la evaluación y establecer la estrategia de mitigación. Informar los resultados obtenidos de la evaluación y las actividades de mitigación a los altos directivos de la empresa Textiles Jhonatex.

- Informarse de las nuevas vulnerabilidades, referentes al software, tecnología y recursos de la información que usa la empresa, suscribiéndose a servicios confiables que ofrezcan una lista de nuevas vulnerabilidades. Con el propósito de conocer vulnerabilidad que pueden ser de alto riesgo para la empresa, asegurándose de que sea analizado de manera oportuna.

3.5.4.2. Responsabilidad del Administrador del Sistema (Evaluador)

Es responsable de las siguientes actividades que se describe a continuación:

- Realizar las evaluaciones de seguridad de acuerdo a la política de evaluación de seguridad o si el Gerente de Sistemas lo indique.

- Comprobar la integridad del sistema, niveles de protección y eventos relacionados con la seguridad durante todo el proceso de evaluación.

- Coordinar las actividades que se llevaran a cabo en la evaluación con el Gerente de Sistemas.

- Documentar y reportar los resultados de la evaluación y o prueba penetración al Gerente de Sistemas, asimismo debe implementar medidas remediación.

3.5.4.3. Responsabilidad la Gerencia

Es responsable de suministrar los recursos y el presupuesto que respalde el proceso de gestión de vulnerabilidades, asimismo debe asegurar de que se reciban informes periódicos sobre las actividades que se llevan cabo en el mismo.

3.5.5. Consideraciones Legales

Si la empresa autoriza realizar esta evaluación a una entidad externa, el departamento legal debe estar involucrado, ayudando a revisar el plan de evaluación y proporcionar cláusulas de indemnización o limitación de responsabilidad en los contratos que rigen las evaluaciones de seguridad, particularmente para los tipos de pruebas que se consideran intrusivas.

3.6. Procedimiento de la gestión de vulnerabilidades

Tabla 3.45: Proceso de gestión de vulnerabilidades

N.º	Responsable	Actividad	Documento asociado
1	Gerente de sistemas	Una vez terminado el plan de evaluación al que se sujetará el administrador del sistema, este debe ser aprobado por los altos directivos, mediante una o varias reuniones.	
2	Gerente de sistemas	Proporcionar al administrador del sistema el plan de evaluación, con 3 días antes de la fecha de la ejecución del mismo.	Memorando con documento del plan de evaluación
3	Administrador del sistema	Coordina con el Gerente de Sistemas mediante una reunión, si todas las actividades mencionadas en el plan de evaluación se pueden realizar en el plazo establecido. Esto se lo debe realizar en un plazo máximo de 3 días después de ser notificado.	
4	Administrador del sistema	Notificar mediante memorando al Gerente de Sistemas, que iniciara la evaluación de seguridad.	Memorando con documento de inicio de la evaluación.
5	Administrador del sistema	Procede a ejecutar el escaneo de vulnerabilidades técnicas, en los activos de información definidos en el plan de evaluación.	
6	Administrador del sistema	Mediante un informe técnico, se debe mostrar los resultados de cada uno de los activos de información con el nivel de riesgo, la vulnerabilidad, y las posibles remediaciones del mismo, esto debe ser entregado al Gerente de Sistemas.	Informe técnico de evaluación de seguridad.

7	Gerente de Sistemas	Establece si las acciones de remediaciones de las vulnerabilidades identificadas por cada activo son viables. Caso contrario se realice acciones de mitigación o aceptación del riesgo.	
8	Gerente de sistemas	Elabora el plan de remediación, este debe ser aprobado por los altos directivos, mediante una reunión.	Informe del plan de remediación
9	Gerente de Sistemas	Proporciona el plan de remediación al Administrador del Sistema.	Informe del plan de remediación
10	Administrador del Sistema	Ejecuta el plan de remediación, establecido en el tiempo proporcionado en el mismo.	
11	Administrador del Sistema	Elabora un informe de los resultados obtenidos del plan de remediación al Gerente de sistemas.	Informe de resultados del plan de remediación.
12	Gerente de Sistemas	Notifica mediante memorando a los altos directivos, los resultados del plan de remediación.	Memorando de resultados obtenidos del plan de remediación
Fin del Proceso			

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- Al conocer la situación actual de la seguridad de la información de la empresa Textiles Jhonatex, se evidenció los controles de seguridad implementados, los cuales no son suficientes para salvaguardar la confidencialidad, integridad y disponibilidad de la información, de igual forma estos no se encuentran correctamente documentados, debido a que no se evidenció que fueron realizados mediante la aplicación de alguna norma.

- La evaluación de riesgos de la seguridad de la información aplicada a la empresa Textiles Jhonatex, basándose en la metodología NIST 800-30, determinó varias amenazas y vulnerabilidades, asimismo se propone controles de mitigación que son responsabilidad de la empresa de ser implementados.

- La metodología NIST 800-115, proporcionó una guía para diseñar un proceso de gestión de vulnerabilidades técnicas, la parte más importante de este proceso son las funciones y responsabilidades de las personas que estarán involucradas en el mismo, el cual permitirá fortalecer la seguridad informática de la empresa.

4.2. Recomendaciones

- Es importante que la empresa mejore sus normas de seguridad, con el fin de salvaguardar la disponibilidad, integridad y confidencialidad de la información.

- Los niveles de riesgo con mayor prioridad identificados en este proyecto, deberían ser tratados con mayor prioridad, puesto que si llegan a materializarse las consecuencias provocarían perjuicio monetario o de prestigio de la empresa, y los riesgos de nivel bajo se los puede aceptar o mitigar dependiendo de la Gerencia.

- La renovación continua de las tecnologías y la integración de estas, generaría la aparición de nuevas amenazas y con esto los riesgos dentro de la organización cambiarían, por tal motivo es esencial realizar evaluaciones periódicas de riesgos basándose en el presente plan de evaluación de riesgos.
- Para mejorar la seguridad informática de la empresa, es primordial implementar el proceso de gestión de vulnerabilidades, con el fin de remediar o mitigar nuevas vulnerabilidades técnica que pueden surgir a lo largo del tiempo.

Bibliografia

[1] J. C. G. Porras, “Modelo de gestión de riesgos de seguridad de la información para pymes en el perú,” *repositorioacademico*, vol. 1, p. 203, 2019.

[2] D. I. Q. Yagual, “Plan de recuperación ante desastres informáticos y solición para el nivel de explotación de amenazas y vulnerabilidades aplicada a centros de cómputos,” *Academia*, pp. 4–5, 2015.

[3] E. M. T. Núñez, “Políticas de seguridad de la información basado en la norma iso/ice 27002:2013 para la dirección de tecnologías de información y comunicación de la universidad técnica de ambato,” *Repositorio Uta*, 2015.

[4] U. C. de Madrid, “Las tecnologias de la información y comunicación,” *Nómadas*, no. 8, 2003.

[5] E. S. Report, “Eset security report latinoamérica 2019,” 2019.

[6] N. Dávalos, “Empresa ecuatoriana protagoniza filtración de millones de datos,” *Primicias*, 2019.

[7] Firma-e, “Sistema de gestión de la seguridad de la información,” 2013.

[8] J. A. F. Suárez, “La seguridad informática y la seguridad de la información,” *Polo del Conocimiento*, vol. 2, no. 12, p. 148, 2020.

[9] E. Mifsud, “Introducción a la seguridad informática,” *Recursostic*, pp. 4–7, 2020.

[10] L. Alegsa, “Sistema informatico,” *Alegsa*, Jan. 2019.

[11] K. G. Bermúdez and E. R. Bailon, “Análisis en seguridad iformática y seguridad de la información basado en la norma iso/iec 27001 - sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros,” *Dspace*, 2015.

[12] P. M. Calderón, “Delitos informaáticos,” *Universidad San Francisco de Quito*, p. 6, 2005.

[13] G. H. Cornejo and S. L. Manchola, "Investigación sobre el hacker y sus posibles comienzos en la comunidad estudiantil," *Unipiloto*, 2010.

[14] E. G. G. y D. A. Rubio, "Análisis y estudio de los virus y antivirus informáticos del mercado local. caso práctico elaboración de un virus que recopile la mayor cantidad de procesos que pueden causar daños en los computadores," *Utc*, 2011.

[15] R. M. A. Hintelholher, "Identidad y diferenciación entre método y metodología," *Scielo*, pp. 86–91, 2013.

[16] M. Tejada, "Análisis de riesgos en seguridad de la información," *Polo del Conociemiento*, pp. 233–234, 2018.

[17] I. N. de Estándares y Tecnología, "Publicación especial del nist 800-30," *Departamento de Comercio*, 2012.

[18] O. G. y J. L. Merino, "Modelo de prevención y defensa contra ataques cibernéticos basado en estandares de seguridad internacionales para it-expert," *UPC*, 2016.

[19] I. N. de Estándares y Tecnología, "Guía técnica para pruebas y evaluación de seguridad de la información," *Departamento de Comercio*, 2008.

[20] A. Armijos, "La diferencia entre evaluación y gestión de vulnerabilidades," *Linkedin*, 2018.

[21] H. Corvo, "Sistema de información: características, elementos, ciclo de vida, tipos," *Lifeder*.

[22] "Microplus sql," *Microplus*, 2015.

[23] Vicenso, "Que es xampp y que necesita para ser instalado,"

[24] M. Day, "Siete cosas que necesita saber sobre kali linux," *Start a Cyber Career*.

[25] VIAFIRMA, "Hacking ético: identificación de servicios con nmap,"

[26] Nessus, "Beneficios profesionales de nessus,"

[27] Magerit, "Metodología de análisis y gestión de riesgos de los sistemas de información,"

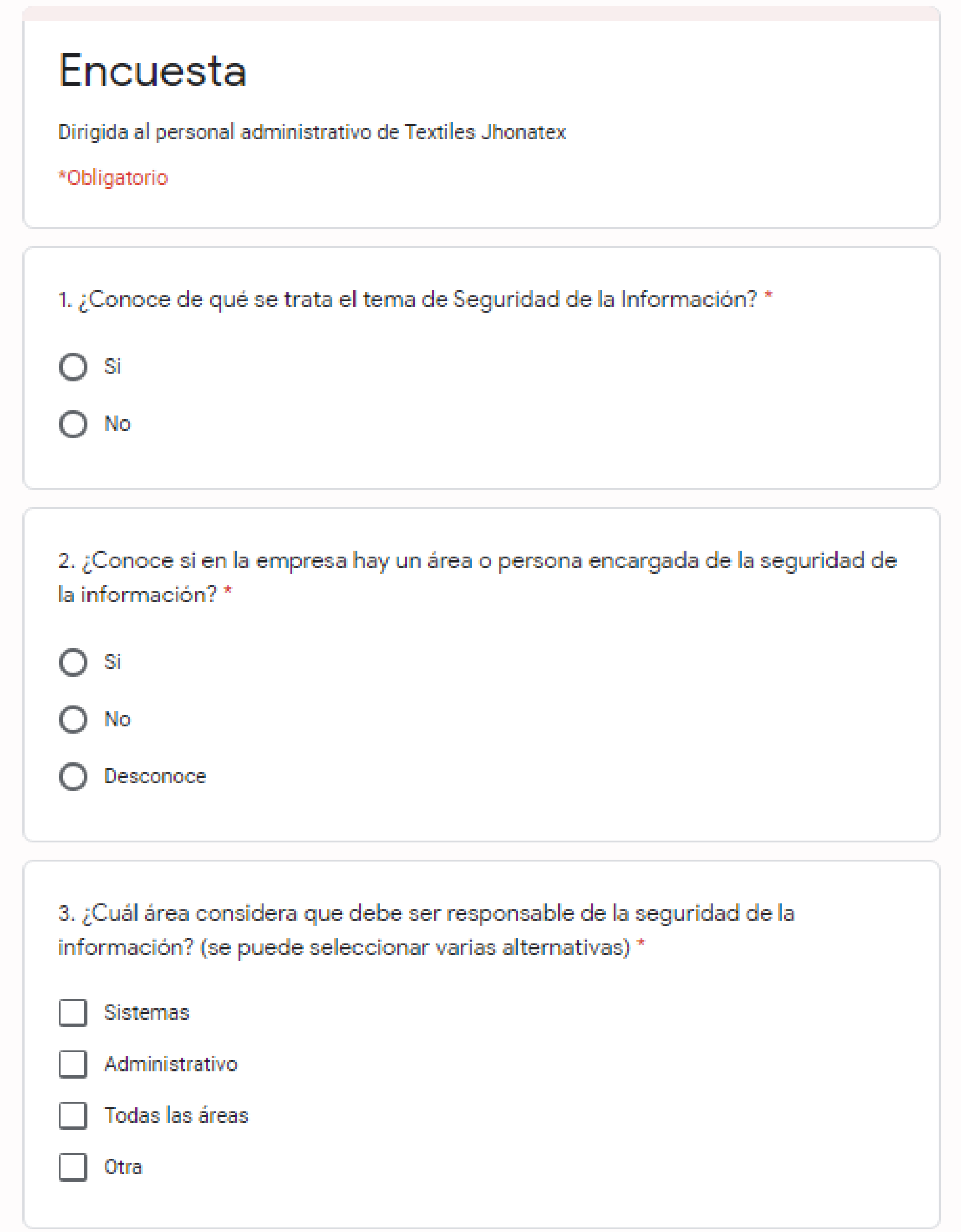
[28] Mintic, "Guía para la gestión y clasificación de activos de información,"

Anexos

Anexo A

Anexo

1.1. Encuesta dirigida al personal de las diferentes áreas de Textiles Jhonatex


Encuesta

Dirigida al personal administrativo de Textiles Jhonatex

*Obligatorio

1. ¿Conoce de qué se trata el tema de Seguridad de la Información? *

- Si
- No

2. ¿Conoce si en la empresa hay un área o persona encargada de la seguridad de la información? *

- Si
- No
- Desconoce

3. ¿Cuál área considera que debe ser responsable de la seguridad de la información? (se puede seleccionar varias alternativas) *

- Sistemas
- Administrativo
- Todas las áreas
- Otra

4. ¿Cuántas capacitaciones ha recibido acerca de seguridad de la información en el último año? *

- ○ Menos de 5
- ○ Más de 5
- ○ Nunca ha recibido

5. ¿Las contraseñas que usa tiene combinación de números, letras y es de más de 10 caracteres? *

- ○ Solo Números y más de 10 caracteres
- ○ Solo letras y más de 10 caracteres
- ○ Números y letras, más de 10 caracteres
- ○ Otra

6. ¿Las contraseñas que utiliza las guarda en un medio físico para no olvidarse? *

- ○ Si
- ○ No

7. ¿Ha ocurrido algún incidente de seguridad en su puesto de trabajo en el último año? (bloqueo de la computadora, daño de computadora, entre otros) *

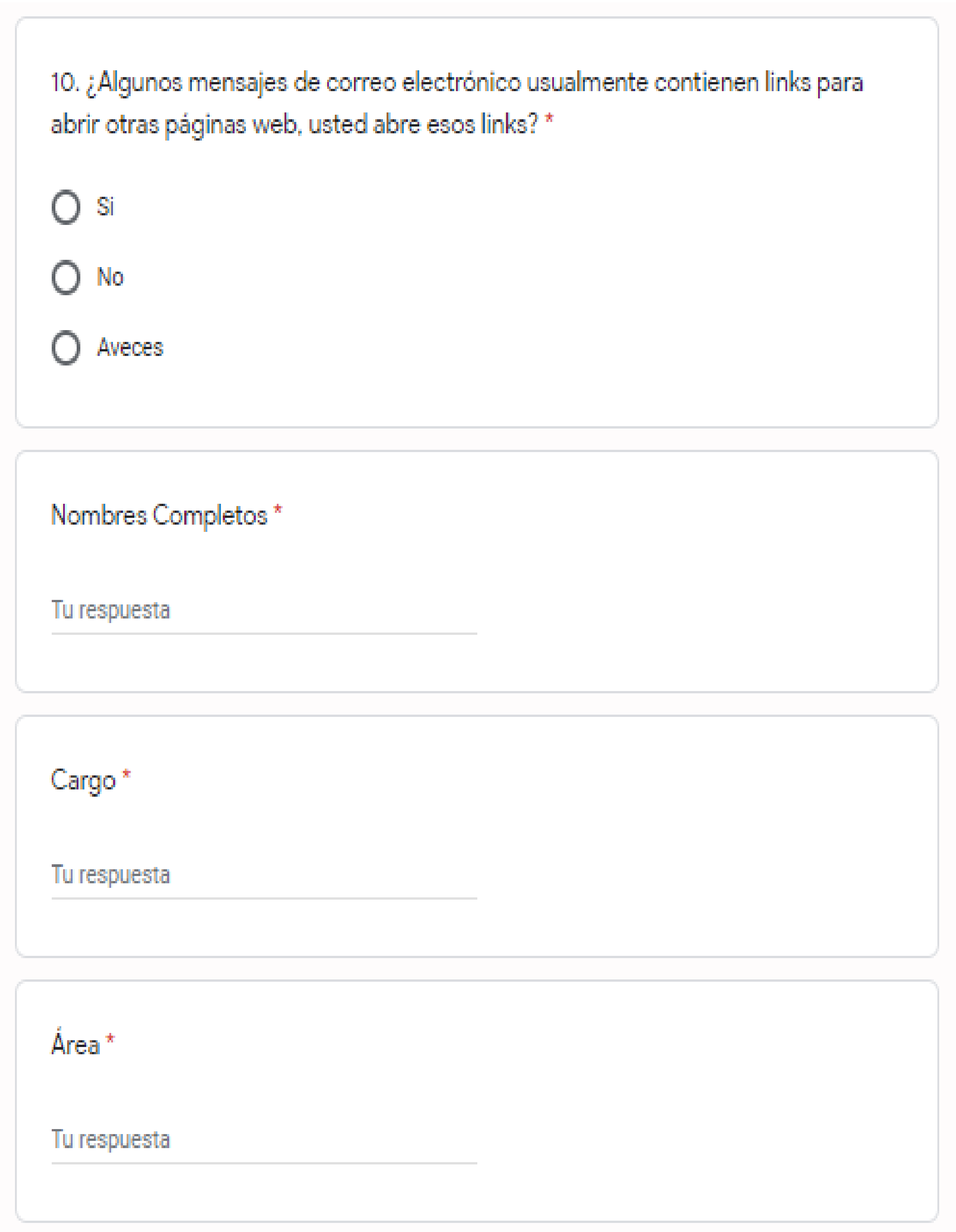
- ◯ Si
- ◯ No
- ◯ Desconoce

8. ¿Se le bloquea automáticamente su computadora cuando no la está utilizando? *

- ◯ Si
- ◯ No
- ◯ Desconoce

9. ¿Cuándo tiene algún incidente de seguridad (falla de equipo, bloqueo de contraseña, pérdida de información) a quién lo notifica? (se puede seleccionar varias alternativas) *

- ☐ Sistemas
- ☐ Jefe Inmediato
- ☐ Altos Directivos
- ☐ No notifica
- ☐ Otra


10. ¿Algunos mensajes de correo electrónico usualmente contienen links para abrir otras páginas web, usted abre esos links? *

- Si
- No
- Aveces

Nombres Completos *

Tu respuesta

Cargo *

Tu respuesta

Área *

Tu respuesta

1.2. Cuestionario de preguntas llevadas a cabo en la entrevista al Gerente de Sistemas

- Conocimiento acerca de Seguridad de la Información.
- Mecanismos de autentificación.
- Respaldos de información.
- Controles y políticas de seguridad implementadas en la empresa.

- Software Malicioso.
- Inventarios tecnológicos.
- Mantenimiento en equipos tecnológicos.
- Existencia del Manual de Políticas de Seguridad de la Información.
- Existencia del área o responsable de Seguridad de la Información.
- Concientizar acerca del tema de la seguridad de la información.
- Incidentes de seguridad.
- Plan de contingencia.

Anexo B

Anexo

Formato Informe Ejecutivo

JHONATEX

INFORME DE EVALUACIÓN DE SEGURIDAD

No. -

Nombre del Área:

Responsable de la Evaluación:

Fecha inicio: **Fecha fin:**

Fecha	Actividad	Tipo de Equipo

Justificación

(Describir que vulnerabilidades son criticas y que consecuencias ocasionaría en el sistema de información al ser explotadas, asimismo los controles recomendados para mitigar los mismos)

____

Firma del Responsable

Anexo C

ANEXO

Informe de escaneo Nessus

192.168.1.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	0	21

Vulnerabilities Total: 23

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification

INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.1.6

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	1	1	0	25

Vulnerabilities Total: 28

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	11936	OS Identification
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	135860	WMI Not Available
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.1.5

3	1	12	1	44
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 61

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	84502	HSTS Missing From HTTPS Server
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	84047	Hyper-V Virtual Machine Detection
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection

INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled