ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA ARROPALMIRA S.A.S.

TATIANA ISABEL HERAZO USTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2020

ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA ARROPALMIRA S.A.S.

TATIANA ISABEL HERAZO USTA

Proyecto de grado para optar el título de Especialista en Seguridad Informática.

Director de proyecto:
MIGUEL ANDRÉS AVILA GUALDRÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2020

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., 2020

DEDICATORIA

A Dios, por haberme dado el don de la vida y permitirme vivir estas experiencias de seguir creciendo como persona y en conocimiento.

A mi madre y mi hijo por ser los pilares importantes, por demostrarme siempre su amor y apoyo incondicional, sin importar las circunstancias.

A mi padre, que por su fallecimiento tan temprano no pudimos vivir muchas cosas, pero sé que este logro sería tan importante para él como para mí.

A mi familia y amigos que de una u otra forma están pendiente de cada logro y se alegran con cada paso que doy, por muy grande o pequeño que sea.

AGRADECIMIENTOS

Agradezco primeramente a Dios por guiarme en mi camino y por permitirme concluir con mi objetivo, a pesar de los tropiezos.

A la Universidad Nacional Abierta y a Distancia – UNAD, por su guía y apoyo en el desarrollo de esta etapa de especialización, e incentivarme en seguir creciendo como persona y en conocimiento.

Al Ingeniero Miguel Ávila, por aportar su experiencia y conocimientos, orientándome en el correcto desarrollo y culminación con éxito este trabajo

A Arropalmira S.A.S por brindarme el escenario para desarrollar este trabajo.

TABLA DE CONTENIDO

LISTA DE TABLAS

pág.

TABLA DE IMÁGENES

pág.

GLOSARIO

AMENAZA: Es una situación que pueda causar daño a los activos informáticos, una amenaza puede ser un virus, una persona, un suceso natural o causado, que afecta negativamente sobre los sistemas informáticos.

BASE DE DATOS: Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las Bases de Datos son uno de los grupos de aplicaciones de productividad personal más extendidos.

CENTRO DE DATOS: Sala o construcción dispuesta para el alojamiento seguro de los equipos de cómputo necesarios para el procesamiento y almacenamiento de la información de una organización (Servidores, Discos externos, equipos de comunicación, etc.)

CONFIDENCIALIDAD: La confidencialidad es una propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas.

COPIA DE RESPALDO o BACKUP: Copia que se realiza a la información institucional definida como sensible o vulnerable, con el fin de utilizarla posteriormente para restablecer el original ante de una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos

DISPONIBILIDAD: Asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requiera

ESTÁNDAR. Publicación que reúne el trabajo en común de los comités de fabricantes, usuarios, organizaciones, departamentos de gobierno y consumidores, que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional con el objeto de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.

IMPACTO: Es el daño producido por la materialización de una amenaza.

HELISA GW: Software para el para el manejo de la información Administrativa y Operativa de cualquier tipo de empresa, La sencillez, confiabilidad y rapidez en su funcionamiento, son características que permiten al sistema, a través de todos sus módulos, brindarle eficiencia al usuario final en la realización de sus labores diarias.

INTEGRIDAD: Salvaguardar que la información y los métodos de procesamiento sean exactos y completos.

KALI-LINUX. El mantenimiento de la seguridad de las redes y sistemas requiere de herramientas específicas para monitorizarlas. Kali Linux tiene las mejores herramientas al alcance de tu mano y agrupadas en una sola distribución GNU/Linux desde la que pone a prueba tus sistemas informáticos.

NESSUS. Herramienta para escanear vulnerabilidades como permitir el control no autorizado o acceso a datos confidenciales de un sistema, configuración incorrecta de parches. Los análisis de Nessus cubren una amplia gama de tecnologías que incluyen sistemas operativos, dispositivos de red, hipervisores, bases de datos, servidores web e infraestructura crítica. Los resultados arrojados por Nessus se pueden visualizar y almacenar en varios formatos planos: XML, HTML.

NORMA: En Tecnología, una norma o estándar es una especificación que reglamenta procesos y productos para garantizar la interoperabilidad. Una norma de calidad es una regla o directriz para las actividades, diseñada con el fin de conseguir un grado óptimo de orden en el contexto de la calidad.

RIESGO: Es la probabilidad de una amenaza de materialice.

SEGURIDAD: Es la forma de minimizar los riesgos a los que están sometidos la infraestructura de TI.

SERVIDORES DE ALMACENAMIENTO: Equipo servidor dotado con arreglos de discos duros destinados a respaldar y compartir datos.

SISCOMBA: Solución para la administración de la operación de las básculas camioneras diseñada para la pequeña y mediana empresa que posee entre una y dos básculas camioneras**.**

VULNERABILIDAD: Es un aspecto susceptible a ser atacado en un sistema informático, el cual representa una debilidad.

RESUMEN

El presente trabajo tiene como finalidad conocer el estado actual de la seguridad de la información de la empresa Arropalmira S.A.S., con el fin de proponer lineamientos para salvaguardar y garantizar la confidencialidad, integridad y disponibilidad de los datos, iniciando con un diagnóstico sobre el manejo de la seguridad de la información, evaluación de los riesgos y así establecer un plan de trabajo con políticas sobre el manejo adecuado de la información, que incluye recomendaciones que permitan cumplir estándares basados en la norma ISO:27001.

Palabras clave: Diagnóstico, ISO:27001, Confidencialidad, Integridad, Disponibilidad, Seguridad, Información.

ABSTRACT

The purpose of this work is to know the current state of information security of the company Arropalmira SAS, in order to propose guidelines to safeguard and guarantee the confidentiality, integrity and availability of the data, starting with a diagnosis on the handling of information security, risk assessment and thus establish a work plan with policies on the proper handling of information, which includes recommendations that allow compliance with standards based on the ISO: 27001 standard.

Key words: Diagnosis, ISO: 27001, Confidentiality, Integrity, Availability, Security, Information.

INTRODUCCIÓN

Los sistemas y las redes de comunicación son activos valiosos para cualquier organización, a través de ellos se realizan procesos y se transmite información importante, factor fundamental para que estos activos sean protegidos frente a cualquier vulnerabilidad o amenaza que ponga en peligro la estabilidad de la empresa en el mercado, lo cual puede afectar su rentabilidad, imagen, nivel de competitividad, entre otros; es por ello que conocer el estado actual de la seguridad de la información de una organización es de vital importancia, de ahí que los temas relacionados a la seguridad de la información no son sólo responsabilidad de un especialista en informática, sino que en realidad son un compromiso de todos los directivos y colaboradores de la compañía, por esta razón, en necesario generar conciencia acerca de los riesgos actuales a todo nivel dentro de las empresas.

Para conocer el estado actual de la seguridad de la información en la organización y para que los sistemas y la información puedan ser tratados adecuadamente, se debe realizar un diagnóstico, basado en normas, estándares y metodologías que permitan determinar en qué estado se encuentra y de esta forma poder determinar controles y procedimientos basados en las mejores prácticas, teniendo en cuenta las necesidades, procesos, tamaño y estructura de la organización, que permitan hacer frente a las diferentes vulnerabilidades y amenazas, disminuyendo el riesgo y elevando los niveles de seguridad en la empresa.

1. FORMULACIÓN DEL PROBLEMA

Cuando las empresas entran en la era de la tecnología de la información, en un principio enfocan sus esfuerzos netamente en las acciones de soporte, mantenimiento, reparación, solución de problemas técnicos, entre otros; a medida que las necesidades del negocio permiten aumentar los desarrollos tecnológicos su orientación en el área de la seguridad de la información debe cambiar, teniendo en cuenta que, aunque los cambios son favorables para ayudar al sostenimiento de la compañía, también se deben contemplar los riegos y amenazas presentes en el ciberespacio, los cuales sin un debido proceso de mitigación y control podrían ocasionar perdidas de todo tipo en los procesos de negocio que tenga la compañía.

De acuerdo con las estadísticas presentadas en el informe de tendencias del Cibercrimen en Colombia 2019-2020[1], *"La dinámica actual del Cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad"* es importante resaltar que según el documento, de los casos registrados durante el 2019, la cifra correspondiente a 15.948 fueron denunciados como infracciones a la ley 1273 de 2009 *"Tipifica las conductas de Delitos Informáticos en Colombia",* contrario, al número expuesto en el año 2015, donde se presentaron 7.523 denuncias, denotando un aumento del 54% aproximadamente.

El informe anterior permite evidenciar que con el paso del tiempo las conductas delictivas en el ciberespacio van en aumento afectado a los ciudadanos del común, y en gran medida a las empresas, las cuales pueden verse afectadas por delitos como: Hurto por medios informáticos, Violación de datos personales (Robo de identidad), Acceso abusivo a sistema informática, Transporte no consentido de activos, entre otros; siendo el desarrollo económico que presenten las diferentes compañías uno de los factores claves para los ciberdelincuentes.

Cabe destacar según el documento, que uno de los ciberataques más sufridos por las compañías en Colombia, se refiere a las diferentes técnicas de Ingeniería Social que utilizan los atacantes, con el fin de obtener información confidencial que les permita realizar la suplantación de las identidades de algunos empleados para lograr, en la mayoría de los casos, efectuar desvíos de dineros hacia otras cuentas bancarias y realizar despachos de mercancía e insumos, engañando a los clientes y proveedores.

[1] CEBALLOS, Adriana, BAUTISTA, Fredy, otros… "Informe de las tendencias del cibercrimen en Colombia (2019-2020)", Primera edición, Bogotá D.C. Octubre 29 de 2019.

Otro de los ataques mencionados dentro del escrito, es el reciente auge de los software de rescate o Ransomware, los cuales utilizan generalmente el envío masivo de correos electrónicos con algún tipo de engaño para que las víctimas (pueden ser empleados de las empresas) se dirijan a un enlace infectado, que finalmente solicita la descarga de un tipo de malware, permitiendo cifrar la información contenida en el dispositivo, evadiendo la acción de los respectivos sistemas de seguridad establecidos, con el fin de solicitar una suma de dinero a cambio del rescate de los datos, la cual, generalmente es cotizada a través de criptomonedas para evitar el rastreo y la ubicación del atacante, en la mayoría de los casos, las empresas realizan pagos sin obtener de vuelta el código para recuperar su información.

Toda lo descrito, nos permite evidenciar que el avance digital en las organizaciones, debe estar acompañado de mecanismos que permitan mitigar los riesgos que le hacen vulnerable, siendo necesario que desde la alta gerencia se destinen recursos y se incluya dentro de la gestión administrativa y organizacional, la implementación de algunas buenas prácticas en seguridad informática, enfocadas en normas, estándares o metodologías, que logren ayudar a los responsables de TI del negocio a prevenir y mitigar los riegos a los que se expone la información de la organización.

Teniendo en cuenta lo anterior, Arropalmira S.A.S que es una empresa dedicada al procesamiento y comercialización de arroz, en el municipio de Sahagún – Córdoba, día a día ha ido creciendo en todas sus áreas de negocio y con ello su tecnología e información se han incrementado de manera considerable, situación que podría convertirse en un punto de vulnerabilidad, si no se cuenta con un estudio que permita determinar el estado actual de la seguridad de la información, así como las recomendaciones y controles que se deberían tener en cuenta para evitar riesgos que afecten el normal funcionamiento de sus labores diarias.

De lo anterior, nace el planteamiento del presente proyecto enfocado en ¿Cómo realizar un diagnóstico para determinar el estado actual de la seguridad de la información en la Empresa Arropalmira S.A.S?

2. JUSTIFICACIÓN

La gestión de riesgos es un tema de gran relevancia para la seguridad de la información en todas las organizaciones, debido a que trata de minimizar las amenazas y vulnerabilidad que se pueden presentar en los sistemas, contrarrestando la afectación de las infraestructuras criticas cibernéticas de las empresas e incluyendo ciertas medidas de seguridad que permitan controlar las amenazas latentes.[2] Mantener la información segura requiere de la utilización de tecnologías y políticas que permitan salvaguardarla aplicando metodologías, estándares y buenas prácticas de seguridad que promuevan la mitigación de los riesgos existentes.[3]

Teniendo en cuenta las crecientes amenazas en el ámbito de la ciberseguridad y la importancia que toma la seguridad de la información para las organizaciones.[4] Es sustancial que las empresas de acuerdo con su contexto estratégico organizacional, realicen una identificación, análisis y valoración del riesgo, para proponer algunos controles que permitan llevar a cabo un tratamiento de las amenazas y vulnerabilidades encontradas; esta labor parte de la concientización a todos los usuarios (de todo nivel) acerca de los ataques que se pueden recibir, permitiendo contrarrestar las brechas de seguridad que pudieran afectar su buen funcionamiento.[5]

Añadido a lo anterior, desarrollar una política de seguridad informática, estudios de seguridad y análisis periódicos, permiten tener claridad sobre los procesos y uso adecuado de los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Estas políticas deben diseñarse teniendo en cuenta el uso y flujo de la información, riesgos frecuentes, errores cometidos, copias de seguridad, usuarios registrados, uso adecuado de contraseñas, entre otros.[6]

---

[2] Conpes 3854, Departamento Nacional de Planeación, Republica de Colombia. “Política Nacional de Seguridad Digital” Bogotá D.C. abril 11 de 2016.

[3] Telefónica, F. "Ciberseguridad, la protección de la información en un mundo digital" Editorial Ariel, S.A, 2016

[4] CEBALLOS, Adriana, BAUTISTA, Fredy, otros… “Informe de las tendencias del cibercrimen en Colombia (2019-2020)”, Primera edición, Bogotá D.C. Octubre 29 de 2019.

[5] MINTIC, Republica de Colombia. Modelo de Seguridad y Privacidad de la Información. “G7 – Guía de gestión de riesgos” 2016.

[6] MINTIC, Republica de Colombia. Modelo de Seguridad y Privacidad de la Información. “G2 – Guía elaboración de la política general de seguridad y privacidad de la información” 2016.

Considerando lo descrito, la realización de un diagnóstico de seguridad de la información le permitirá a la Empresa Arropalmira S.A.S, tener claridad sobre las vulnerabilidades, riesgos y amenazas presentes en su infraestructura, al igual que generar una conciencia acerca del uso adecuado de la información, la importancia de su seguridad y confidencialidad, facilitando el desarrollo adecuado de los procesos de negocio sin colocar en riesgo sus datos y la productividad.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Evaluar el estado actual de la seguridad de la información en la Empresa Arropalmira S.A.S, brindando algunos lineamientos para salvaguardar la información a través del diseño de un plan de mejoramiento que reduzca las vulnerabilidades encontradas en los sistemas.

3.2. OBJETIVOS ESPECÍFICOS

- Elaborar un diagnóstico que identifique los riesgos en la seguridad de la información de la Empresa.

- Valorar las amenazas halladas en los sistemas, a la luz de algunas metodologías de análisis de riesgos de seguridad informática y sus fases propuestas.

- Diseñar un plan de mejoramiento que establezca las políticas, lineamientos y procedimientos, sobre el manejo adecuado de la información para garantizar la seguridad informática.

4. DELIMITACIÓN Y PERMISO

4.1. DELIMITACIÓN.

Realizar un diagnóstico para la seguridad de la información, permite brindar a la industria Arropalmira S.A.S un conocimiento de su estado actual y a la vez, la proposición de algunos lineamientos que logren salvaguardar la información, garantizando la confidencialidad, integridad y disponibilidad de los datos, teniendo en cuenta ciertos aspectos de la norma ISO 27001 y algunos pasos referenciados en metodologías de análisis de riesgos.

4.2. PERMISO.

Para la realización del presente proyecto se solicitó el permiso a la gerencia de la empresa Arropalmira S.A.S, de forma escrita con la Dra. Vanessa Besaile.

5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO

En la actualidad el activo de mayor valor para todas las organizaciones es la información, y a diario se está viendo amenazada por riesgos que ponen en peligro su integridad, es importante la identificación de estas vulnerabilidades, tanto internas como externas, que puedan significar un factor de riesgo para buscar las mejores alternativas de aseguramiento y un entorno de trabajo fiable.[7]

Es así, que las organizaciones pueden proteger sus datos e información de valor con el planteamiento de una guía de Seguridad de la Información que permita conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la misma, alineando cada uno de sus pasos con lo provisto en normas y estándares internacionales como ISO 27001, que permita una certificación de acuerdo con un modelo sólido y reconocido.

5.1.1. NTC-ISO/IEC 27001:20013.

La norma ISO 27001:2013 es la norma principal de la serie ISO 27000. Se puede aplicar a cualquier tipo de organización, independientemente de su tamaño y de su actividad. La norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información.[8]

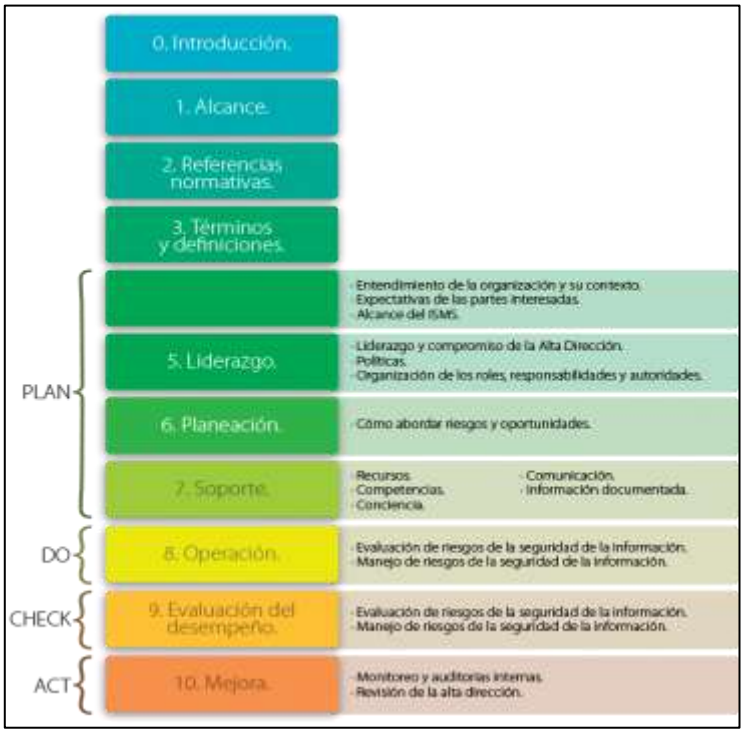
Imagen 1. Estructura ISO 27001.

Fuente: Estándar ISO 27001:2013.

[7] CEBALLOS, Adriana, BAUTISTA, Fredy, otros… "Informe de las tendencias del cibercrimen en Colombia (2019-2020)", Primera edición, Bogotá D.C. Octubre 29 de 2019.
[8] Estándares y Normas de seguridad: http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf

Esta norma recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del sistema. Asimismo, especifica los requisitos para implementar controles y medidas de seguridad adaptados a las necesidades de cada organización.[9]

Imagen 2. Estructura ISO 27001.



Fuente: González Trejo, 2013 - Estructura del estándar ISO/IEC 27001:2013.

A continuación, se describe la estructura de la norma ISO27001:2013[10]

0. Introducción. EL SGSI preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de la gestión del riesgo y brinda confianza a las partes interesadas acerca de qué los riesgos son gestionados adecuadamente. Esta norma puede ser usada partes internas y externas para evaluar la capacidad de la organización y para cumplir los requisitos de seguridad.

[9] Estándares y Normas de seguridad: http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf
[10] ISOTools Excellence. ISO 27001: ¿Cuál es la estructura de la nueva norma ISO 27001 2013? {En línea}. disponible en(https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/).

1. Alcance. Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. Incluye también los requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información. Los requisitos son genéricos y están previstos para ser aplicables a todas las organizaciones, independiente de su tipo, tamaño o naturaleza. No se permite la exclusión de los requisitos especificados en los apartados 4 a 10

2. Referencias normativas. Se recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO27001.Términos y definiciones, adherida esta la norma ISO 27003.

3. Términos y definiciones. Describe la terminología aplicable a este estándar.

4. Contexto de la organización. Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.

5. Liderazgo. Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.

6. Planeación. Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.

7. Soporte. En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.

8. Operación. Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.

9. Evaluación del desempeño. En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.

10. Mejora. Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

Por otra parte, es importante tener presente algunos conceptos y/o definiciones que fortalezcan el entendimiento de lo que puede incluir un sistema de seguridad de la información:

Administración de la seguridad. En una organización, es indispensable las buenas prácticas en la administración de la información, lo cual permite que las políticas creadas, den facilidad al cumplimiento de las reglas y que sean vistas de forma obligatoria.

Esto se convierte en un reto para la alta gerencia, la cual dentro de su gestión, debe tener presente la incorporación de planes de inversión y mejoramiento de la seguridad de la información, que le permitan a la organización garantizar que sus datos se encuentren resguardados bajo políticas y procedimientos estandarizados. *"que solucione las falencias, ubicando la seguridad informática al mismo nivel que otras actividades sustantivas de la organización, elaborando un plan de seguridad informática clara, promulgando políticas que se deriven de dicha misión y determinando que mecanismos se requieren para implementar esas políticas".*[11]

Política de Seguridad. Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan, estás políticas deben estar basadas en un análisis previo de los riesgos a los que está expuesta la información[12].

[11] DALTABIT GODAS Enrique, VASQUEZ, José. "La Seguridad de la Información" Limusa Noriega Editores, 2007. Pág. 215.
[12] UNIR, Políticas de Seguridad Informática. Unir Revista en línea. Mayo 14 de 2014: https://www.unir.net/ingenieria/revista/noticias/politicas-seguridad-informatica/549204996232/

Análisis de riesgo. Este es un paso intermedio que permite realizar la identificación de los activos informáticos con los que cuenta una organización, con el fin de efectuar una evaluación de las amenazas y vulnerabilidades presentes para proponer un plan de mejoramiento que permita mitigar los riesgos encontrados a través de la implementación de algunas salvaguardas "podríamos decir que este proceso consiste en identificar los riesgos de seguridad en la organización, determinar su magnitud e identificar las áreas que requieren salvaguardarlas, es decir gracias al análisis de riesgo conoceremos el impacto económico de un fallo de seguridad y la probabilidad realista de que este fallo ocurra".[13]

Se hace necesario entonces que se pueda identificar cualquier aspecto que ponga en riesgo la seguridad de la información, las buenas prácticas nos llevan a conservar la confidencialidad, integridad y disponibilidad de la información.

Dentro de este punto, es importante mencionar la existencia de metodologías de análisis de riesgos que permiten realizar una validación del estado actual de una organización, con el fin establecer controles que logren reducir al máximo los niveles de exposición que presentan los diferentes activos informáticos, como se observa en la siguiente imagen, algunos de los pasos que contemplan recomiendan comenzar con la identificación de las iniciativas y los procesos críticos del negocio, las tecnologías que los soportan, las amenazas que pudieran actuar en contra, las vulnerabilidades que las exponen, la cuantificación y priorización de los riesgos y los controles para mitigarlos.[14]

Imagen 3. Gestión de Ciber Riesgos.

Fuente: Julián Zamora – Gestión de Ciber Riesgos. [15]

[13] INTECO, Implantación de un SGSI en la empresa. Plan avanza2. Pág. 22.
[14] ZAMORA, Julián. Cyber Security. "Gestión de Ciber Riesgos" 2020.
[15] ZAMORA, Julián. Cyber Security. "Gestión de Ciber Riesgos" 2020.

Algunas de las metodologías existentes son:

5.1.2. Magerit.

Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza[16].

Básicamente Magerit tiene unos pasos pautados:

1. Determinar los activos más relevantes y su interrelación, valor (en el sentido de perjuicio) y costo que supone su afectación.
2. Determinar a qué amenazas están expuestos los activos.
3. Determinar qué salvaguardas hay y cuán eficaces son frente al riesgo.
4. Estimar el impacto (daño del activo) y el riesgo (expectativa de materialización de la amenaza)[17].

Esta metodología ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y apoyar en la preparación de la organización para procesos de evaluación, auditoría, certificación o acreditación; así mismo, una de sus mayores ventajas es que las decisiones que se tomen y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente demostradas. Otro de sus aspectos positivos radica en que sus resultados se expresan en valores económicos lo que, a su vez, también es una desventaja por cuanto el hecho de tener que traducir de forma directa todo el score en valores económicos, hace que la aplicación de esta metodología sea muy costosa[18].

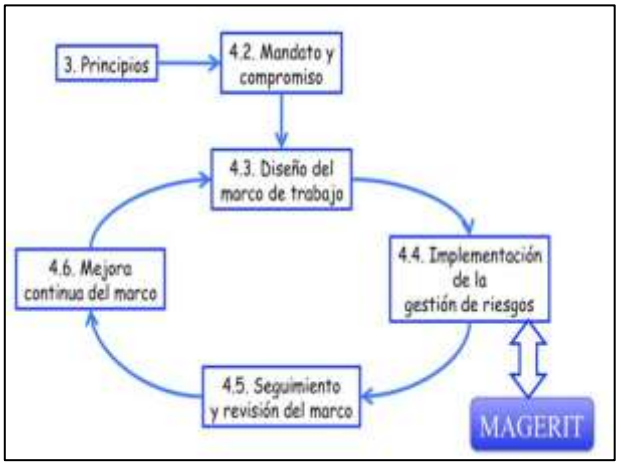
---

[16] INTERPOLADOS. (2018). MAGERIT V.3 : metodología de análisis y gestión de riesgos de los sistemas de información. 2018, octubre 2, de INTERPOLADOS Recuperado de https://interpolados.wordpress.com/2018/10/02/magerit-v-3-metodologia-de-analisis-y-gestion-de-riesgos-de-los-sistemas-de-informacion/

[17] Magerit v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [On line]. Disponible en: http://administracionelectronica.gob. es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#. VRMl5_yG8ms.

[18] Carvajal, (2008). Análisis y Gestión del Riesgo, Base Fundamental del SGSI, Caso: Metodología Magerit Disponible en:

Imagen 4. Metodología Magerit.



Fuente: Metodología Magerit.

5.1.3. Nist.

(National institute of standards and technology): Guía de gestión de riesgo para sistemas de tecnología de la información –recomendaciones del instituto nacional de estándares y tecnología[19].

Esta metodología propone un conjunto de actividades y recomendaciones para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información. Está compuesta por 9 pasos básicos:

- Caracterización del sistema.
- Identificación de amenaza.
- Identificación de vulnerabilidades.
- Control de análisis.
- Determinación del riesgo.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendaciones de control[20].

---

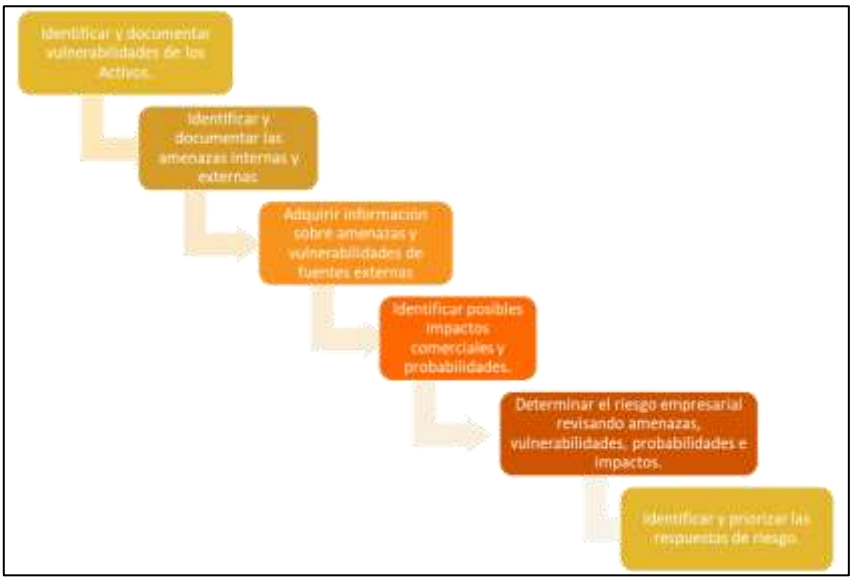
http://52.0.140.184/typo43/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdfhttps://www.ccncert.cni.es/documentospublicos/1789-magerit-libro-i-metodo/file.html

[19] R. Alexandra, O. Zulima. (2011).Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios, Ingeniería 16(2), 56-66

[20] Seguridad 7" A"Metodología NIST SP 800-30 (National Institute of Standards and Technology), [On line]. Disponible en:http://seguridades7a.blogspot.com/p/nist-sp-800-30.html

Nist se destaca por ser muy robusta, pero se convierte en una limitante para la pequeña empresa que tiene limitaciones en su recurso humano, en conocimiento o en capacidad de ampliar la contratación. Aplica más para organizaciones gubernamentales.

Imagen 5. Pasos Metodología Nist.



Fuente: Metodología Nist.

5.1.4. Gestión de riesgo de seguridad digital - Gobierno de Colombia.

Brindar un marco de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control, intensificar la confianza de las múltiples partes interesadas en el medio digital e impulsar la prosperidad económica, social de la entidad y, por ende, del país[21].

Fases:

- ***Fase 1.*** *Planificación de la gestión del riesgo en seguridad digital, comprende actividades como:*

[21] Gobierno de Colombia (2018). *7. Estructura general del modelo nacional de gestión de riesgos de seguridad digital.*

- Definición del contexto interno, externo y de los procesos de la entidad pública.
- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades.
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos.
- Identificación de riesgos[22].
- Valoración de riesgos[23].
- Definición del tratamiento de los riesgos

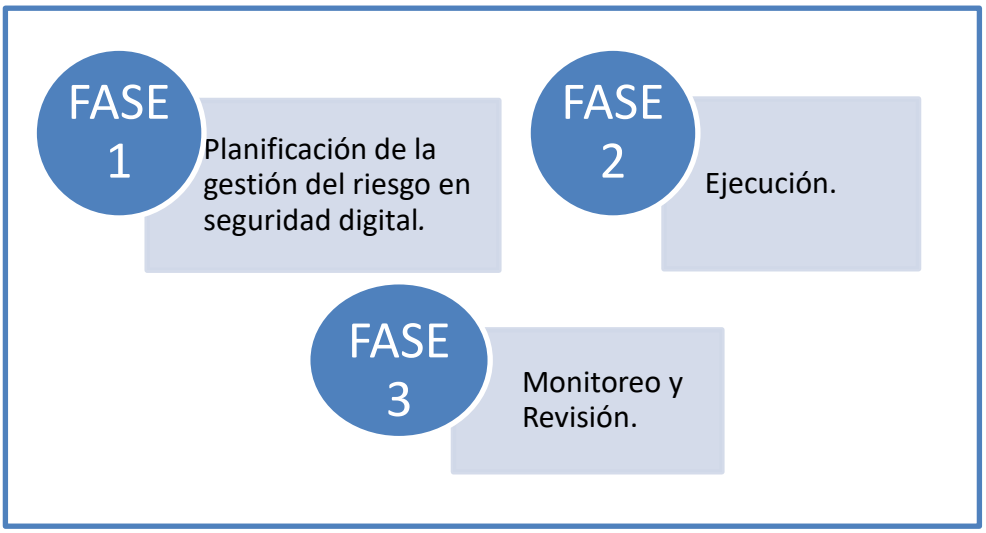
- ***Fase 2.*** *Ejecución.* Esta fase se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo planeado en la Fase 1.

- ***Fase 3.*** *Monitoreo y Revisión.* Se debe hacer un seguimiento a los planes de tratamiento de riesgo de acuerdo con lo siguiente:

  - Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
  - Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
  - Realizar monitoreo de los riesgos y controles tecnológicos.
  - Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
  - Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
  - Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

[22] MINTIC, República de Colombia. Modelo de Gestión de Riesgos de Seguridad Digital {En línea}. disponible en: https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b?version=1.0
[23] MINTIC. Modelo De Gestión de Riesgos de Seguridad Digital - MGRSD). 2018

Imagen 6. Modelo de Gestión de Riesgos de Seguridad Digital.



Fuente: El Autor.

5.2. MARCO CONCEPTUAL

Proteger la información de la organización, independientemente del lugar en que se localiza: servidores, sistemas de almacenamiento, papel, discos, entre otros; eso es darle seguridad a la información, esta seguridad se basa en tres principios fundamentales: Confidencialidad, Integridad y Disponibilidad. El radio de acción de la seguridad de la información debe cubrir análisis de riesgos, seguridad personal, seguridad física y del entorno, gestión de comunicaciones, desarrollo y mantenimiento de sistemas, control de accesos, entre otros, de acuerdo a la norma ISO 27001.[24]

Integridad. Salvaguardar que la información y los métodos de procesamiento sean exactos y completos.

Disponibilidad. Asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requiera

[24] CAMELO, Leonardo. Seguridad de la Información en Colombia. Seguridad de la Información y Seguridad Informática. [En línea].2010. Disponible en Internet: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html.

Confidencialidad. La confidencialidad es una propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas.

Norma. En Tecnología, una norma o estándar es una especificación que reglamenta procesos y productos para garantizar la interoperabilidad. Una norma de calidad es una regla o directriz para las actividades, diseñada con el fin de conseguir un grado óptimo de orden en el contexto de la calidad.[25]

Estándar. Publicación que reúne el trabajo en común de los comités de fabricantes, usuarios, organizaciones, departamentos de gobierno y consumidores, que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional con el objeto de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.[26]

Nessus. Herramienta para escanear vulnerabilidades, verificación de controles no autorizados o acceso a datos confidenciales de un sistema y configuración incorrecta de parches. Los análisis de Nessus cubren una amplia gama de tecnologías que incluyen sistemas operativos, dispositivos de red, hipervisores, bases de datos, servidores web e infraestructura crítica. Los resultados arrojados por Nessus se pueden visualizar y almacenar en varios formatos planos: XML, HTML[27].

Acunetix. Es una herramienta automatizada de seguridad para aplicaciones Web. Acunetix WVS es capaz de escanear cualquier sitio Web o aplicación Web que sea accesible a través del protocolo HTTP / HTTPS. Sin embargo, no todas las pruebas se pueden realizar de forma automática, y por lo tanto Acunetix WVS proporciona herramientas de Penetración manuales para pruebas particulares[28].

Kali. El mantenimiento de la seguridad de las redes y sistemas requiere de herramientas específicas para monitorizarlas. Kali Linux tiene las mejores aplicaciones agrupadas en una sola distribución GNU/Linux desde la que pone a prueba los sistemas informáticos[29].

---

[25] TECCELAYA. Norma, Estándar, Modelo. http://equipoteccelaya.blogspot.es/1234029360/

[26] MINTIC. República de Colombia. Modelo de seguridad de la información. Sitio web: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

[27] Tenable. (2019). TENABLE. Retrieved 9 August, 2019, from https://es-la.tenable.com/products/nessus/nessus-faq

[28] SEAQ. Acunetix Web Vulnerability Scanner. Recuperado de: https://www.seaq.co/acunetix.html, mayo de 2018.

[29] RUBEN, A. Kali Linux. Recuperado de: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671. 2016

5.3. MARCO LEGAL

El principio de la seguridad de la información es la preservación de la confidencialidad, disponibilidad e integridad, además de todos los sistemas implicados en su tratamiento, es así que, para implementar un sistema de seguridad de la información, toda organización debe obligatoriamente cumplir con las leyes, normas y decretos que sean aplicables. Uno de los estándares más utilizados por las empresas como marco normativo para elaborar e implementar un Sistema de Gestión de Seguridad de la Información, evaluar los riesgos que se presentan en sus activos y proponer controles para salvaguardar la información es:

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos, adherida a esta norma esta la ISO 27003 (guía de implementación de un SGSI).

Por otra parte, algunas leyes que se deben tener en cuenta para fortalecer un Sistema de Gestión de Seguridad de la Información son:

LEY 23 DE 1982 sobre Derechos de Autor. Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor.

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

LEY 527 DE 1999; por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

LEY 1266 DE 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos

personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1273 DE 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

DECRETO 2693 DE 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones

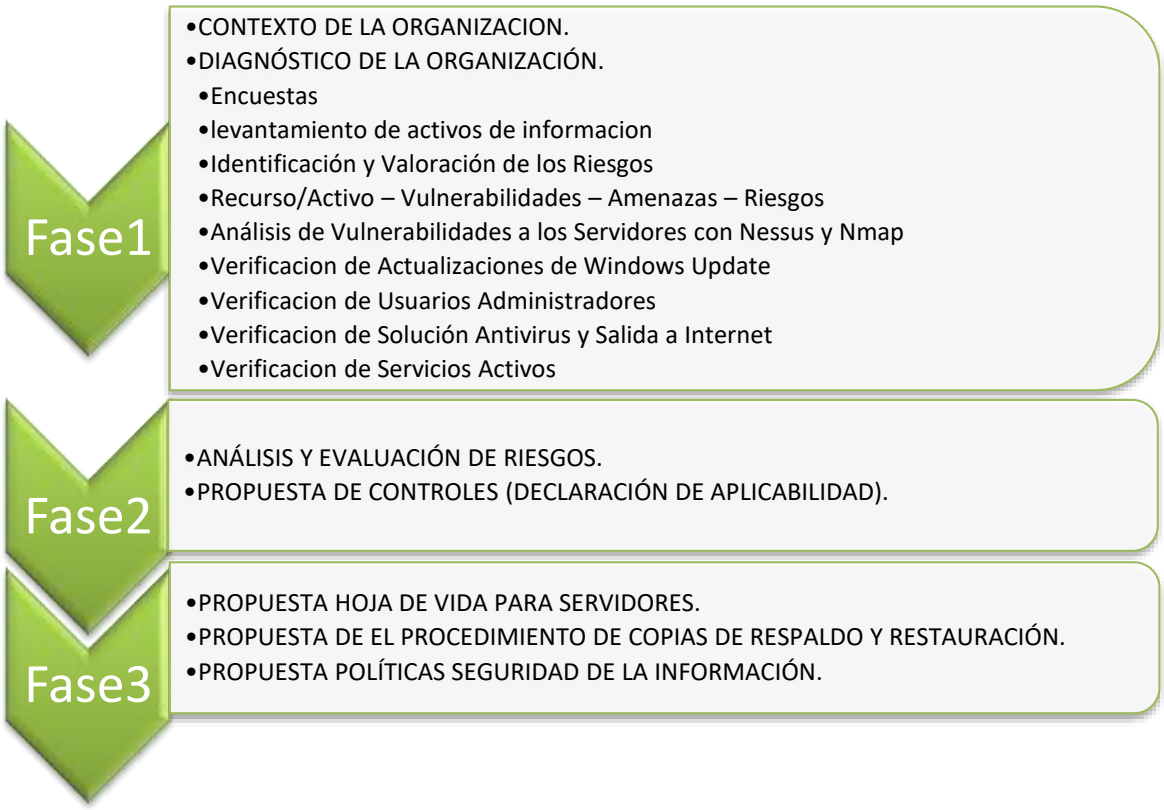
6. METODOLOGÍA

La realización de un diagnóstico para la seguridad de la información incluye un enfoque sistemático, aplicado a la seguridad informática, que ofrece métodos, políticas y técnicas basados en estándares de seguridad, con etapas claras y definidas de los diferentes procesos que se desean realizar.

El presente proyecto se desarrolla basado en algunos conceptos y/o fases descritos por la norma ISO 27001:2013, al igual, que ciertos pasos de las metodologías nombradas en el marco teórico del documento, con el fin de alinear su despliegue en etapas que permitan conservar una estructura clara y metódica para resolver los objetivos planteados.

Su distribución contendrá tres (3) fases, dentro de las cuales se desarrollaran etapas de contextualización, diagnostico, valoración y análisis, al igual, que propuestas para mejorar las falencias encontradas, como se observa en la siguiente imagen.

Imagen 7. Metodología de desarrollo del proyecto.



Fuente: El Autor.

6.1. FASE 1. CONTEXTUALIZACIÓN Y DIAGNÓSTICO.

Para iniciar el desarrollo del proyecto se dará a conocer la reseña historia, estructura y organización de la Empresa Arropalmira SAS.

Población y Muestra. La población para llevar a cabo el diagnóstico para la seguridad de la información es el área administrativa de la Empresa Arropalmira SAS.

El paso inicial es realizar un diagnóstico para identificar y analizar el uso de los activos informáticos que se manejan en la Empresa Arropalmira SAS, lo anterior, se realizará indagando los procesos y siguiendo algunos pasos establecidos en las metodologías estudiadas en el marco teórico del presente documento, que permitirán evaluar el riesgo y establecer un plan de mejoramiento.

Los pasos que se seguirán serán:

- CONTEXTO DE LA ORGANIZACIÓN.
- DIAGNÓSTICO DE LA ORGANIZACIÓN
  - ✓ Encuestas
  - ✓ Levantamiento de activos de información
  - ✓ Identificación y Valoración de los Riesgos
  - ✓ Recurso/Activo – Vulnerabilidades – Amenazas – Riesgos
  - ✓ Análisis de Vulnerabilidades a los Servidores con Nessus y Nmap
  - ✓ Verificación de Actualizaciones de Windows Update
  - ✓ Verificación de Usuarios Administradores
  - ✓ Verificación de Solución Antivirus y Salida a Internet
  - ✓ Verificación de Servicios Activos

6.2. FASE 2. VALORACIÓN Y ANÁLISIS DE LAS AMENAZAS ENCONTRADAS.

Durante este paso se expondrán los resultados del diagnóstico y la valoración de los riesgos, lo cual, se considera un punto importante en el proceso, permitiendo determinar las principales vulnerabilidades de los activos de información y cuales son las amenazas que podrían hacer explotar esas debilidades en el sistema.

Los pasos que se seguirán serán:

- ANÁLISIS Y EVALUACIÓN DE RIESGOS.
- PROPUESTA DE CONTROLES (DECLARACIÓN DE APLICABILIDAD)

6.3. FASE 3. PLAN DE MEJORAMIENTO.

En esta etapa se realizaran las propuestas de algunos formatos, procedimientos y políticas que se deben implantar en la organización, basadas en el diagnóstico y evaluación del riesgo, con la finalidad de mejorar la seguridad de la información y salvaguardar la confidencialidad, integridad y disponibilidad de la empresa.

Los pasos que se seguirán serán:

- PROPUESTA HOJA DE VIDA PARA SERVIDORES
- PROPUESTA DE EL PROCEDIMIENTO DE COPIAS DE RESPALDO Y RESTAURACIÓN
- PROPUESTA POLÍTICAS SEGURIDAD DE LA INFORMACIÓN

7. FASE 1. CONTEXTUALIZACIÓN Y DIAGNOSTICO

7.1. CONTEXTO DE LA ORGANIZACIÓN

7.1.1. Reseña Histórica

INDUSTRIA ARROCERA ARROPALMIRA S.A.S es una empresa de compra, procesamiento, y venta de arroz y sus subproductos, la cual fue fundada en el año 1956 con el nombre de ARROCERA PALMIRA por los señores Baldomero Aldana y Pedro Aldana. Su domicilio inicio en la carrera 14 entre las calles 12 y 13. Su planta física estaba conformada por tres (3) bodegas con capacidad de almacenamiento de 1.800 bultos de arroz paddy, en el cual el proceso de recibimiento de arroz era completamente manual, secado al sol, contaba con una capacidad de procesamiento de 8 bultos por hora y su nómina estaba compuesta por un total de ocho (8) empleados.

En 1984 la empresa fue arrendada al señor Luis Dume y en 1986 al señor Juan Rad Cure. Para el año 1987 fue adquirida en calidad de compra por el señor Musa Besaile Jalife.

Durante el año 1988 la Arrocera se trasladó a su actual domicilio en la Carretera Troncal Kilómetro 1, salida a Montería y para el año 1.989 se adquirieron nuevos equipos con el objeto de aumentar la capacidad de recibo y procesamiento.

En el año 2010 cambia su razón social a ARROCERA PALMIRA BESAILE FAYAD Y CIA S EN C y finalmente en el 2011 cambia a INDUSTRIA ARROCERA ARROPALMIRA S.A.S. apostándole a la tecnificación, con la adquisición de maquinarias de alta tecnología para el mejoramiento de la productividad, redefiniendo los estándares de calidad de la empresa aumentando así, la competitividad en la región.

7.1.2. Misión

Industria Arrocera Arropalmira S.A.S es una organización agroindustrial ubicada en el municipio de Sahagún (córdoba), dedicada a la transformación, producción y comercialización de arroz y sus derivados, Integrando, en nuestra calidad de empresa Agroindustrial, muchos sectores de la economía, comenzando por la agricultura, base fundamental para el desarrollo de Colombia, y a la vez realizando continuamente inversiones e innovaciones tecnológicas y capacitación de nuestros

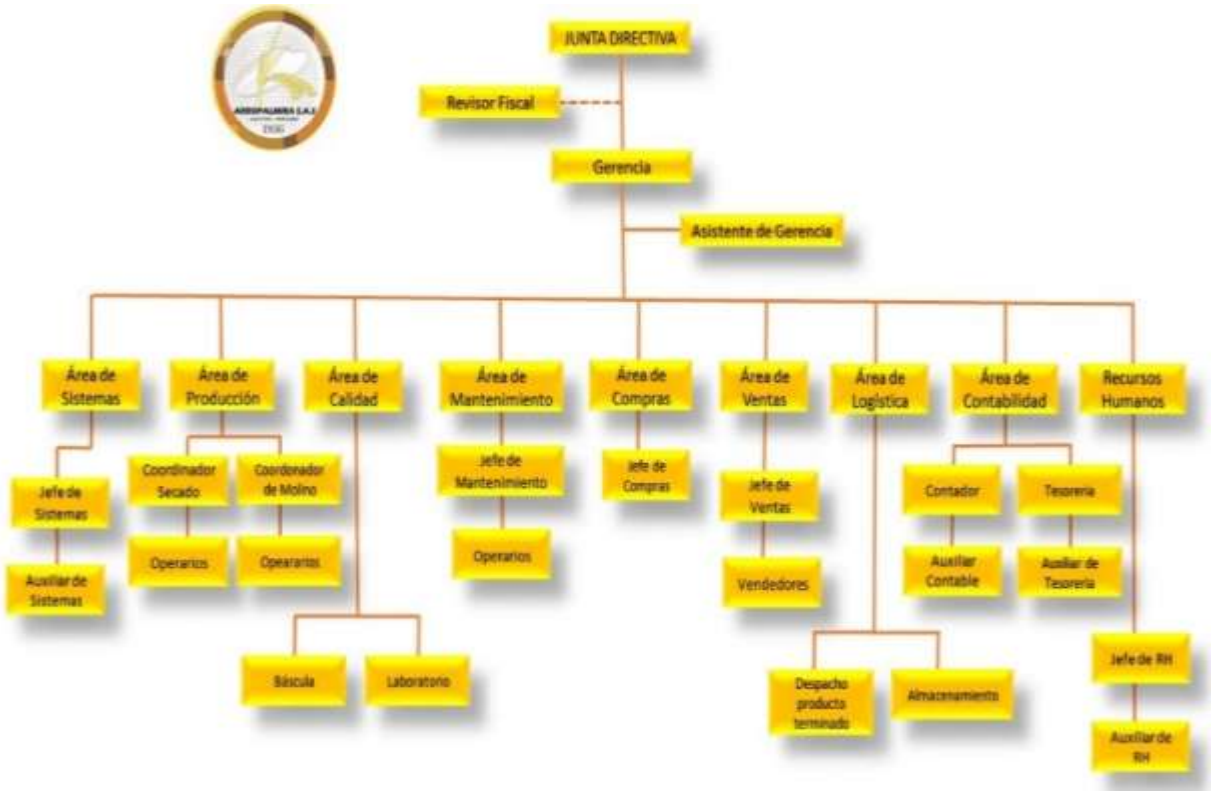
empleados, generando un sistema de gestión de calidad y un talento humano competente y comprometido; para satisfacer las necesidades de los clientes, con el fin de alcanzar un control total de la calidad que nos permita ser cada día más competitivos dentro de las nuevas exigencias del mercado.

7.1.3. Visión

Industria Arrocera Arropalmira S.A.S en el año 2025 será líder en el mercado regional arrocero, con alta calidad en nuestros productos, inversión constante en tecnología e investigación, con un enfoque social, ambiental y económico en la eficiencia de nuestros procesos que responda a las necesidades y expectativas de nuestros clientes y un desarrollo sostenible en el sector arrocero del país.

7.1.4. Organigrama General

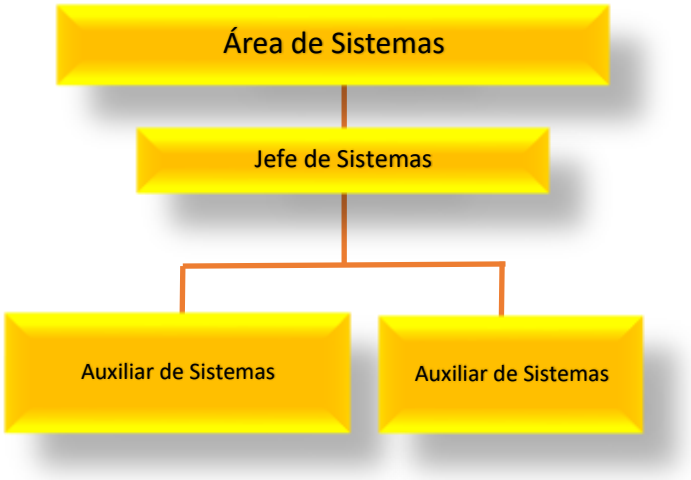
Imagen 8. Organigrama General Arropalmira S.A.S.



Fuente: Arropalmira S.A.S.

7.1.5. Estructura Organizacional del Área Informática, Cargos y Funciones

Imagen 9. Organigrama del área de sistemas



Fuente: Arropalmira S.A.S.

7.1.6. Área de Sistemas

Es el área encargada de gestionar ante la gerencia lo referente a infraestructura a nivel de software y hardware.

7.1.7. Jefe de Sistemas

- Es el encargado de planificar y administrar la infraestructura de TI (Hardware y Software) en conjunto a las necesidades de las áreas de la empresa.
- Coordina los mantenimientos de la infraestructura de TI.
- Velar por el cumplimiento de las actividades asignadas a los auxiliares de sistemas.

7.1.8. Auxiliar de Sistemas

- Soporte a la infraestructura de TI.
- Manteamiento de equipos (Computadores, impresoras, Red LAN).
- Apoyo a la gestión del jefe de sistemas.

7.2. DIAGNÓSTICO DE LA ORGANIZACIÓN

Teniendo en cuenta lo mencionado en la metodología del proyecto, en este punto se desarrollarán algunas encuestas, levantamiento de activos, identificación y valoración de los riesgos, análisis de vulnerabilidades y otras verificaciones, que permitirán establecer el estado actual de la seguridad de la información y realizar un diagnóstico de la empresa Arropalmira S.A.S., abarcando aspectos como infraestructura física, software, recurso humano, activos de información, entre otros.

7.2.1. Encuestas

Administración del centro de cómputo, la seguridad de la red y las comunicaciones.

Tabla 1. Encuesta administración centro de cómputo.

Información Solicitada	Si	No
Diagrama de la red y las comunicaciones, actualizada	X	
Diagrama de la infraestructura de tecnología, actualizada	X	
Hojas de vida de los servidores y otros dispositivos		X
Inventario de software (sistemas operativos servidores y estaciones de trabajo	X	
Ejecución de aseguramiento en servidores y estaciones de trabajo		X
Inventario de equipos del centro de cómputo (servidores y estaciones de trabajo)	X	

Fuente: El autor.

Respaldos de información

Tabla 2. Encuesta respaldos de información.

Información Solicitada	Si	No
Procedimientos de backup y restauración		X
Prueba de restauración		X

Fuente: El autor.

Licencias de software

Tabla 3. Encuesta licenciamiento de software.

Información Solicitada	Si	No
Licencias de los paquetes Office usados dentro de la compañía	X	
Licencias de software para fines especializados	X	
Licencias de Software utilizado en los servidores de los centros de cómputos	X	

Fuente: El autor.

Políticas de seguridad

Tabla 4. Encuesta política de seguridad de la información e inventario de activos.

Información Solicitada	Si	No
Política de seguridad de la información		X
Existe un inventario de activos	X	

Fuente: El autor.

Recurso humano área de tecnología

Tabla 5. Encuesta Recursos humanos personal de TI.

Información Solicitada	Si	No
Recurso Humano del Área de Tecnología o Sistemas en donde se detalle: • Número de personas • Cargos con funciones definidas • Nivel de estudios • Funciones dentro de la compañía • Si existe un Help Desk y como es administrado	X X X X	X

Fuente: El autor.

Seguridad informática

Tabla 6. Encuesta vulnerabilidades.

Información Solicitada	Si	No
Si ejecutan pruebas de vulnerabilidades y Etical Hacking:		X

Fuente: El autor.

7.2.2. Levantamiento de Activos de Información

Tabla 7. Levantamiento de activos de información.

TIPO	NOMBRE DEL ACTIVO
DATOS / INFORMACIÓN	1. [db_clientes] Base de datos clientes
	2. [db_proveedores_paddy] Base de datos Proveedores arroz paddy
	3. [db_proveedores_blanco] Base de datos Proveedores arroz blanco

	4. [siscomba_db] Base de datos Sistema Bascula
	5. [lab_db] Base de datos laboratorio de arroz
	6. [BD_personal] Base de datos empleados
	7. [db_inventarioTI] Base de datos inventario de equipos TI
	8. [helisagw_finandb] Base de datos sistema financiero
	9. [db_producpaddy] Base de datos sistema de producción molino
APLICACIONES	10. [HELISA_GW] Software Contable y Financiero
	11. [SI_SISCOMBA] Software de Bascula
	12. [SI_LABOARROZ] Software para laboratorio de materia prima y producto final.
	13. [SO] Sistema Operativo
	14. [HER_OFI] Herramientas de ofimática
	15. [ANT_VIR] Antivirus
EQUIPAMIENTO INFORMÁTICO	16. [SRV-AP-APP] Servidor de Aplicaciones 17. [SRV-AP-APP] Servidor de Base de Datos 18. [SRV-AP-FILE] Servidor de Archivos
	19. [PC] Estaciones de trabajo
REDES DE COMUNICACIONES	20. [ADSL] Conexión a internet
EQUIPAMIENTO AUXILIAR	21. [CAB_RED] Sistema de Red
INSTALACIONES	22. [CENTROD] Centro de datos
	23. [RACK] Gabinete de Red
PERSONAL	24. [JEFTI] Jefe de departamento de sistemas
	25. [AUX_SIST] Auxiliar de Sistemas.

Fuente: Arropalmira S.A.S.

7.2.3. Identificación y Valoración de los Riesgos

Se valoran los riesgos de 0 a 4 teniendo 0 como la valoración mínima y 4 como la máxima

A continuación, la valoración de los riegos de los activos de información, catalogados el ítem anterior.

Tabla 8. Valoración de riesgos software contable.

HELISAGW			
Amenaza	**Riesgo de confidencialidad**	**Riesgo de integridad**	**Riesgo de disponibilidad**
Fuego	0	0	3
Robo	0	0	3
Error de mantenimiento	2	3	3
Fallo de software	1	2	3
Fallo de comunicaciones	0	0	3
Errores de usuario	1	2	1

Fuente: El autor y Arropalmira S.A.S.

Tabla 9. Valoración de riesgos software inventario.

INVENTARIO_TI			
Amenaza	**Riesgo de confidencialidad**	**Riesgo de integridad**	**Riesgo de disponibilidad**
Fuego	0	0	3
Robo	0	0	3
Error de mantenimiento	2	3	3
Fallo de software	1	2	3
Fallo de comunicaciones	0	0	3
Errores de usuario	1	2	1

Fuente: El autor

Tabla 10. Valoración de riesgos software báscula peso ingreso de materia prima y salida producto terminado.

SISCOMBA			
Amenaza	**Riesgo de confidencialidad**	**Riesgo de integridad**	**Riesgo de disponibilidad**
Fuego	0	0	3
Robo	0	0	3
Error de mantenimiento	2	3	3
Fallo de software	1	2	3
Fallo de comunicaciones	0	0	3
Errores de usuario	1	2	1

Fuente: El autor y Arropalmira S.A.S.

Tabla 11. Valoración de riesgos software para pruebas de laboratorio a materia prima y producto final.

LABOARROZ			
Amenaza	**Riesgo de confidencialidad**	**Riesgo de integridad**	**Riesgo de disponibilidad**
Fuego	0	0	3
Robo	0	0	3
Error de mantenimiento	2	3	3
Fallo de software	1	2	3
Fallo de comunicaciones	0	0	3
Errores de usuario	1	2	1

Fuente: El autor y Arropalmira S.A.S.

Tabla 12. Valoración de riesgos sistema de red empresa Arropalmira S.A.S.

Sistema de Red				
Amenaza	**Probabilidad**	**Degradación de confidencialidad**	**Degradación de integridad**	**Degradación de disponibilidad**
Fuego	1	0	0	3
Robo	2	2	0	2
Error de mantenimiento	2	2	0	3
Fallo de software	2	2	2	3
Fallo de comunicaciones	2	2	1	3
Errores de usuario	2	2	1	1

Fuente: El autor y Arropalmira S.A.S.

Tabla 13. Valoración de riesgos sistema de correo electrónico empresa Arropalmira S.A.S.

Sistema de Correo electrónico				
Amenaza	**Probabilidad**	**Degradación de confidencialidad**	**Degradación de integridad**	**Degradación de disponibilidad**
Fuego	0	0	0	0
Robo	1	1	0	0

Error de mantenimiento	1	0	0	1
Fallo de software	0	0	0	0
Fallo de comunicaciones	1	0	0	3
Errores de usuario	1	0	0	2

Fuente: El autor y Arropalmira S.A.S.

Tabla 14. Valoración de riesgos estaciones de trabajo Arropalmira S.A.S.

Estaciones de Trabajo (PC – Portátiles)				
Amenaza	**Probabilidad**	**Degradación de confidencialidad**	**Degradación de integridad**	**Degradación de disponibilidad**
Fuego	1	0	0	2
Robo	2	1	0	2
Error de mantenimiento	1	2	2	1
Fallo de software	1	0	2	2
Fallo de comunicaciones	1	1	0	1
Errores de usuario	2	2	2	3

Fuente: El autor y Arropalmira S.A.S.

Tabla 15. Valoración de riesgos equipos servidores empresa Arropalmira S.A.S

Servidores				
Amenaza	**Probabilidad**	**Degradación de confidencialidad**	**Degradación de integridad**	**Degradación de disponibilidad**
Fuego	1	0	1	2
Robo	1	1	0	3
Error de mantenimiento	1	2	2	3
Fallo de software	1	0	3	3
Fallo de comunicaciones	1	1	0	3

Errores de usuario	2	2	2	3

Fuente: El autor y Arropalmira S.A.S.

7.2.4. Recurso/Activo – Vulnerabilidades – Amenazas – Riesgos

A continuación, se hace una descripción de la valoración de vulnerabilidades y amenazas, al igual que la valoración de los riesgos, con una escalabilidad de 1 a 3.

Donde las probabilidades se clasifican en baja, media y alta, siento 3 el valor más alto, y para el impacto se clasifican en leve, moderado y catastrófico, utilizando el 3 para el valor más alto.

Tabla 16. Clasificación para la valoración de vulnerabilidades, amenazas y riesgos.

Escala de Probabilidad		**Escala de Impacto**	
Descripción	**Calificación**	**Descripción**	**Calificación**
Baja	1	Leve	1
Media	2	Moderado	2
Alta	3	Catastrófico	3

Fuente: El autor.

7.2.5. Análisis de Vulnerabilidades a los Servidores

Para este análisis se utilizó la herramienta NMAP (Network Mapper o Mapeador de Redes), contenida en Kali-Linux, de uso libre.

NMAP es una herramienta para escanear puertos abiertos. Se diseñó para explorar grandes redes, aunque funciona a perfecto también para hacer mapeos a equipos individuales. A demás de puertos, también dice que servicio lo utiliza y sus versiones. Otra de las cosas que suele mostrar es que filtros o cortafuegos tiene, y a veces hasta el sistema operativo que tiene el equipo entre otras docenas de cosas. Nmap es una herramienta que se usa mucho en auditorias de seguridad.[30]

Lo primordial para comprender el análisis del escaneo de puertos son los estados de los puertos, los cuales son:

Closed: Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento.

[30] (UNDERCODE, 2018)

Open: Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto.

Filtred: Filtrado indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado.

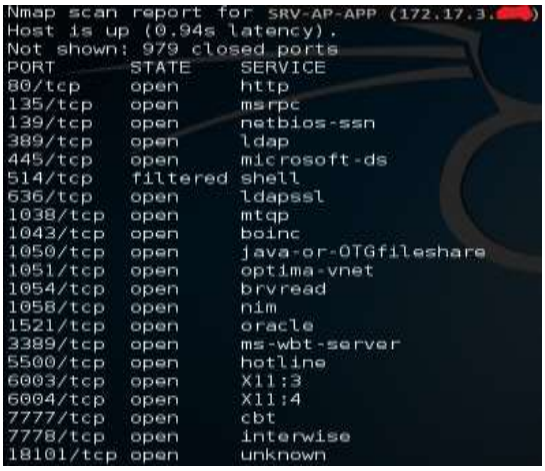
Unfiltred: Los clasificados como no filtrados son aquellos que responden a los sondeos de Nmap, pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados.

Para el análisis de las vulnerabilidades se utilizó la herramienta Nessus, la cual permite escaneo de seguridad remota, que escanea una computadora y/o servidor, generando una alerta si descubre cualquier vulnerabilidad que los piratas informáticos maliciosos puedan usar para acceder a cualquier equipo que haya conectado a una red. Lo hace ejecutando más de 1200 comprobaciones en una computadora determinada, probando para ver si alguno de estos ataques podría usarse para ingresar a la computadora o dañarla[31].

- **Análisis de vulnerabilidades al servidor de aplicaciones (SRV-AP-APP).**

Se recomienda cerrar los puertos que no son necesarios.

Imagen 10. Resultado de escanear con nmap el servidor de aplicaciones



Fuente: El autor.

[31] (TENABLE, 2018)

Vulnerabilidades Encontradas con Nessus.

Imagen 11. Resultado gráfico del análisis de vulnerabilidades

Fuente: El autor.

Vulnerabilidades Críticas

1. CRITICAL: MS17-010: Security Update for Micrsoft Windows SMB Server.
Varias vulnerabilidades de ejecución remota de código existen en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo incorrecto de determinadas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario.[32] (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146,CVE-2017-0148)

Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo incorrecto de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)

POSIBLE SOLUCIÓN:
Ejecutar las actualizaciones de Microsoft en el servidor.
Método 1: Windows Update: Esta actualización está disponible a través de Windows Update. Cuando active las actualizaciones automáticas, esta actualización se descargará y se instalará automáticamente. Para obtener más información acerca de cómo activar actualizaciones automáticas, consulte Obtener actualizaciones de seguridad automáticamente.

[32] Resultado herramienta Nessus.

Método 2: Catálogo de Microsoft Update : Para obtener el paquete independiente de esta actualización, visite el sitio web de Catálogo de Microsoft Update.

También se recomienda leer boletín de seguridad emitido para esta vulnerabilidad. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN

2. CRITICAL: Oracle Database Unsupported Version Detection.
La versión de Oracle Database que se ejecuta en el host remoto ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

POSIBLE SOLUCIÓN:
Actualizar a una versión de Oracle Database que sea compatible.

Vulnerabilidades Altas

1. HIGH: Unsupported Web Server Detection
Según su versión, el servidor web remoto está obsoleto y ya no es mantenido por su proveedor o proveedor. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.

POSIBLE SOLUCIÓN:
Elimine el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor.

Vulnerabilidades Medias

1. MEDIUM: HTTP TRACE/TRACK Methods Allowed
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.

POSIBLE SOLUCIÓN:
Deshabilite estos métodos. Consulte el siguiente enlace como guía de la solución: https://www.tenable.com/plugins/nessus/11213

2. MEDIUM: Web Server Expect Header XSS
El servidor web remoto no puede desinfectar el contenido de un encabezado de solicitud 'Expect' antes de usarlo para generar contenido web dinámico. Un atacante remoto no autenticado puede aprovechar este problema para lanzar ataques de secuencias de comandos entre sitios contra el servicio afectado, tal vez a través de archivos ShockWave (SWF) especialmente diseñados.

POSIBLE SOLUCIÓN:
Ejecute una actualización del servidor web. Para Apache, el problema es fijado según las versiones 1.3.35 / 2.0.57 / 2.2.2; Para IBM HTTP Server, actualizar a 6.0.2.13 / 6.1.0.1; Para IBM WebSphere Application Server, actualice a 5.1.1.17.

Consultar el siguiente enlace para guiarse en la solución.
https://www.tenable.com/plugins/nessus/22254

3. MEDIUM: Apache HTTP Server httoOnly Cookie Information Disclosure

La versión de Apache HTTP Server que se ejecuta en el host remoto está afectada por una vulnerabilidad de divulgación de información.

POSIBLE SOLUCIÓN:
Actualizar a Apache versión 2.0.65 / 2.2.22 o posterior.
Consultar el siguiente enlace como guía para la solución.
https://beyondsecurity.com/scan-pentest-network-vulnerabilities-apache-http-server-httponly-cookie-information-disclosure.html?cn-reloaded=1

4. MEDIUM: LDAP NULL BASE Search Access

El servidor LDAP remoto admite solicitudes de búsqueda con un objeto base NULL o vacío. Esto permite recuperar información sin ningún conocimiento previo de la estructura de directorios. Junto con un NULL BIND, un usuario anónimo puede consultar su servidor LDAP utilizando una herramienta como 'LdapMiner'.

POSIBLE SOLUCIÓN:
Si el servidor LDAP remoto admite una versión del protocolo LDAP antes de v3, considere si desea deshabilitar consultas NULL BASE en su servidor LDAP.
Consultar el siguiente enlace como guía para la solución.
https://www.tenable.com/plugins/nessus/10722

5. MEDIUM: HTTP TRACE/TRACK Methods Allowed

Ejemplo JSPs y Servlets se instalan en el contenedor servlet / JSP de Apache Tomcat remoto. Estos archivos deben eliminarse ya que pueden ayudar a un atacante a descubrir información sobre la instalación o el host remoto de Tomcat. Los archivos de ejemplo también pueden contener vulnerabilidades como vulnerabilidades de secuencias de comandos entre sitios.

POSIBLE SOLUCIÓN:
Revise los archivos y elimine los que no sean necesarios.
Consultar el siguiente enlace como guía para la solución.
https://www.tenable.com/plugins/nessus/11213

6. MEDIUM: Microsoft Windows Remote Desktop Protocolo Server Man-in-the Middle Weakness.

La versión remota del Servidor de Protocolo de Escritorio remoto (Terminal Service) es vulnerable a un ataque en el medio (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado.

POSIBLE SOLUCIÓN:

- ✓ Forzar el uso de SSL como capa de transporte para este servicio si se admite
- ✓ Seleccione la opción 'Permitir conexiones sólo de equipos que ejecutan Escritorio remoto con autenticación de nivel de red' si está disponible.

Consultar el siguiente enlace para ejecutar las posibles soluciones. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc782610(v=ws.10)?redirectedfrom=MSDN

7. MEDIUM: Microsoft Windows SMB NULL Session Autentication

El host remoto ejecuta Microsoft Windows. Es posible iniciar sesión con una sesión NULL (es decir, sin inicio de sesión ni contraseña).

POSIBLE SOLUCIÓN:

Aplique los siguientes cambios de registro por los avisos Technet que se refieren:
Conjunto:
- HKLM \ SYSTEM \ CurrentControlSet \ Control \ LSA \ RestrictAnonymous = 1
- HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ restrictnullsessaccess = 1
Elimine BROWSER de:
- HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ NullSessionPipes

Consultar el siguiente enlace como referencia:
https://docs.microsoft.com/en-us/previous-versions/windows/embedded/ms913275(v=winembedded.5)?redirectedfrom=MSDN

Reinicie una vez que los cambios en el registro estén completos.

8. MEDIUM: Security Update for SAM and LSAD Remote Protocols.

El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos SAM (Security Account Manager) y la Autoridad de seguridad local (Domain Policy) (LSAD) debido a una negociación de nivel de autenticación incorrecta en los canales RPC (Remote Procedure Call).

POSIBLE SOLUCIÓN:
Ejecutar las actualizaciones de Microsoft en el servidor, consultar el siguiente enlace para guiarse en la solución:
https://support.microsoft.com/es-co/help/3148527/ms16-047-security-update-for-sam-and-lsad-remote-protocols-april-12-20

9. MEDIUM: SSL Medium Strength Cipher Suites Supported

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Nessus considera la resistencia media como cualquier cifrado que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de codificación 3DES.

POSIBLE SOLUCIÓN:
Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de intensidad media, consultar el siguiente enlace para su solución.
https://shieldnow.co/2020/02/06/ssl-medium-strength-cipher-suites-supported-sweet32/

10. MEDIUM: SSLv3 Padding Oracle on Downgraded Legacy Encryption vulnerability (POODLE)

El host remoto está afectado por una vulnerabilidad de divulgación de información de tipo man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la manera en que SSL 3.0 maneja los bytes de relleno al descifrar los mensajes encriptados utilizando cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC).

POSIBLE SOLUCIÓN:
Deshabilitar SSLv3.
Los servicios que deben soportar SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda desactivar SSLv3.
Consultar el siguiente enlace para su posible solución.
https://www.tenable.com/plugins/nessus/78479

11. MEDIUM: Terminal Services Doesn´t Use Network Level Authentication (NLA) Only

Los Servicios de Terminal Server remotos no están configurados para utilizar autenticación de nivel de red (NLA) solamente. NLA utiliza el protocolo CredSSP (Credential Security Support Provider) para realizar autenticación de servidor fuerte a través de TLS / SSL o mecanismos Kerberos, que protegen contra los ataques de man-in-the-middle.

POSIBLE SOLUCIÓN:
Habilite autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto se hace generalmente en la pestaña 'Remote' de la configuración 'System' de Windows.

Consultar los siguientes enlaces para la solución.
https://www.tenable.com/plugins/nessus/58453

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

Vulnerabilidades Bajas

1. LOW: SSL Anonymous Cipher Suites Supported
El host remoto admite el uso de cifrados SSL anónimos. Si bien esto permite a un administrador configurar un servicio que cifra el tráfico sin tener que generar y configurar certificados SSL, no ofrece ninguna forma de verificar la identidad del host remoto y hace que el servicio sea vulnerable a un ataque de intermediario.

POSIBLE SOLUCIÓN:
Reconfigure la aplicación afectada si es posible para evitar el uso de cifras débiles.
Consultar el siguiente enlace para posibles soluciones:
https://shieldnow.co/2018/12/19/ssl-anonymous-cipher-suites-supported-cve-2007-1858/

2. LOW: SSL RC4 Cipher Suistes Supported (Bar Mitzvah)
El host remoto admite el uso de RC4 en una o más suites de cifrado. El cifrado RC4 está defectuoso en su generación de una secuencia pseudo-aleatoria de bytes de modo que una amplia variedad de sesgos pequeños se introduce en la corriente, disminuyendo su aleatoriedad.

POSIBLE SOLUCIÓN:
Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifras RC4. Considere la posibilidad de utilizar TLS 1.2 con las suites AES-GCM sujetas al soporte de navegador y servidor web.
Consultar el siguiente enlace como guía para la solución:
https://shieldnow.co/2015/07/15/ssl-rc4-cipher-suites-supported-bar-mitzvah/

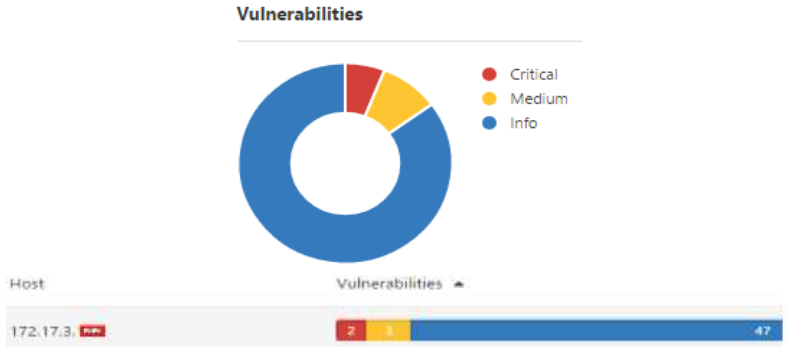
3. LOW: Terminal Services Encryption Level is not FIPS-140 Compliant
La configuración de cifrado utilizada por el servicio de servicios de Terminal Server remoto no es compatible con FIPS-140.

POSIBLE SOLUCIÓN:
Cambie el nivel de cifrado de RDP a: 4. Cumple con FIPS

- **Análisis de vulnerabilidad y soluciones al servidor SRV-AP-DB.**

Vulnerabilidades Encontradas con Nessus

Imagen 12. Resultado escáner de vulnerabilidades con Nessus al servidor de bases de datos.



Fuente: El autor.

Vulnerabilidades Criticas

1. CRITICAL: MS17-010: Security Update for Micrsoft Windows SMB Server
Varias vulnerabilidades de ejecución remota de código existen en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo incorrecto de determinadas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146,CVE-2017-0148)

Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo incorrecto de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)

Ejecutar las actualizaciones de Microsoft en el servidor.
Método 1: Windows Update: Esta actualización está disponible a través de Windows Update. Cuando active las actualizaciones automáticas, esta actualización se descargará y se instalará automáticamente. Para obtener más información acerca de cómo activar actualizaciones automáticas, consulte Obtener actualizaciones de seguridad automáticamente.

Método 2: Catálogo de Microsoft Update : Para obtener el paquete independiente de esta actualización, visite el sitio web de Catálogo de Microsoft Update.

También se recomienda leer boletín de seguridad emitido para esta vulnerabilidad. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN

Vulnerabilidades Medias

1. MEDIUM: Methods Microsoft Windows SMB NULL Session Authentication
El host remoto ejecuta Microsoft Windows. Es posible iniciar sesión con una sesión NULL (es decir, sin inicio de sesión ni contraseña).

POSIBLE SOLUCIÓN:
Aplique los siguientes cambios de registro por los avisos Technet que se refieren:

Consultar el siguiente enlace como guía de la solución.
https://docs.microsoft.com/en-us/previous-versions/windows/embedded/ms913275(v=winembedded.5)?redirectedfrom=MSDN

Conjunto:
- HKLM \ SYSTEM \ CurrentControlSet \ Control \ LSA \ RestrictAnonymous = 1
- HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ restrictnullsessaccess = 1
Elimine BROWSER de:
- HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ NullSessionPipes

2. MEDIUM: MS16-047: Security Update for SAM and LSAD Remote Protocols
El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos SAM (Security Account Manager) y la Autoridad de seguridad local (Domain Policy) (LSAD) debido a una negociación de nivel de autenticación incorrecta en los canales RPC (Remote Procedure Call).

POSIBLE SOLUCIÓN:
Ejecutar las actualizaciones de Microsoft en el servidor
Reinicie una vez que los cambios en el registro estén completos.
Consultar el siguiente enlace como guía para la solución.
https://support.microsoft.com/es-co/help/3148527/ms16-047-security-update-for-sam-and-lsad-remote-protocols-april-12-20

3. MEDIUM: SMB Signing Disabled

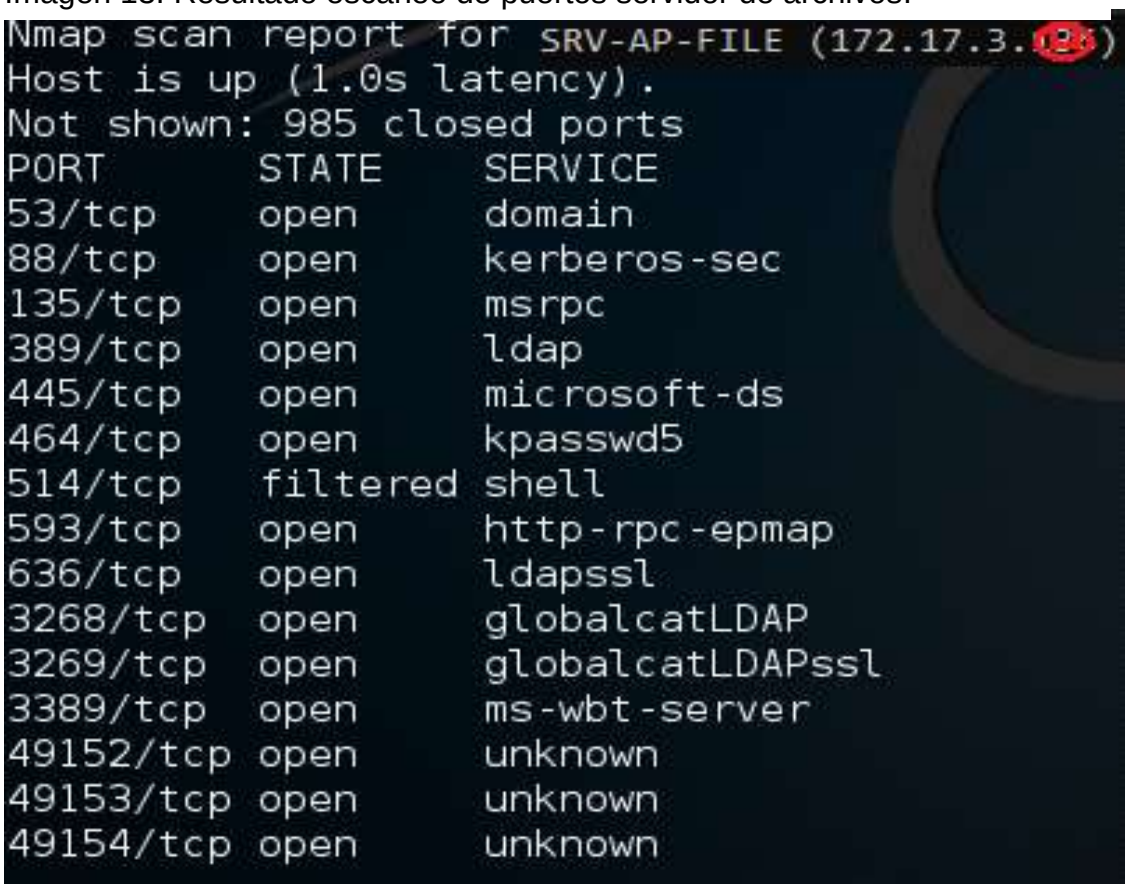
La firma no es necesaria en el servidor SMB remoto. Un atacante remoto, no autenticado, puede explotar esto para realizar ataques man-in-the-middle contra el servidor SMB.

POSIBLE SOLUCIÓN:

Imponga la firma de mensajes en la configuración del host. En Windows, se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firma digital de comunicaciones (siempre)'. En Samba, la configuración se denomina "firma de servidor".

- **Análisis de vulnerabilidad y soluciones al servidor SRV-AP-FILE.**

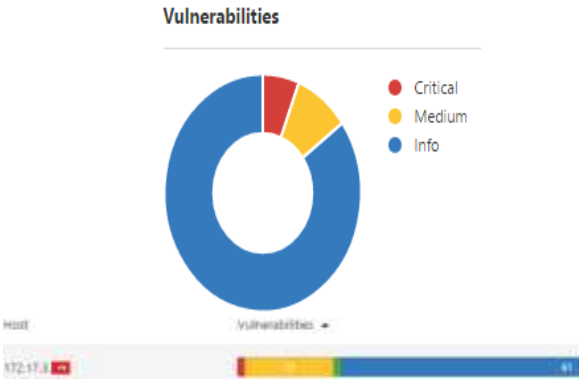
Imagen 13. Resultado escaneo de puertos servidor de archivos.



Fuente: El Autor.

Vulnerabilidades Encontradas con Nessus

Imagen 14. Resultado escaneo de puertos servidor de archivos.



Fuente: El autor

Vulnerabilidades Criticas

1. CRITICAL: MS17-010: Security Update for Micrsoft Windows SMB Server
El servidor de Windows remoto está afectado por las siguientes vulnerabilidades:
- Varias vulnerabilidades de ejecución remota de código existen en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo incorrecto de determinadas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148).

Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo incorrecto de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)

POSIBLE SOLUCIÓN:
Ejecutar las actualizaciones de Microsoft en el servidor.
Método 1: Windows Update: Esta actualización está disponible a través de Windows Update. Cuando active las actualizaciones automáticas, esta actualización se descargará y se instalará automáticamente. Para obtener más información acerca de cómo activar actualizaciones automáticas, consulte Obtener actualizaciones de seguridad automáticamente.

Método 2: Catálogo de Microsoft Update : Para obtener el paquete independiente de esta actualización, visite el sitio web de Catálogo de Microsoft Update.

También se recomienda leer boletín de seguridad emitido para esta vulnerabilidad. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN

Vulnerabilidades Medias

1. MEDIUM: MS16-047: Security Update for SAM and LSAD Remote Protocols

El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos SAM (Security Account Manager) y la Autoridad de seguridad local (Domain Policy) (LSAD) debido a una negociación de nivel de autenticación incorrecta en los canales RPC (Remote Procedure Call).

POSIBLE SOLUCIÓN:

Se recomienda actualizar el sistema operativo. Consultar el siguiente enlace como guía para la solución.
https://support.microsoft.com/es-co/help/3148527/ms16-047-security-update-for-sam-and-lsad-remote-protocols-april-12-20

2. MEDIUM: DNS Server Cache Snooping Remote Information Disclosure

El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen el bit de recursividad establecido.

POSIBLE SOLUCIÓN:

Realice un análisis al estado de saludo al DNS.
Consulte el siguiente enlace como guía para la solución.
https://support.microsoft.com/es-co/help/3149090/ms16-047-description-of-the-security-update-for-sam-and-lsad-remote-pr

3. MEDIUM: DNS Server Dynamic Update Record Injection

Fue posible agregar un registro en una zona utilizando el protocolo de actualización dinámica de DNS.

POSIBLE SOLUCIÓN:

Limitar las direcciones que están autorizadas a realizar actualizaciones dinámicas (por ejemplo, con la opción 'allow-update' de BIND).
Consultar el siguiente enlace como guía para la solución.
https://nmap.org/nsedoc/scripts/dns-update.html

4. MEDIUM: Microsoft Windows Remote Desktop Protocolo Server Man-in-the Middle Weakness

La versión remota del Servidor de Protocolo de Escritorio remoto (Terminal Service) es vulnerable a un ataque en el medio (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado. Un atacante

con la capacidad de interceptar tráfico desde el servidor RDP puede establecer cifrado con el cliente y el servidor sin ser detectado.

POSIBLE SOLUCIÓN:
Forzar el uso de SSL como capa de transporte para este servicio si se admite, o / y Seleccione la opción 'Permitir conexiones sólo de equipos que ejecutan Escritorio remoto con autenticación de nivel de red' si está disponible.
Consultar el siguiente enlace como guía para la solución.
https://www.tenable.com/plugins/nessus/18405

5. MEDIUM: SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

El host remoto admite el uso de un cifrado de bloque con bloques de 64 bits en una o más suites de cifrado. Es, por lo tanto, afectado por una vulnerabilidad, conocida como SWEET32, debido al uso de débiles cifrados de bloque de 64 bits. Un atacante en el medio que tiene recursos suficientes puede explotar esta vulnerabilidad, a través de un ataque de "cumpleaños", para detectar una colisión que filtra el XOR entre el secreto fijo y un texto claro conocido, permitiendo la divulgación del texto secreto, Como las cookies HTTPS seguras y, posiblemente, el secuestro de una sesión autenticada.

POSIBLE SOLUCIÓN:
Reconfigure la aplicación afectada, si es posible, para evitar el uso de todos los cifrados de bloques de 64 bits. Como alternativa, coloque limitaciones en el número de solicitudes que se permiten procesar a través de la misma conexión TLS para mitigar esta vulnerabilidad.
Consultar el siguiente enlace como guía para la solución.
https://social.technet.microsoft.com/Forums/en-US/e5c9f6fd-5486-4941-9c6b-e60d1832bcbc/ssl-64bit-block-size-cipher-suites-supported-sweet32-vulnerability-observed?forum=winserversecurity

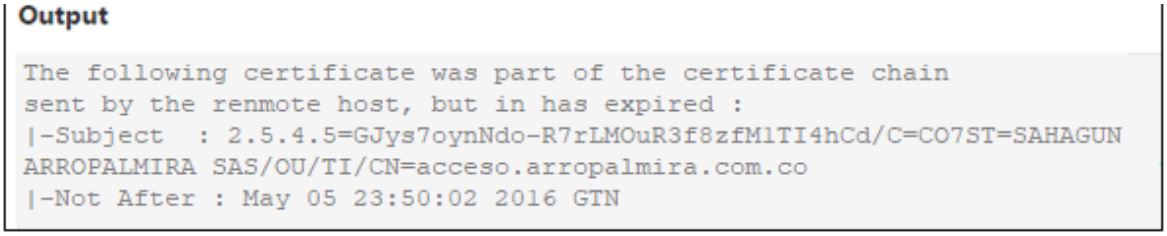
6. MEDIUM: SSL Certificate Cannot Be Trusted

No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza.

Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.

POSIBLE SOLUCIÓN:
Compre o genere un certificado adecuado para este servicio.
Consultar el sguiente enlace como guía para la solución.
https://www.tenable.com/plugins/nessus/51192

Imagen 15. Imagen generación del certificado empresa Arropalmira.



Fuente: El autor

7. MEDIUM: SSL Certificate Signed Using Weak Hashing Algorithm

El servicio remoto utiliza una cadena de certificados SSL que se ha firmado utilizando un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1).

POSIBLE SOLUCIÓN:

Póngase en contacto con la Autoridad de Certificación para que se vuelva a emitir el certificado.

Consultar el siguiente enlace como guía para la solución.

https://shieldnow.co/2017/02/26/ssl-certificate-signed-using-weak-hashing-algorithm/

8. MEDIUM: SSL Medium Strength Cipher Suites Supported

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Nessus considera la resistencia media como cualquier cifrado que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de codificación 3DES.

POSIBLE SOLUCIÓN:

Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de intensidad media. Consultar el siguiente enlace guía para la solución.

https://shieldnow.co/2020/02/06/ssl-medium-strength-cipher-suites-supported-sweet32/

9. MEDIUM: SSL Self-Signed Certificate

La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

POSIBLE SOLUCIÓN:

Compre o genere un certificado adecuado para este servicio.

10. MEDIUM: Terminal Services Doesn´t Use Network Level Authentication (NLA) Only

Los Servicios de Terminal Server remotos no están configurados para utilizar autenticación de nivel de red (NLA) solamente. NLA utiliza el protocolo CredSSP (Credential Security Support Provider) para realizar autenticación de servidor fuerte a través de TLS / SSL o mecanismos Kerberos, que protegen contra los ataques de man-in-the-middle.

POSIBLE SOLUCIÓN:
Habilite autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto se hace generalmente en la pestaña 'Remote' de la configuración 'System' de Windows.
Consultar el siguiente enlace como guía para la solución.
https://www.tenable.com/plugins/nessus/58453

11. MEDIUM: Terminal Services Encryption Leve lis Medium or Low

El servicio de servicios de Terminal Server remoto no está configurado para utilizar criptografía fuerte.

POSIBLE SOLUCIÓN:
Cambiar el nivel de cifrado RDP a uno de los siguientes:
3. Alta
4. Cumple con FIPS

Vulnerabilidades Bajas

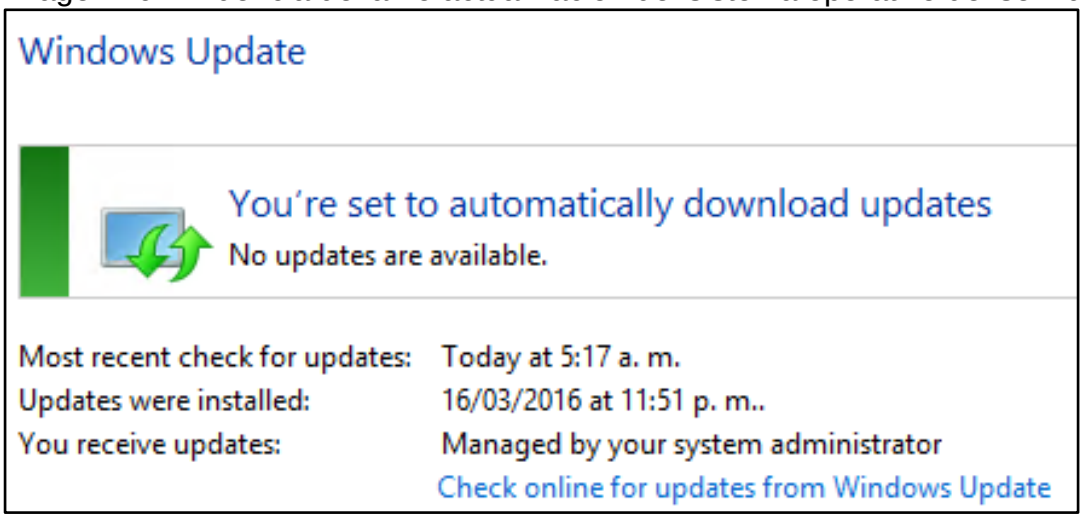
1. LOW: Terminal Services Encryption Level is not FIPS-140 Compliant

La configuración de cifrado utilizada por el servicio de servicios de Terminal Server remoto no es compatible con FIPS-140.

POSIBLE SOLUCIÓN:
Cambie el nivel de cifrado de RDP a:
4. Cumple con FIPS
Consultar el siguiente enlace como guía para la solución.
https://shieldnow.co/2017/03/15/terminal-services-encryption-level-is-not-fips-140-compliant/

- **Verificación de Actualizaciones de Windows Update**

Imagen 16. Evidencia de la no actualización del sistema operativo del servidor.



Fuente: El autor.

Este servidor no se actualiza desde el 16-Mar-2016, revisión realizada el 04 de octubre de 2018.

POSIBLE SOLUCIÓN:
Ejecutar las actualizaciones de Microsoft desde Windows Update.

- **Verificación de Usuarios Administradores**

Se encontró que existen usuarios que tienen privilegios de administrador, adicionalmente renombrados como el super administrador que viene por defecto.

admin.servidores
administrador
Administrator
Default

POSIBLE SOLUCIÓN:
Utilizar los usuarios con privilegios de administrador parametrizados desde el domain controller principal.

- **Verificación de Solución Antivirus y Salida a Internet**

Este servidor tiene instalado el Antivirus Avira y adicionalmente se tiene salida a internet sin restricción alguna.

Imagen 17. Evidencia acceso a internet del servidor de archivo.

Fuente: El autor**.**

<u>POSIBLE SOLUCIÓN:</u>
Desconectar el internet y usarlo solo para posibles actualizaciones del sistema operativo.

8. FASE 2. VALORACIÓN Y ANÁLISIS DE LAS AMENAZAS ENCONTRADAS

8.1. ANÁLISIS Y EVALUACIÓN DE RIESGOS

Activo	ID Riesgo	Riesgo	Vulnerabilidad	Amenaza	Probabilidad	Impacto	Riesgo
HELISAGW DB	DB1	Falta de disponibilidad por eventos de incendio	N/A	Fuego	Baja - 1	Moderado - 2	Medio - 2
	DB2	Filtración de información confidencial por robo de información.	Mal uso de contraseñas	Robo	Baja - 1	Moderado - 2	Medio - 2
	DB3	Falta de disponibilidad por errores de mantenimiento	Falta de control de mantenimientos por parte de personal interno.	Error de mantenimiento	Media - 2	Moderado - 2	Medio - 2
	DB4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	N/A	Fallo de software	Media - 2	Moderado - 2	Medio - 2
	DB5	Falta de disponibilidad por error en la red de datos	No se cuenta con línea de datos de respaldo	Fallo de comunicaciones	Media - 2	Moderado - 2	Medio - 2

	DB6	Resultados inesperados del sistema por errores en procesos inducidos por los usuarios.	Falta de Manuales de usuario y debilidades en entrenamientos.	Errores de usuario	Alta -3	Moderado - 2	Medio - 2
SISCOMBA DB_BAS	DB_BAS 1	Falta de disponibilidad por eventos de incendio	N/A	Fuego	Baja - 1	Catastrófico -3	Medio - 2
	DB_BAS 2	Filtración de información confidencial por robo de información.	Mal uso de contraseñas	Robo	Baja - 1	Moderado - 2	Medio - 2
	DB_BAS 3	Falta de disponibilidad por errores de mantenimiento	Falta de control de mantenimientos por parte de personal interno.	Error de mantenimiento	Media - 2	Catastrófico -3	Medio - 2
	DB_BAS 4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	Debilidades en el soporte del sistema	Fallo de software	Media - 2	Catastrofico -3	Medio - 2
	DB_BAS 5	Falta de disponibilidad por error en la red de datos	No se cuenta con línea de datos de respaldo	Fallo de comunicaciones	Media - 2	Catastrofico -3	Medio - 2

	DB_BAS 6	Resultados inesperados del sistema por errores en procesos inducidos por los usuarios.	Falta de Manuales de usuario y debilidades en entrenamientos.	Errores de usuario	Alta -3	Moderado - 2	Medio - 2
INVENTARIO_TI (DB_N)	DB_N 1	Falta de disponibilidad por eventos de incendio	N/A	Fuego	Baja - 1	Moderado - 2	Medio - 2
	DB_N 2	Filtración de información confidencial por robo de información.	Mal uso de contraseñas	Robo	Baja - 1	Moderado - 2	Medio - 2
	DB_N 3	Falta de disponibilidad por errores de mantenimiento	Falta de control de mantenimientos por parte de personal interno.	Error de mantenimiento	Alta -3	Moderado - 2	Medio - 2
	DB_N 4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	Debilidades en el soporte del sistema	Fallo de software	Alta -3	Moderado - 2	Medio - 2
	DB_N 5	Falta de disponibilidad por error en la red de datos	No se cuenta con línea de datos de respaldo	Fallo de comunicaciones	Alta -3	Moderado - 2	Medio - 2

	DB_N 6	Falta de disponibilidad por eventos de incendio	N/A	Errores de usuario	Alta -3	Moderado - 2	Medio - 2
LABOARROZ (DB_LAB)	DB_LAB 1	Falta de disponibilidad por eventos de incendio	N/A	Fuego	Baja - 1	Leve - 1	Bajo -1
	DB_LAB 2	Filtración de información confidencial por robo de información.	Mal uso de contraseñas	Robo	Baja - 1	Leve - 1	Bajo -1
	DB_LAB 3	Falta de disponibilidad por errores de mantenimiento	Falta de control de mantenimientos por parte de personal interno.	Error de mantenimiento	Alta -3	Leve - 1	Bajo -1
	DB_LAB 4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	Errores por obsolescencia	Fallo de software	Alta -3	Leve - 1	Bajo -1
	DB_LAB 5	Falta de disponibilidad por error en la red de datos	No se cuenta con línea de datos de respaldo	Fallo de comunicaciones	Alta -3	Leve - 1	Bajo -1
	DB_LAB 6	Falta de disponibilidad por eventos de incendio	N/A	Errores de usuario	Alta -3	Leve - 1	Bajo -1

Discovery (BD)	BDD1	Falta de disponibilidad por eventos de incendio	N/A	Fuego	Baja - 1	Leve - 1	Bajo -1
	BDD2	Filtración de información confidencial por robo de información.	Mal uso de contraseñas	Robo	Baja - 1	Leve - 1	Bajo -1
	BDD3	Falta de disponibilidad por errores de mantenimiento	Falta de control de mantenimientos por parte de personal interno.	Error de mantenimiento	Baja - 1	Leve - 1	Bajo -1
	BDD4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	N/A	Fallo de software	Baja - 1	Leve - 1	Bajo -1
	BDD5	Falta de disponibilidad por error en la red de datos	No se cuenta con línea de datos de respaldo	Fallo de comunicaciones	Baja - 1	Leve - 1	Bajo -1
	BDD6	Falta de disponibilidad por eventos de incendio	N/A	Errores de usuario	Media - 2	Leve - 1	Bajo -1
	CAB1	Falta de disponibilidad por eventos de incendio	Cableado en mal estado	Fuego	Media - 2	Moderado - 2	Medio - 2

Sistema de Red (CAB)	CAB2	Filtración de información confidencial por robo de información.	Falta de protocolos de seguridad lógica y física	Robo	Baja - 1	Moderado - 2	Medio - 2
	CAB3	Falta de disponibilidad por errores de mantenimiento	Falta de control de mantenimientos por parte de personal interno.	Error de mantenimiento	Media - 2	Moderado - 2	Medio - 2
	CAB4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	N/A	Fallo de software	Baja - 1	Moderado - 2	Medio - 2
	CAB5	Falta de disponibilidad por error en la red de datos	No se cuenta con línea de datos de respaldo	Fallo de comunicaciones	Baja - 1	Moderado - 2	Medio - 2
	CAB6	Fallo en las comunicaciones por errores de configuración	N/A	Errores de usuario	Media - 2	Moderado - 2	Medio - 2
	E-MAIL 1	Falta de disponibilidad por eventos de incendio	N/A	Fuego	Baja - 1	Moderado - 2	Medio - 2
	E-MAIL 2	Filtración de información confidencial por	Mal uso de contraseñas	Robo	Baja - 1	Moderado - 2	Medio - 2

Sistema de Correo electrónico (E-MAIL)		robo de información.					
	E-MAIL 3	Falta de disponibilidad por errores de mantenimiento	Falta de control de mantenimientos por parte de personal interno.	Error de mantenimiento	Baja - 1	Moderado - 2	Medio - 2
	E-MAIL 4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	N/A	Fallo de software	Baja - 1	Moderado - 2	Medio - 2
	E-MAIL 5	Falta de disponibilidad por error en la red de datos	No se cuenta con línea de datos de respaldo	Fallo de comunicaciones	Baja - 1	Moderado - 2	Medio - 2
	E-MAIL 6	Falta de disponibilidad por errores en la configuración	Debilidad en la gestión de archivos de configuración	Errores de usuario	Media - 2	Moderado - 2	Medio - 2
Estaciones de Trabajo (ET)	ET1	Falta de disponibilidad por eventos de incendio	N/A	Fuego	Media - 2	Moderado - 2	Medio - 2
	ET2	Filtración de información confidencial por robo de información.	Mal uso de contraseñas	Robo	Media - 2	Moderado - 2	Medio - 2
	ET3	Falta de disponibilidad	Falta de control de	Error de mantenimiento	Media - 2	Moderado - 2	Medio - 2

		por errores de mantenimiento	mantenimientos por parte de personal interno.				
	ET4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	Errores por no verificación de rendimiento de equipos	Fallo de software	Media - 2	Moderado - 2	Medio - 2
	ET5	Falta de disponibilidad por error en la red de datos	No se gestiona la configuración de los equipos adecuadamente	Fallo de comunicaciones	Media - 2	Moderado - 2	Medio - 2
	ET6	Falta de disponibilidad por errores en la configuración	Debilidad en la gestión de archivos de configuración	Errores de usuario	Media - 2	Moderado - 2	Medio - 2
Servidores (SRV)	SRV1	Falta de disponibilidad por eventos de incendio	N/A	Fuego	Media - 2	Catastrófico -3	Alto - 3
	SRV2	Filtración de información confidencial por robo de información.	Mal uso de contraseñas	Robo	Baja - 1	Catastrófico -3	Alto - 3
	SRV3	Falta de disponibilidad por errores de mantenimiento	Falta de control de mantenimientos por parte de personal interno.	Error de mantenimiento	Media - 2	Catastrófico -3	Alto - 3

	SRV4	Falta de disponibilidad e integridad de la aplicación por errores del sistema	No se cuenta con personal interno experto	Fallo de software	Media - 2	Catastrófico -3	Alto - 3
	SRV5	Falta de disponibilidad por error en la red de datos	N/A	Fallo de comunicaciones	Media - 2	Catastrófico -3	Alto - 3
	SRV6	Falta de disponibilidad por errores en la configuración	Debilidad en la gestión de archivos de configuración	Errores de usuario	Media - 2	Catastrófico -3	Alto - 3

8.2. PROPUESTA DE CONTROLES (DECLARACIÓN DE APLICABILIDAD)

Arropalmira S.A.S.
Riesgo y Control Informático
La Empresa Arropalmira S.A.S. y partiendo los resultados del primer análisis de identificación de riesgos asociados, se ha determinado que conforme a los controles que se debe implementar para mitigar estos riesgos y para operar de forma segura y conforme a los requisitos de los servicios ofrecidos. Con controles aplicables, y los numerales que se muestran a continuación toman como base las recomendaciones de la norma NTC/ISO 27001:2013.

DOMINIOS	OBJETIVOS DE CONTROL	CONTROLES	OBJETIVO DE CONTROL	DECLARACIÓN DE APLICABILIDAD	SI	NO	OBSERVACIONES
A.5 Políticas de Seguridad de la Información	A.5.1 Orientación de la dirección para la gestión de la Seguridad de la Información	A 5.1.1	Políticas para la seguridad de la Información	¿Documento de la política de seguridad de la información aprobado por la dirección de Arropalmira S.A.S.		X	Crear: 1. Política del SIGS. 2. Marco de Referencia para las políticas de seguridad. 3. Políticas de apoyo para la seguridad de la información.
		A 5.1.2	Revisión de las Políticas para la seguridad de la Información	De manera periódica se debe realizar la revisión y documentar las acciones de mejora		X	Acta de revisión periódica
A.6 Organización de la Seguridad de la Información	A.6.1 Organización Interna	A 6.1.1	Roles y responsabilidades para la Seguridad de la Información	1. Documento de Funciones y Perfiles de las personas inmersas en cada unidad.		X	Documento soporte
		A 6.1.2	Separación de Deberes	1. Matriz de Funciones y Responsabilidades.		X	Documento soporte
		A 6.1.3	Contacto con las autoridades	1. Listado de contactos de interés		X	Elaborar documento
		A 6.1.4	Contacto con los grupos de interés especial	1. Instructivo contactos de interés		X	Elaborar documento
		A 6.1.5	Seguridad de la Información en la Gestión de Proyectos	1. Instructivo Gestión de Proyectos		X	Documento soporte

	A.6.2 Dispositivos móviles y teletrabajo	A 6.2.1	Política para dispositivos móviles	1. Marco de Referencia para las políticas de seguridad		X	
		A 6.2.2	Teletrabajo	1. Marco de Referencia para las políticas de seguridad		X	No existe, pero se deben elaborar los documentos
A.7 Seguridad de los Recursos Humanos	A.7.1 Antes de asumir el empleo	A 7.1.1	Seguridad de los Recursos humanos / Selección	1. Procedimiento para la solicitud de personal para Arropalmira S.A.S., con verificación de antecedentes		X	
		A.7.1.2	Términos y condiciones del empleo	1. Acción de mejora para que GTHUM adicione al contrato cláusula de seguridad de la información		X	
	A.7.2 Durante la ejecución del empleo	A 7.2.1	Responsabilidades de la Dirección	1. Documento responsabilidades de la dirección		X	
		A 7.2.2	Toma de Conciencia, Educación y Formación en la Seguridad de la Información	1. Acción de mejora GTHUM para incluir en inducción y reinducción los temas referentes a seguridad de la información 2. Realizar solicitud para incluir en PIC la capacitación en seguridad de la información		X	Acción de mejora para que GTHUM elaboración de los documentos concernientes.
		A 7.2.3	Proceso Disciplinario	1. Check list para gestión de incidentes 2. Procedimiento de gestión de incidentes y requerimientos		X	

	A.7.3 Terminación y cambio de empleo	A 7.3.1	Terminación o cambio de responsabilidades de empleo	1. Procedimiento de gestión de usuarios		X	
A.8 Gestión de Activos	A.8.1 Responsabilidad por los activos	A8.1.1	Inventario de activos	1. Procedimiento de gestión de activos 2. Formato diligenciado de gestión de activos		X	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento, procedimiento de gestión, formato diligenciados, instructivo para uso aceptable, instructivo de devolución.
		A8.1.2	Propiedad de los activos	1. Procedimiento de gestión de activos 2. Formato diligenciado de gestión de activos		X	
		A8.1.3	Uso aceptable de los activos	1. Instructivo de uso aceptable de los activos		X	
		A8.1.4	Devolución de Activos	1. Instructivo de devolución de los activos		X	
	A.8.2 Clasificación de la Información	A8.2.1	Clasificación de la Información	1. Clasificación de seguridad propuesta 2. Inclusión de la casilla de clasificación de la información en las plantillas utilizadas. 3. Instructivo de clasificación de la información		X	Revisión de los documentos existentes y tener en cuenta cumplir con lo requerido en la declaración de aplicabilidad.
		A8.2.2	Etiquetado y manejo de información	1. Instructivo de clasificación de la información		X	
		A8.2.3	Manejo de Activos	1. Instructivo de clasificación de la información		X	

	A.8.3 Manejo de medios	A8.3.1	Gestión de Medios Removibles	1. Procedimiento reutilización de elementos tecnológicos		X	
		A8.3.2	Disposición de los Medios	1. Procedimiento reutilización de elementos tecnológicos		X	
		A8.3.3	Transferencia de Medios Físicos	1. Marco de Referencia para las políticas de seguridad 2. Instructivo de manejo de medios extraíbles		X	
A.9 Control de Acceso	A.9.1 Requisitos del negocio para control de acceso	A.9.1.1	Política de Control de Acceso	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales		X	1. Marco de Referencia para las políticas de seguridad 2. Procedimiento de gestión de usuarios
		A.9.1.2	Acceso a redes y a servicios de red			X	1. Procedimiento de gestión de usuarios 2. Procedimiento administración de redes locales
	A.9.2 Gestión de acceso de usuarios	A.9.2.1	Registro y cancelación del registro de usuarios	1. Procedimiento de gestión de usuarios, con los respectivos permisos dependiendo el nivel de usuario		X	1. Procedimiento de gestión de usuarios
		A.9.2.2	Suministro de Acceso a Usuarios			X	1. Procedimiento de gestión de usuarios

		A.9.2.3	Gestión de Derechos de Acceso Privilegiado			X	1. Procedimiento de gestión de usuarios 2. Instructivo de derechos de acceso de usuarios privilegiados
		A.9.2.4	Gestión de información de autenticación secreta de usuarios			X	1. Procedimiento de gestión de usuarios
		A.9.2.5	Revisión de los derechos de Acceso de Usuarios			X	1. Procedimiento de gestión de usuarios
		A.9.2.6	Retiro o ajuste de derechos de acceso			X	1. Procedimiento de gestión de usuarios
	A.9.3 Responsabilidades de los usuarios	A9.3.1	Uso de información de autenticación secreta			X	1. Procedimiento de gestión de usuarios 2. Instructivo del uso adecuado de los recursos tecnológicos
	A.9.4 Control de acceso a sistemas y aplicaciones	A9.4.1	Restricción de Acceso a la Información			X	1. Procedimiento de gestión de usuarios
		A9.4.2	Procedimiento de Ingreso Seguro			X	1. Procedimiento de gestión de usuarios

		A9.4.3	Sistema de Gestión de Contraseñas	Instructivo de gestión de usuarios y uso de recursos tecnológicos.		X	1. Procedimiento de gestión de usuarios 2. Instructivo del uso adecuado de los recursos tecnológicos
		A9.4.4	Uso de programas utilitarios privilegiados	1. Instructivo de uso de las herramientas de mesa de ayuda		X	1. Instructivo de uso de las herramientas de mesa de ayuda
		A9.4.5	Control de Acceso a Códigos Fuente de Programas	1. Instructivo de Desarrollo de Software		X	1. Instructivo de Desarrollo de Software
A.11 Seguridad Física y del Entorno	A.11.1 Áreas seguras	A.11.1.1	Perímetro de seguridad física	1. Copias de estudios de seguridad de la empresa que ofrece la vigilancia a Arropalmira S.A.S.. 2. Documento con identificación de áreas críticas		X	1. Estudio de Seguridad.
		A.11.1.2	Controles de acceso físico	1. Instructivo para validar la gestión de acceso físico.		X	1. Instructivo.
		A.11.1.3	Seguridad de oficinas, recintos e instalaciones	1. Instructivo para validar la gestión de acceso físico.		X	1. Instructivo.
		A.11.1.4	Protección contra amenazas externas y ambientales	1. Matriz comparativa de amenazas y vulnerabilidades		X	1. Instructivo
		A.11.1.5	Trabajo en áreas seguras	1. Instructivo para validar la gestión de acceso físico.		X	
		A.11.1.6	Áreas de despacho y carga	1. Instructivo para validar la gestión de acceso físico.		X	

	A.11.2 Equipos	A.11.2.1	Ubicación y protección de los equipos	1. Instructivo del uso adecuado de los recursos tecnológicos		X	
		A.11.2.2	Servicios de suministro	1. Documento protocolo de revisión y administración de los tableros eléctricos de los centros de cableado. 2. Procedimiento de gestión de contrato leasing		X	Protocolo
		A.11.2.3	Seguridad del cableado	1. Documento protocolo de revisión y administración de los tableros eléctricos de los centros de cableado.		X	Protocolo
		A.11.2.4	Mantenimiento de los equipos	1. Contrato de suministro de equipos que especifique las modalidades y actividades de mantenimiento. 2. Registros (evidencia) de las actividades de mantenimiento realizadas.		X	Documentos relacionados.
		A.11.2.5	Retiro de Activos	1. Procedimiento para el control y seguimiento de bienes		X	1. Procedimiento
		A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	1. Instructivo de cifrado de disco 2. Instructivo del uso adecuado de los recursos tecnológicos		X	2. Instructivos

		A.11.2.7	Disposición Segura o Reutilización de equipos	1. Procedimiento estrategia de reutilización de elementos tecnológicos		X	Documentos relacionados.
		A.11.2.8	Equipos de Usuario Desatendido	1. Marco de Referencia para las políticas de seguridad 2. Instructivo del uso adecuado de los recursos tecnológicos		X	
		A.11.2.9	Política de Escritorio Limpio y pantalla limpia	1. Marco de Referencia para las políticas de seguridad 2. Instructivo del uso adecuado de los recursos tecnológicos		X	
A.12 Seguridad de las	A.12.1 Procedimientos operacionales y responsabilidades	A.12.1.1	Procedimientos de Operación Documentados	1. Procedimientos e instructivos de operación de Arropalmira S.A.S.		X	Documentos relacionados.
		A.12.1.2	Gestión de Cambios	1. Marco de Referencia para las políticas de seguridad 2. Procedimiento gestión de cambios		X	
		A.12.1.3	Gestión de Capacidad	1. Procedimiento de gestión de la capacidad		X	
		A12.1.4	Separación de las instalaciones de desarrollo, ensayo y operación	1. Procedimiento de desarrollo 2. Procedimiento de pruebas 3. Procedimiento de gestión de cambios		X	

	A.12.2 Protección contra códigos maliciosos	A12.2.1	Controles contra códigos maliciosos	1. Instructivo de administración de la seguridad perimetral 2. Instructivo de uso del antivirus		X	Instructivo
	A.12.3 Copias de respaldo	A12.3.1	Respaldo de la Información	1. Política de respaldo de la información 2. Estrategia de respaldo de la información 3. Procedimiento de respaldo de la información e instructivos asociados		X	Política de respaldo. Procedimiento de respaldo.
	A.12.4 Registro y seguimiento	A12.4.1	Registro de Eventos	1. Instructivo de revisión de eventos automáticos 2. Bitácora de revisión		X	Documentos relacionados.
		A12.4.2	Protección de la información del registro	1. Instructivo de revisión de eventos automáticos 2. Bitácora de revisión		X	
		A12.4.3	Registros del Administrador y del Operador	1. Instructivo de administración de cuentas y claves sensibles		X	
		A12.4.4	Sincronización de Relojes	1. Instructivo de sincronización de relojes		X	
	A.12.5 Control de software operacional	A12.5.1	Instalación de Software en Sistemas Operativos	1. Instructivo de instalación de software 2. Formato de liberación de responsabilidades		X	Instructivos y Formatos

	A.12.6 Gestión de la vulnerabilidad ténica	A12.6.1	Gestión de las Vulnerabilidades Técnicas	1. Inventario de Herramientas de SW para vulnerabilidades. 2. Instructivo de uso de las herramientas. 3. Documento consideraciones de aplicabilidad de los hallazgos y planes de tratamiento (Justificación para no ejecutarlos)		X	Documentos relacionados
		A12.6.2	Restricciones sobre la instalación de Software	1. Instructivo de instalación de software 2. Formato de liberación de responsabilidades		X	
	A.12.7 Consideraciones sobre auditorias de sistemas de información	A12.7.1	Controles de auditorías de sistemas de información	1. Instructivo de revisión de eventos automáticos		X	
A.13 Seguridad de las Comunicaciones	A.13.1 Gestión de la seguridad de las redes	A.13.1.1	Controles de Redes	1. Instructivo de administración de redes locales (LAN y WiFi)		X	Instructivos y Procedimientos
		A.13.1.2	Seguridad en los servicios de red	1. Procedimiento de administración de las redes y los contratos asociados WAN/LAN		X	
		A.13.1.3	Separación en las Redes	1. Instructivo de segmentación lógica y distribución de red 2. Gráficas de separación de redes: Topología, VLAN		X	Instructivos y Procedimientos

	A.13.2 Transferencia de información	A.13.2.1	Políticas y procedimientos de transferencia de información	1.Marco de Referencia para las políticas de seguridad 2. Procedimiento de transferencia de información		X	Documentos relacionados.
		A.13.2.2	Acuerdos sobre transferencia de Información	1.Marco de Referencia para las políticas de seguridad 2. Procedimiento de transferencia de información		X	
		A.13.2.3	Mensajería Electrónica	1. Instructivo mensajería electrónica		X	
		A.13.2.4	Acuerdos de Confidencialidad o de NO divulgación	1. Formato de Acuerdo de confidencialidad 2. Instructivo sobre acuerdos de confidencialidad		X	
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.1 Requisitos de seguridad de los sistemas de información	A.14.1.1	Análisis y especificación de requisitos de Seguridad de la Información	1. Instructivo de Desarrollo de Software		X	
	A.14.2 Seguridad en los procesos de desarrollo y de soporte	A.14.2.1	Política de Desarrollo Seguro	1. Marco de Referencia para las políticas de seguridad		X	
		A.14.2.2	Procedimiento de Control de Cambios en sistemas	1. Procedimiento de gestión de cambios		X	Instructivos y Procedimientos.
		A.14.2.3	Revisión Técnicas de las Aplicaciones después de los cambios en la	1. Instructivo para actualización de parches (HW y SW (S.O), y BD)		X	

			plataforma de operación				
		A.14.2.4	Restricciones en los cambios a los paquetes de software	1. Procedimiento de desarrollo de software 2. Instructivos asociados a desarrollo de software		X	
		A.14.2.5	Principios de construcción de sistemas seguros	1. Instructivo de Desarrollo de Software		X	
		A.14.2.6	Ambiente de desarrollo seguro	1. Instructivo de Desarrollo de Software		X	
		A.14.2.7	Desarrollo contratado externamente	1. Procedimiento de desarrollo de software		X	
		A.14.2.8	Pruebas de seguridad de sistemas	1. Instructivo de aplicación de pruebas para las aplicaciones desarrolladas		X	
		A.14.2.9	Pruebas de aceptación de sistemas	1. Instructivo de aplicación de pruebas para las aplicaciones desarrolladas		X	Instructivos y Procedimientos.
	A.14.3 Datos de prueba	A.14.3.1	Protección de datos de prueba	1. Instructivo de aplicación de pruebas para las aplicaciones desarrolladas		X	
A.15 Relaciones con los proveedores	A.15.1 Seguridad de la información en las relaciones con los proveedores	A.15.1.1	Política de Seguridad de la Información para las relaciones con proveedores	1. Procedimiento de Gestión de proveedores		X	No existen estos documentos, elaborarlos, aplica

		A.15.1.2	Tratamiento de la Seguridad dentro de los acuerdos con proveedores	1. Procedimiento de Gestión de proveedores		X	
		A.15.1.3	Cadena de Suministro de Tecnología de Información y Comunicación	1. Procedimiento de Gestión de proveedores		X	
A.16 Gestión de Incidentes de Seguridad de la Información	A.16.1 Gestión de incidentes y mejoras en la seguridad de la información	A16.1.1	Gestión de Incidentes / Responsabilidades y Procedimientos	1. Procedimiento de Gestión de Incidentes Tecnológicos		X	No existe, se debe crear.| |
		A16.1.2	Reporte de Eventos de Seguridad de la Información	1. Procedimiento de Gestión de Incidentes Tecnológicos		X	
		A16.1.3	Reporte de debilidades de seguridad de la información	1. Procedimiento de Gestión de Incidentes Tecnológicos		X	No existe, se debe crear
		A16.1.4	Evaluación de Eventos de Seguridad de la Información y decisiones sobre ellos	1. Procedimiento de Gestión de Incidentes Tecnológicos		X	
		A16.1.5	Respuesta a incidentes de seguridad de la información	1. Procedimiento de Gestión de Incidentes Tecnológicos		X	
		A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	1. Procedimiento de Gestión de Incidentes Tecnológicos 2. Procedimiento de Estrategia de Comunicaciones		X	

		A16.1.7	Recolección de Evidencia	1. Procedimiento de Gestión de Incidentes Tecnológicos 2. Procedimiento de Recolección de evidencias (Cómputo Forense)		X	
		A18.1.5	Reglamentación de Controles Criptográficos	1. Procedimiento de uso de los controles criptográficos		X	
	A.18.2 Revisiones de seguridad de la información	A18.2.1	Revisión Independiente de la Seguridad de Información	1. Procedimiento de Auditorías integrales		X	
		A18.2.2	Cumplimiento con las políticas y normas de seguridad	1. Procedimiento de Auditorías integrales		X	No existe, se debe realizar.
		A18.2.3	Revisión del cumplimiento técnico	1. Procedimiento de Gestión de vulnerabilidades		X	

9. FASE 3. PLAN DE MEJORAMIENTO.

Teniendo en cuenta el alcance del documento y luego del diagnóstico y valoración de los riesgos encontrados, se evidencia lo siguiente:

- En la empresa Arropalmira S.A.S., no existe hoja de vida de los servidores que hacen parte de la infraestructura tecnológica.
- En la empresa Arropalmira S.A.S., no existe política de aseguramiento de los servidores.
- En la empresa Arropalmira S.A.S., no existe procedimiento de backup y restauración.
- En la empresa Arropalmira S.A.S., no existe políticas de seguridad de la información.

9.1. PROPUESTA HOJA DE VIDA PARA SERVIDORES

Se elaboró una propuesta de hoja de vida por cada servidor que forma parte de la infraestructura tecnológica de la empresa Arropalmira S.A.S, la cual está conformada por:

Servidor de aplicaciones (1)
Servidor de base de datos (1)
Servidor de archivos (1)

Para la elaboración de la hoja de vida propuesta se tomaron aspectos como control de actualizaciones, características, configuraciones, roles, soporte, almacenamiento externo, configuración de red, usuarios y aplicaciones.

9.1.1. Servidor de aplicaciones SRV-AP-APP

Servidor dónde se alojan las aplicaciones utilizadas por la empresa, para el desarrollo de todos sus procesos, contables, de producción, laboratorios, entre otras.

FORMATO HOJA DE VIDA SERVIDORES						CÓDIGO:
						VERSIÓN:
						PÁGINAS:
CARACTERÍSTICAS GENERALES						
CONTROL DE ACTUALIZACION						
REVISÓ		**ELABORÓ / ACTUALIZÓ**				
Área	TECNOLOGÍA	**Área**	TECNOLOGÍA			
Nombre:	Ing. Roque Avilez	**Nombre:**	Carlos Parra – Javier Mendoza			
Cargo:	Jefe de Sistemas	**Cargo:**	Administrador de Servidores			
Fecha:		**Fecha:**	01-05-2018			
Firma:		**Firma:**				
CARACTERÍSTICAS FISICAS						
CARACTERÍSTICA	**DESCRIPCIÓN**					
Hostname	**SRV-AP-APP (Servidor-ArroPalmira-Aplicaciones)**					
DNS						
Tipo de servidor	Servidor Virtual	**Servidor Clúster**	No			
Marca y Modelo	N/A					
Ficha Técnica	N/A					
Ubicación del servidor	Centro de Cómputo					
Posición	U12	**Rack:**	1			
Tipo de Procesador	Intel ® Xenon ® E5649	**Nº de Procesadores**	4	**Velocidad Procesador (Ghz)**	2.53	
Dimensiones (cm)	N/A					
Color	N/A					
Consumo de potencia (Watts)	N/A	**Peso (Kg)**	N/A			
BIOS versión	Virtual American Megatrends 9.00.06	**Firmware**	N/A			
Controlador RED	Microsoft Virtual Machine Bus Network Adapter	**Adaptador RAID**	N/A			
Memoria (GB)	14 Gb					
Raid controllers	N/A					

Rack de discos / discos internos	Virtual HD ATA Device		
Módulo de video	Microsoft Virtual Machine Bus Video Device		
Numero de fuentes	N/A		
Elementos adicionales	N/A		
CONFIGURACIÓN DEL SERVIDOR			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Sistema Operativo	Microsoft Windows(R) Server 2016, Enterprise Edition	Microsoft(R) Windows(R) Server 2016, Enterprise Edition Build 3790	
Idioma	Ingles	**Kernel**	Windows NT 5.2
Parches aplicados	Service Pack 2		
Particiones (File System)	C: 137 Gb Total – Usados: 100 Gb – Libres: 37 Gb		
Antivirus	Avira Server Security		
Agente de Backup	Windows Server Backup	**Agente Monitoreo**	N/A
ROL DEL SERVIDOR			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Rol Primario	SERVIDOR Fase de Aplicación		
Ambiente	Productivo	**Disponibilidad**	7x24
Criticidad del Servidor	Alta		
SOPORTE HARDWARE			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Contrato de Mantenimiento	**CMSERV-56TY678 Proveedor**	**Fecha Vencimiento Garantía**	Extendida
ALMACENAMIENTO ESTERNO			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Almacenamiento (GB)	N/A		
Tipo de almacenamiento	N/A		
Capacidad Almacenamiento	N/A		

Numero de HBA	N/A	**Velocidad HBA**	N/A

CONFIGURACION DE RED			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Direcciones Estáticas	180.154.XX.XX		
IP ILO - IDRAC	N/A		
NIC 1	Activa		
IP	172.17.3.XXX	**Tipo de IP**	Estática
MAC	00-1F-29-E1-CE-54	**Gateway**	180.154.28.XXX
Velocidad de la tarjeta	1.0 Gbps	**VLAN**	13
Marca NIC	Microsoft Hyper-V Network Adapter		
DNS Primario	180.154.3.190		
DNS Secundario	180.154.3.131		

USUARIOS		
ADMINISTRADORES	**TIPO ACCESO**	**PERMISOS OTORGADOS**
Roque Avilez	Super administrador	Administradores, operador. de cuentas, admins. del dominio

APLICACIONES	
1	Hyper-V Integration Services
2	Avira Server Security
3	Avira Managament Console
3	Microsoft .Net Framework 2.0/3.0/3.5
4	Microsoft Visual C++ 2005
5	Microsoft Operations Manager

APLICACIÓN Y/O SERVICIO CRÍTICOS	
1	DHCP Client
2	DNS Client
3	Hyper-V Hearbeat Service, debe estar ejecutándose
4	Hyper-V Data Exchange Service, debe estar ejecutándose
5	Hyper-V Time Synchronization Service
6	Hyper-V Guest Shutdown Service
7	INVENT_TI (inventario ti-inhouse)
8	OracleCSService
13	SI_SISCOMBA (Software de báscula)
14	SI_LABOARROZ (Software laboratorio arroz blanco y paddy)
11	Oracleoracleas1ProcessManager
12	HelisaGW (software contable)

9.1.2. Servidor de base de datos

Propuesta hoja de vida para servidor de base de datos SRV-AP-DB

CONTROL DE ACTUALIZACIÓN			
REVISO		**ELABORÓ / ACTUALIZÓ**	
Área	TECNOLOGÍA	**Área**	TECNOLOGÍA
Nombre:	Ing. Roque Avilez	**Nombre:**	Carlos Parra Javier Mendoza
Cargo:	Jefe de Sistemas	**Cargo:**	Administrador de Servidores
Fecha:		**Fecha:**	01-05-2018
Firma:		**Firma:**	

CRACTERÍSTICAS GENERALES					
CARACTERÍSTICA	**DESCRIPCIÓN**				
Hostname	**SRV-AP-DB (Servidor ArroPalmira Base de Datos)**				
DNS					
Tipo de servidor	Servidor Virtual	**Servidor Clúster**	No		
Marca y Modelo	N/A				
Ubicación del servidor	Centro de Cómputo				
Posición	SRV-AP-DB	**Rack**	2		
Tipo de Procesador	Intel ® Xeon ® E5649	**Nº de Procesadores**	6	**Velocidad Procesador (Ghz)**	2.53
Propiedad de equipo	N/A				
Consumo de potencia (Watts)	N/A	**Peso (Kg)**	N/A		
BIOS versión	Virtual American Megatrends 9.00.06		N/A		
Controlador RED	Microsoft Hyper-V Network Adapter	**Adaptador RAID**	N/A		
Memoria (GB)	12 Gb				
Rack de discos / discos internos	Virtual HD ATA Device				
Módulo de video	Microsoft Virtual Machine Bus Video Device				

CONFIGURACION DEL SERVIDOR			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Sistema Operativo	Windows Server 2016 SP2 Enterprise Edition	Windows Server 2016 Enterprise Edition SP2 5.2.3790 Build 3790	
Idioma	Español	**Kernel**	Windows NT 5.2.3790
Parches aplicados	Service Pack 2		
Particiones (File System)	C: 137 Gb Total – Usados: 32 Gb – Libres: 7 Gb – sin Asignar 98 Gb E: 137 Gb Total – Usados: 6 Gb – Libres: 91 Gb – sin Asignar 40 Gb		
Área de SWAP	15 Mb		
Antivirus	Avira Server Security		
Agente de Backup	N/A	**Agente Monitoreo**	N/A
ROLES DEL SERVIDOR			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Rol Primario	SERVIDOR Base de Datos		
Ambiente	Productivo	**Disponibilidad**	7x24
Criticidad del Servidor	Alta		
SOPORTE			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Fecha de Compra	Junio de 2016	**Fecha Vencimiento Garantía**	Extendida
Contrato de Mantenimiento	CMSERV-56TY678IJ – Proveedor		
ALMACENAMIENTO EXTENO			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Almacenamiento (GB)	N/A		
Tipo de almacenamiento	N/A		
Capacidad Almacenamiento	N/A		
Numero de HBA	N/A	**Velocidad HBA**	N/A

CONFIGURACIÓN DE RED			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Direcciones Estáticas	180.154.XX.XX		
IP ILO - IDRAC	N/A		
NIC 1	Activa		
IP	172.17.3.XXX	**Tipo de IP**	Estática
MAC	00-1F-29-E1-CE-54	**Gateway**	180.154.28.XXX
Velocidad de la tarjeta	1.0 Gbps	**VLAN**	13
Marca NIC	Microsoft Hyper-V Network Adapter		
DNS Primario	180.154.3.190		
DNS Secundario	180.154.3.131		

USUARIOS		
ADMINISTRADORES	**TIPO ACCESO**	**PERMISOS OTORGADOS**
Roque Avilez	Super administrador	Administradores, opers. de cuentas, admins. del dominio

SERVICIOS CRITICOS Y BASES DE DATOS	
1	Hyper-V Integration Services
2	Avira Server Security
3	Avira Managament Console
3	BDE Oracle 10g
4	Microsoft Visual C++ 2005
5	PostgreSQL 8.2
1	DHCP Client
2	DNS Client
3	Hyper-V Hearbeat Service, debe estar ejecutándose
4	Hyper-V Data Exchange Service, debe estar ejecutándose
5	Hyper-V Time Synchronization Service
6	Hyper-V Guest Shutdown Service
7	Hyper-V Volumen Shadow Copy Requestor
8	OracleCSService
9	OracleDBConsoleorcl
10	Oracleoracleas1ASControl
11	Oracleoracleas1ProcessManager
12	HelisaGW.DB (db software contable)
13	SI_SISCOMBA.DB (db Software de báscula)
14	SI_LABOARROZ.DB (db Software laboratorio arroz blanco y paddy)

9.1.3. Servidor de archivos

Permite almacenar y compartir información entre todos los usuarios de la red.

CONTROL DE ACTUALIZACIÓN			
REVISO		**ELABORO / ACTUALIZO**	
Área	TECNOLOGÍA	**Área**	TECNOLOGÍA
Nombre:	Ing. Roque Avilez	**Nombre:**	Carlos Parra Javier Mendoza
Cargo:	Jefe de Sistemas	**Cargo:**	Administrador de Servidores
Fecha:		**Fecha:**	01-05-2018
Firma:		**Firma:**	

CARACTERISTICAS GENERALES					
CARACTERÍSTICA	**DESCRIPCIÓN**				
Hostname	SRV-AP-FILE				
Tipo de servidor	Servidor Virtual	**Servidor Clúster**	No		
Marca y Modelo	N/A				
Ubicación del servidor	Centro de Cómputo				
Posición	SRV-AP-FILE	**Rack**	2		
Tipo de Procesador	Intel ® Xeon ® E5649	**Nº de Procesadores**	6	**Velocidad Procesador (Ghz)**	2.53
Consumo de potencia (Watts)	N/A	**Peso (Kg)**	N/A		
BIOS versión	Virtual American Megatrends 9.00.06		N/A		
Controlador RED	Microsoft Hyper-V Network Adapter	**Adaptador RAID**	N/A		
Memoria (GB)	12 Gb				
Raid controllers	N/A				
Rack de discos / discos internos	Virtual HD ATA Device				
Módulo de video	Microsoft Virtual Machine Bus Video Device				

CONFIGURACIÓN DEL SERVIDOR			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Sistema Operativo	Windows Server 2016 SP2 Enterprise Edition	Windows Server 2016 Enterprise Edition SP2 5.2.3790 Build 3790	
Idioma	Español	**Kernel**	Windows NT 5.2.3790
Parches aplicados	Service Pack 2		
Particiones (File System)	C: 99,4 Gb Total – Usados: 13.2 Gb – Libres: 86.2 Gb – sin Asignar 98 Gb E: 99.8 Gb Total – Usados: 1.3 Gb – Libres: 98.5 Gb – sin		
Área de SWAP	15 Mb		
Antivirus	Avira Server Security		
Agente de Backup	N/A	**Agente Monitoreo**	N/A

ROLES DEL SERVIDOR			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Rol Primario	SERVIDOR DE ARCHIVOS		
Ambiente	Productivo	**Disponibilidad**	7x24
Criticidad del Servidor	Alta		

SOPORTE HARDWARE			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Fecha de Compra	Junio de 2016	**Fecha Vencimiento Garantía**	Extendida
Contrato de Mantenimiento	CMSERV-56TY678IJ - Proveedor		

ALMACENAMIENTO EXTERNO			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Almacenamiento (GB)	N/A		
Tipo de almacenamiento	N/A		
Capacidad Almacenamiento	N/A		
Numero de HBA	N/A	**Velocidad HBA**	N/A

CONFIGURACIÓN DE RED			
CARACTERÍSTICA	**DESCRIPCIÓN**		
Direcciones Estáticas	172.17.3.XXX		
IP ILO - IDRAC	N/A		
NIC 1	Activa		
IP	180.154.28.XXX	**Tipo de IP**	Estática
MAC	00-1F-29-E1-CE-54	**Gateway**	180.154.28.XXX
Velocidad de la tarjeta	1.0 Gbps	**VLAN**	13
Marca NIC	Microsoft Hyper-V Network Adapter		
DNS Primario	180.154.3.190		
DNS Secundario	180.154.3.131		

USUARIOS		
ADMINISTRADORES	**TIPO ACCESO**	**PERMISOS OTORGADOS**
Roque Avilez	Super administrador	Administradores, opers. de cuentas, admins. del dominio

APLICACIONES Y BASES DE DE DATOS	
1	N/A
2	N/A
3	N/A
3	N/A
4	N/A
5	N/A

APLICACIONES Y/O SERVICIO CRÍTICOS	
1	DHCP Client
2	DNS Client
3	Active Directory Domain Services
4	Active Directory Web Services
5	Hyper-V Hearbeat Service, debe estar ejecutándose
6	Hyper-V Data Exchange Service, debe estar ejecutándose
7	Hyper-V Time Synchronization Service
8	Hyper-V Guest Shutdown Service
9	Hyper-V Volumen Shadow Copy Requestor

9.2. PROPUESTA DE EL PROCEDIMIENTO DE COPIAS DE RESPALDO Y RESTAURACIÓN

1) Descripción del Procedimiento	
1.1) Nombre del Proceso o Cadena de Valor (Procesos Misionales):	PROCEDIMIENTO PARA COPIAS DE RESPALDO Y PROTECCIÓN DE LA INFORMACIÓN
1.2) Nombre del Procedimiento:	PROCEDIMIENTO PARA COPIAS DE RESPALDO
1.3) Unidad Responsable:	ÁREA DE SISTEMAS
1.4) Objetivo:	Establecer los lineamientos para la realización de copias de respaldo de los recursos del sistema de información, propendiendo por que éstos se mantengan respaldados y sean recuperables en el momento en que se necesiten.
1.5) Alcance:	Este procedimiento inicia con la programación para la realización de las copias de respaldo de los servidores físicos, máquinas virtuales, aplicaciones y bases de datos de la empresa ARROPALMIRA SAS, según los instructivos respectivos y culmina con la verificación de la copia de seguridad.

2) Definiciones	
2.1) Concepto	**2.2) Definición**
CENTRO DE DATOS	Sala o construcción dispuesta para el alojamiento seguro de los equipos de cómputo necesarios para el procesamiento y almacenamiento de la información de una organización (Servidores, Discos externos, equipos de comunicación, etc.)
COPIA DE RESPALDO o BACKUP	Copia que se realiza a la información institucional definida como sensible o vulnerable, con el fin de utilizarla posteriormente para restablecer el original ante de una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos
EXPORT	Función para exportar configuración completa de máquinas virtuales a respaldar.

MAQUINA VIRTUAL (VM)	Una máquina virtual es un contenedor de software perfectamente aislado que puede ejecutar sus propios sistemas operativos y aplicaciones como si fuera un ordenador físico. Una máquina virtual se comporta exactamente igual que lo hace un ordenador físico y contiene sus propios CPU, RAM, disco duro y tarjetas de interfaz de red (NIC) virtuales (es decir, basados en software).
TIPOS DE BACKUP	Según la cantidad de datos copiados, los backup se dividen en: • **Total o Full**. Este tipo de backup hace un respaldo completo de todas las carpetas y archivos seleccionados, configuración de máquinas, entre otros. • **Incremental.** El backup incremental se usa para respaldos diarios, y copia únicamente los archivos que se modificaron después de una copia Total o del último respaldo Incremental. Para recuperar la información de un backup incremental se requiere del backup total y de todos los respaldos incrementales. • **Diferencial.** Un respaldo diferencial copia los archivos modificados luego de una copia Total. Al igual que el backup incremental, es usado para copias diarias. Para recuperar la información de un backup diferencial se requiere de este más el backup total.
SERVIDORES DE ALMACENAMIENTO	Equipo servidor dotado con arreglos de discos duros destinados a respaldar y compartir datos.
VACIADO DE INFORMACIÓN A DISCO	Traslado de la información respaldada y más crítica, (bases de datos y aplicaciones) a una unidad de almacenamiento ubicada en un lugar diferente al actual, el cual garantizará la existencia de un backup fuera de los centros de cómputo como lugar alterno.
Base de Datos:	Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las Bases de Datos son uno de los grupos de aplicaciones de productividad personal más extendidos.
ENTORNOS	• Preproducción: entorno en el cual se prepara una base de datos para dar inicio a un período contable. • Test: Entorno en el cual se crean bases de datos de pruebas

	• Producción: Entorno en el cual las bases de datos están activas
Recuperación de Bases de Datos	Consiste en extraer la información almacenada en medios externos, en una base de datos determinada.
RTO (Recovery Time Objective)	Es el tiempo máximo en el que se debe alcanzar un nivel de servicio mínimo tras una caída del servicio (por ejemplo, debido a pérdida de datos) para no causar consecuencias inaceptables en el negocio.
RPO (Recovery Point Objective)	Es el periodo de tiempo máximo en el que se pueden perder datos de un servicio. Si el periodo de tiempo es de 6 horas, se deben realizar backups cada menos tiempo y poder recuperar la información antes de agotar el periodo.
MySQL: mysqldump	realiza un volcado en los datos de la base de datos en SQL. Esto permite realizar backups y crear esclavos entre otros usos.
PostgreSQL: pg_dump	Hace, igual que mysqldump, un volcado de los datos en lenguage SQL.
Shell Script	Corresponde a un archivo de procesamiento por lotes, que por lo regular se almacena en un archivo de texto plano. El uso habitual de los scripts consiste en diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario.
CRONTAB	Es un archivo de GNU Linux que contiene las diferentes tareas programadas de los usuarios.
LIAVE RSA	(Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública
LIAVE DSA	(Digital Signature Algorithm) Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en su Estándar de Firma Digital (DSS), este algoritmo como su nombre lo indica, sirve para firmar el mensaje.
Backup por demanda:	Es el backup solicitado por un área específica, que puede encontrarse en un acuerdo de servicio o un backup eventual, que no tiene unos parámetros específicos (día, hora), y se debe solicitar al área de sistemas.
Backup por acuerdo de servicio	Es aquel backup que debe realizarse periódicamente por su criticidad y debe tener tiempos de ejecución e información a respaldar, los cuales están previamente

	definidos y contar con la aprobación del Jefe del Área de Sistemas.
Backup por política	Es aquel que se ejecuta según las políticas de backup establecidas, por base de datos y no cuentan con acuerdos de servicios.
Recuperaciones	Técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo).
Restauraciones	Volver a poner algo en el estado inicial, Una Base de Datos, una aplicación, se restaura en otro dispositivo después de un desastre.

3) Condiciones Generales
3.1. Los medios de respaldo para efectuar las copias de seguridad son los discos duros externos y de los Servidores de almacenamiento de datos, existentes para este fin.
3.2. Periodicidad de los backups. (Se realiza de acuerdo a lo relacionado en las bitácoras de backup). • Diarias: todos los días de la semana, exceptuando el domingo. • Semanales: Todos los domingos, exceptuando los que correspondan a fin de mes o año. • Mensuales: Los días que correspondan a fin de mes**.** • Anuales: Día final del año**.**
3.3. Los tipos de backup que se utilizarán en la empresa, serán **totales** e **incrementales**. Totales para copias semanales, mensuales y anuales; los incrementales se emplearán para respaldos diarios.
3.4. La ejecución de los backup se hará de forma manual, para servidores y configuraciones, utilizando Backup de Windows, Windows Server Backup, el Export de Hyper-V para máquinas virtuales; Los respaldos de bases de datos se generan usando un script.
3.5. El horario de ejecución o Lanzamiento de los backups debe llevarse a cabo en horas de poca o ninguna actividad laboral; por lo tanto, el horario de ejecución estará comprendido entre las 10:00 p.m. y las 6:00 a.m.
3.6. Las pruebas periódicas se realizan mensualmente de forma aleatoria para bases de datos, aplicaciones y servidores, en equipos asignados para tal fin. También se aprovechan las solicitudes de recuperación de datos borrados por los usuarios para hacer la prueba de los backups
3.7. Responsables
3.7.1. Ingeniero jefe de sistemas. • Diligenciar completamente la tarea establecida para la operación. • Seguir la matriz de escalamiento en caso de cualquier eventualidad. • Ejecutar las actividades descritas en los procedimientos.

• Verificar acuerdos de niveles de servicios. • Verificar o realizar la actividad solicitada.
3.7.2. Área Solicitante • Enviar la solicitud por correo electrónico
3.8. La información de los archivos contenidos en las copias de seguridad debe ser única y exclusivamente de uso de la empresa, no personales,
3.9. El área de sistemas no se hace responsable por el daño o la perdida de la información contenida en las computadoras de los usuarios que no almacenen su información en la unidad asignada.
3.10. La realización del vaciado de información está limitada únicamente para la información crítica de la empresa, esta información crítica contempla únicamente las Bases de Datos y las Aplicaciones definidas en el Inventario de Aplicaciones y Bases de Datos.
3.14. ¿Qué debe tener copias de respaldo?
3.14.1. Bases de datos: Administrativas: Financieras y de Operación.
3.14.2. Aplicaciones Administrativas: Financieras y de Operación.
3.14.3. Datos Administrativas: Financieras y de Operación.

9.3. PROPUESTA POLÍTICAS SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EMPRESA ARROPALMIRA SAS

Considerando que la Empresa ARROPALMIRA SAS es una empresa de compra, procesamiento, y venta de arroz y sus subproductos, y que debido a su amplio crecimiento ha ampliado su infraestructura tecnológica:

RESUELVE

Que el **ÁREA DE SISTEMAS** tiene como objetivo en la empresa, gestionar los recursos nuevos y actuales relacionados con las Tecnologías de la Información de acuerdo con los requerimientos internos y los avances tecnológicos aplicables para apoyar las labores de la misma.

El **ÁREA DE SISTEMAS** ha definido que, mediante la realización de un diagnóstico, se estableció e implementó un Sistema de Gestión de Seguridad de la Información SGSI, que permita cumplir con la preservación de la información.

POLÍTICAS

PSI-AP-001. GENERALIDADES

ART. 1: Preservar y administrar, la confidencialidad e integridad de la información de la Empresa ARROPALMIRA SAS.

ART. 2: Definiciones:

1. Activos de Información: Cualquier componente (humano, tecnológico, software, manuales, documentación, entre otros) que tiene valor para la organización y signifique riesgo si llega a manos de personas externas o no autorizadas.
2. Activo tecnológico: Todo aquel recurso tecnológico necesario para realizar las actividades productivas específicas de una organización.
3. Base de Datos: Conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación mediante un computador o cualquier otro dispositivo diseñado para tal fin.
4. Correo Electrónico Institucional. Recurso de la institución a disposición de los funcionarios, contratistas, docentes, estudiantes y egresados, el cual permite el envío y recepción de información institucional.
5. Credenciales de acceso: Privilegios de seguridad agrupados bajo un nombre y contraseña, que conceden acceso a los sistemas de información y/o áreas físicas definidas.
6. Custodio (de Activos de Información): Es el usuario y/o los usuarios finales o persona(s) que opera(n) el activo y que se asegura(n) que la información relacionada con este activo esté protegida.
7. Hardware: Todos los recursos tecnológicos físicos (por extensión también computadores virtuales) incluyendo equipos portátiles, servidores, impresoras, y por la dinámica actual también los dispositivos móviles, teléfonos inteligentes o dispositivos de almacenamiento extraíble.
8. Información: Datos (físicos, electrónicos, verbales) que conforman el conocimiento de la empresa, que sean necesario para cumplir con sus objetivos corporativos.
9. Información sensible o vulnerable: También llamado activo sensible, es el nombre que recibe la información personal o institucional (datos personales,

información financiera, contraseñas de correo electrónico, domicilio, datos de investigaciones), la cual, en caso de ser alterada, descompuesta, mal utilizada, divulgada y/o eliminada, puede causar graves daños a la organización propietaria.

10. Infraestructura: Las instalaciones físicas y servicios de suministro que contribuyen al cumplimiento de los objetivos de la organización. Entre los activos de la información de infraestructura se encuentran las oficinas, los centros de cómputo, los centros de cableado, los servicios de electricidad regulada y normal y el aire acondicionado.
11. Personas: Las personas también se deberían consideran activos de la información, porque ellos también tienen una gran cantidad de información y conocimientos (por lo general en sus cabezas), y suele ser muy común que esta información no esté disponible en otras formas.
12. Propietario (de Activos de Información): En la estructura administrativa de la institución, cada una de las unidades estratégicas, divisiones organizacionales, gerencias, rectorías o vicerrectorías a la cual se le otorga la propiedad del activo.
13. Recursos Tecnológicos: Todas aquellas aplicaciones, bases de datos, servidores, servidores web, equipos de comunicaciones, grabadores de video digital (DVR, Digital Video Recorder), impresoras, escáner de red y cualquier otro dispositivo tecnológico diseñado para la administración o el acceso a la información.
14. Redes de Computadores: También llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.
15. El responsable (de Activos de Información): El Jefe de Área, será el responsable ante el SGSI, de los activos de información registrados como de su propiedad.
16. Seguridad Física: Todos aquellos mecanismos (generalmente de prevención y detección) destinados a proteger físicamente cualquier recurso tecnológico del sistema.
17. 23. SGSI (Sistema de Gestión de Seguridad de la Información): Conjunto de políticas, procedimientos, guías, recursos y actividades administradas por una organización en procura de proteger sus activos de información. El término es utilizado principalmente por la ISO/IEC 27001.
18. Seguridad Informática: Proceso de prevenir y detectar el uso no autorizado de los recursos tecnológicos.
19. Seguridad de la Información: Son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.

20. Seguridad Perimetral: Corresponde a la integración de elementos y sistemas, tanto electrónicos, como lógicos y mecánicos, para la protección de perímetros físicos y/o virtuales, detección de tentativas de intrusión en instalaciones y/o sistemas de información especialmente sensibles.
21. Servidor: Equipo de computación físico o virtual, en el cual funciona un software, cuyo propósito es proveer servicios a otros dispositivos dentro de la red.
22. Sistema Operativo (SO) u Operating System (OS): Programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación.
23. Software: Programas y aplicaciones compiladas a partir de lenguajes de programación que cumplen funciones específicas para que los usuarios hagan uso del hardware para el tratamiento de la información en medios digitales.
24. WIFI (Wireless Fidelity): Dispositivo electrónico que permite intercambiar datos de forma inalámbrica en una red de computadores, incluyendo conexiones de Internet de alta velocidad.

ART. 3: Todo personal de la entidad, está obligado a reportar cualquier vulnerabilidad, riesgo o inconveniente presentado, con el fin de evaluarlos seguir ajustando el presente documento y los planes de contingencia dispuestos para los equipos de cómputo y el sistema operativo en cada uno de ellos. Por lo anterior, el personal del Departamento de Tecnología debe mantener un sentido ético y responsable de la información recibida de carácter personal y/o confidencial

PSI-AP-002. DISPOSICIÓN Y MANEJO DE LOS EQUIPOS DE CÓMPUTO

ART. 4: equipos de cómputo.

1. De ser necesario, se asignará a cada funcionario una estación de trabajo para apoyar al cumplimiento de sus labores.
2. Estos equipos son parte del patrimonio de la empresa.
3. Cada usuario es responsable del equipo que se le asigne, por lo que debe procurar su cuidado.
4. No deben ser trasladados los equipos a áreas diferentes a la que fue asignado sin previa autorización del área de sistemas.
5. Solo el personal del área de sistemas está facultado para abrir, desarmar, cambiar o instalar piezas del equipo de cómputo, así como formatear, instalar, reinstalar o modificar el sistema operativo o cualquier otro programa en la estación de trabajo.
6. No es permitido el uso de dispositivos de almacenamiento extraíbles como memorias USB o discos externos,
7. Los equipos deben estar conectados correctamente en las tomas de corriente regulada.

8. Evitar la exposición directa al sol o al polvo.
9. No está permitido fumar, así como tampoco el consumo de alimentos y/o bebidas en los puestos de trabajo.
10. Informar de forma oportuna cualquier incidente que impida el buen funcionamiento del equipo y/o del sistema operativo al Departamento de Tecnología.
11. Las solicitudes de instalación o cambio, ya sea del equipo completo o alguna de sus partes, deben ser aprobadas por los jefes del área solicitante y del Departamento de Tecnología.

PSI-AP-003. RED INTERNA

ART. 5: La empresa ARROPALMIRA SAS, asignará a cada usuario una cuenta para el ingreso a la red de datos, con la cual podrán acceder a una carpeta personal, así como otra para compartir archivos con los demás usuarios. Para el correcto uso y funcionamiento, se establecen lo siguiente:

1. Deben ser utilizados solo por personal de la empresa.
2. Los directorios asignados deben utilizarse sólo para fines empresariales, evitando guardar archivos personales además de fotos, música, videos o material innecesario.
3. Realizar una copia de seguridad de la información el último día laboral de la semana por cada usuario.
4. Evitar acceder, modificar o borrar información privada de otros usuarios ajenos a su propiedad.
5. Los archivos y carpetas almacenados en la red son propiedad de la entidad, sin que exista un derecho particular sobre ellos.
6. Queda terminantemente prohibido el uso de archivos o programas que permitan realizar actividades ilícitas.

PSI-AP-004. CUENTAS DE USUARIO

ART. 6: Cada funcionario debe estar identificado para acceder al sistema operativo y al sistema de información mediante una cuenta de usuario, la cual tendrá ciertos permisos o privilegios dependiendo del rol asignado. Para este ítem se aplicarán las siguientes reglas:

1. Toda solicitud de creación de cuenta o modificación de la misma debe realizarse por escrito, debidamente autorizada por los jefes del área solicitante y del Departamento de Tecnología.
2. Al entregar los datos de una nueva cuenta, el funcionario debe declarar que conoce y aplicará cada una de las políticas y procedimientos establecidos para el uso de la misma, aceptando las responsabilidades por el uso que se le dé a esta.

3. No se crearán cuentas de Invitado, tampoco a personal externo.
4. Sólo el personal autorizado del Departamento de Tecnología podrá eliminar una cuenta de usuario.
5. El Departamento de Gestión Humana deberá informar de manera oportuna situaciones que impliquen creación, modificación y/o borrado de cuentas de usuario, tales como rotación de personal, despidos o renuncias, etc., con el fin de mantener la base de datos de usuarios actualizada.

PSI-AP-005. AUTENTICACIÓN DE USUARIO

ART. 7: Se verifica que el usuario que intenta ingresar al sistema operativo sea quien die ser, mediante un mecanismo de autenticación, compuesto por la combinación de usuario y contraseña.

1. La contraseña es un conjunto de caracteres que cada funcionario debe entregar al sistema operativo y a la aplicación de la entidad para poder uso del equipo, debe contener caracteres en minúsculas y mayúsculas, números y al menos un carácter especial, completando un mínimo de ocho (8) caracteres.
2. Sólo los funcionarios debidamente autorizados, identificados y autentificados, tendrán acceso al sistema operativo y a los sistemas de información, limitados por los roles establecidos de acuerdo a sus funciones y responsabilidades.
3. El usuario y la contraseña deben ser de uso personal, siendo el dueño responsable de todas las acciones realizadas; confidenciales, ya que sólo el dueño debe conocerla; y además la contraseña debe ser robusta, que no sea fácil adivinar por terceros.
4. Queda prohibido imprimir o mostrar la combinación de usuario y contraseña.
5. Se limita a 3 intentos de acceso, después de éstos, se suspenderá por quince (15) minutos la cuenta. Si es necesaria la activación en menor tiempo, debe ser solicitado por escrito, debidamente autorizada por los jefes del área solicitante y del Departamento de Tecnología.

PSI-AP-006. INTERNET

ART. 8: ARROPALMIRA SAS, permitirá el acceso a internet a sus funcionarios, ~~de acuerdo a~~de acuerdo con las siguientes políticas:

1. Se utilizará solamente para fines laborales, evitando de esta forma saturar el ancho de banda, haciendo buen uso del servicio.
2. Queda prohibido el uso de redes sociales, páginas de entretenimiento, pornografía, violencia o cualquier otra ajena a las funciones diarias.
3. Queda prohibida la descarga de material ilícito o de contenido con derechos de autor.

4. No está permitida instalación de software que utilice el ancho de banda para acceder o descargar cualquier contenido, o para realizar llamadas nacionales o internacionales.
5. El Departamento de Tecnología estará facultada para filtrar páginas web, de tal modo que se controle el contenido servido y el ancho de banda utilizado. También podrá revisar de forma periódica los *logs* de navegación.

PSI-AP-007. CORREO ELECTRÓNICO

ART. 9: Es una herramienta que facilitará la comunicación del dueño de la cuenta, apoyando la gestión institucional de la empresa.

1. Sólo se permitirán usuarios permanentes de la institución.
2. Toda comunicación debe ser de carácter laboral.
3. Queda prohibido iniciar o responder cadenas de cualquier tipo.
4. Los usuarios deben ser precavidos al abrir mensajes de personas desconocidas, evitando abrir archivos adjuntos que puedan afectar el software instalado en el equipo.
5. Evitar el envío de correos de forma masiva, enviando los mensajes sólo a personas estrictamente necesarias.
6. Se limita el tamaño de envío y recepción de mensajes a 5MB de información adjunta.
7. No facilitar el usuario y la contraseña a terceras personas.
8. Queda prohibido el envío de correos con material ilícito, contenido sexual o violento.

PSI-AP-008. ADMINISTRACIÓN DE SERVIDORES.

ART. 10: En relación con los servidores y área de sistemas, se establecen las siguientes políticas:

1. El área de los servidores debe permanecer con acceso restringido, sólo el personal autorizado tiene permitido el ingreso.
2. Cualquier persona externa que ingrese a la Oficina de Sistemas, debe registrarse en la bitácora de ingreso, proporcionando su nombre, firma y motivo de ingreso.
3. Queda prohibida la manipulación de los equipos del área de servidores por personal no autorizado para ello.
4. Un conjunto de copias de seguridad de la información de los servidores debe ser trasladada a otro sitio seguro.
5. Todos los equipos deben estar conectados a un sistema de alimentación ininterrumpida de corriente eléctrica.
6. El cuarto de servidores debe estar en la temperatura adecuada, manteniendo un segundo aire acondicionado de respaldo.

PSI-AP-009. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

ART. 11: El escritorio de trabajo de todos los empleados de la empresa debe permanecer completamente despejado y libre de documentos controlados y/o reservados a la vista del público.

ART. 12: Todos los documentos controlados y/o reservados y en general, toda la documentación clasificada como “Información confidencial” debe permanecer guardados en un lugar seguro (archivadores con llaves o cajas fuertes), ya sea en un espacio físico o virtual, siempre que mantenga las debidas condiciones de almacenamiento y claves de acceso.

PSI-AP-010. BACKUPS O COPIAS DE SEGURIDAD

ART. 13: La responsabilidad de los ~~backups~~backup estará a cargo del personal del área de sistemas.

ART. 15: Se hará Respaldo a los archivos, aplicaciones, bases de datos y sistemas operativos de los servidores calificados como críticos para la empresa, siguiendo el documento procedimiento para copias de respaldo. Se incluye como información a respaldar las configuraciones completas de los servidores relacionados en el Inventario de Servidores Críticos.

ART. 14: La ejecución de las copias de seguridad debe llevarse a cabo en horas de poca o ninguna actividad laboral; por lo tanto, el área de sistemas será El responsable de definir el horario de ejecución de éstas.

Parágrafo. En los casos en que el backup no finalice exitosamente dentro de los tiempos establecidos, éste se relanzará después de evidenciado el fallo, en los tiempos establecidos en el procedimiento de Copias de Respaldo.

ART. 16: Cuando sea necesario un respaldo por demanda de los servidores críticos, se debe solicitar formalmente mediante correo electrónico por parte del personal autorizado, para informar mínimo con 24 horas de antelación sobre posibles interrupciones en el servicio a las personas afectadas.

ART. 17: Todos los respaldos se revisarán con la periodicidad definida en el Procedimiento de Copias de respaldo y se evidenciarán en la bitácora de backups.

ART. 18: La Comprobación periódica del estado de las copias se llevará a cabo con el fin de garantizar la disponibilidad e integridad de los datos almacenados. Los

responsables de la administración de equipos de respaldo masivo de datos evidenciarán la comprobación periódica del estado de las copias de seguridad en el formato para pruebas periódicas de restauración de ~~backups~~backup

PSI-AP-011. GESTIÓN DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

ART. 19: La Alta Gerencia de ARROPALMIRA SAS deberá aprobar un plan de continuidad del negocio para evitar las interrupciones en las actividades Misionales, como consecuencia de fallos, desastres o manipulación indebida de los sistemas que impidan su normal funcionamiento; el cual estará orientado a las dependencias involucradas en el SGSI, teniendo en cuenta la fase de análisis de riesgos.

ART. 20: La revisión del Plan de Continuidad de Seguridad de la Información debe hacerse con la periodicidad definida por la entidad, dependiendo de los cambios y nuevos requerimientos en los procesos.

PSI-AP-012. CAPÍTULO V APLICABILIDAD

ART. 21: Ámbito de Aplicación. Esta política aplica a todos los procesos y procedimientos, así como a todas las actuaciones administrativas que desarrollen sus distintas áreas, por intermedio de sus empleados.

PSI-AP-013. EXCEPCIONES

ART. 22: Existirán algunos casos en los que no una política específica, ya que no pueden ser creadas e impuestas en un 100% para todas las actividades de la institución. En los casos en que sea necesaria la ejecución de acciones que estén en conflicto con una o varias políticas estipuladas en este documento, se procederá de acuerdo a la siguiente instrucción:

Parágrafo: Cualquier funcionario que siguiendo sus obligaciones laborales observe la necesidad de aplicarse una excepción a una determinada política, deberá informarla por escrito al Departamento de Tecnología, el cual evaluará el caso y determinará si es o no válida la excepción, basándose en un análisis de riesgos. En caso de ser válida, enviará comunicación por escrito informando la duración de la excepción y los riesgos a los cuales se expondrá, informando los pasos que debe seguir. Al finalizar el tiempo expuesto, se valorará la continuidad de la excepción, que deberá ser evaluada y aprobada nuevamente, siguiendo los mismos lineamientos.

PSI-AP-013. SANCIONES

ART. 23: Todo el personal de la entidad queda sujeto al cumplimiento de las normas aquí expuestas, so pena de ser sancionado disciplinaria y/o legalmente, si hubiera lugar a ellas. Las sanciones van desde un llamado de atención hasta la suspensión del cargo, dependiendo de la gravedad de la falta cometida, además de la malicia o perversidad con que se cometa.

La Ley 1273 establece los atentados contra los sistemas de información, afectando la confidencialidad, integridad y disponibilidad de los datos, para lo cual se regirá de acuerdo a ésta para efectos de sanciones legales.

10. CONCLUSIONES

Con desarrollo del presente trabajo, se logró evidenciar la importancia de efectuar un diagnóstico y análisis de riesgos en una empresa, permitiendo identificar los puntos vulnerables o las falencias existentes para proponer controles que minimicen el impacto que pudieran tener en la organización de ser explotadas, por otra parte, se logró estudiar algunas metodologías de riesgos de seguridad informática, observar sus fases y a través de estas, proponer los pasos metódicos que se siguieron en el desarrollo del proyecto, es importante resaltar que también se estudió la norma ISO27001:2013 y se observó la importancia de aplicar algunos de los controles que propone, en beneficio de la empresa Arropalmira S.A.S.

De acuerdo con los resultados obtenidos en el desarrollo del trabajo, se puede establecer que la falta de conocimiento sobre la importancia de la seguridad de la información permite que se realicen malas prácticas u omisión de controles, debido a la falta de políticas que permitan la protección de la información de forma adecuada.

Cabe destacar que luego del diagnóstico del estado actual de la seguridad de la información en la empresa Arropalmira S.A.S. y el respectivo análisis de su situación, se propone un plan de mejoramiento que puede apoyar a futuro la implementación de un SGSI.

11. RECOMENDACIONES

De acuerdo con el desarrollo del presente proyecto se recomienda que la empresa Arropalmira S.A.S., implemente, mantenga y actualice de forma constante los siguientes aspectos:

- Diagnósticos de seguridad informática: Es recomendable que se realice la revisión de cada ítem contenido en el diagnóstico anualmente, debido a que se pueden presentar cambios dentro de la infraestructura de TI de la Empresa Arropalmira S.A.S.

- Implementación de políticas: Es importante que se realice la implementación y actualización constante de las políticas presentadas en el documento con el fin de verificar que se esté dando cumplimiento y poder garantizar la seguridad de la información de la empresa.

- Procedimientos: La empresa debería implementar cada uno de los procedimientos recomendados en el presente proyecto, al igual que debería mantener una actualización constante de los mismos de acuerdo con la alta gerencia y las personas implicadas.

- Formatos: Para una adecuada organización se hace necesario que la empresa implemente los formatos propuestos y realice las respectivas actualizaciones en su sistema de gestión documental, teniendo en cuenta que de esta forma se lleva un control de cambios en la infraestructura de TI de la empresa.

12. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación del mismo; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de diagnóstico de seguridad en empresas, puedan acceder al documento.

BIBLIOGRAFÍA

CALDERON, Hugo. Metodología de la investigación científica, Tipos de investigación 2014, UNIVERSIDAD NACIONAL DEL SANTA Escuela Académica Profesional Ingeniería en Energía, Disponible en: http://biblioteca.uns.edu.pe/saladocentes/archivoz/curzoz/002_clase4.pdf

CAMELO, Leonardo. Seguridad de la Información en Colombia. Seguridad de la Información y Seguridad Informática. [En línea].2010. Disponible en Internet: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html.

Carvajal, (2008). Análisis y Gestión del Riesgo, Base Fundamental del SGSI, Caso: Metodología Magerit Disponible en: http://52.0.140.184/typo43/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf https://www.ccncert.cni.es/documentospublicos/1789-magerit-libro-i-metodo/file.html

CEBALLOS, Adriana, BAUTISTA, Fredy, otros… "Informe de las tendencias del cibercrimen en Colombia (2019-2020)", Primera edición, Bogotá D.C. Octubre 29 de 2019.

CISNEROS, M. (2012). Cómo elaborar trabajos de grado (2a. ed.). Recuperado de http://bibliotecavirtual.unad.edu.co:2055/lib/unadsp/docDetail.action?docID=10626100&p00=C%C3%B3mo+elaborar+trabajos+de+grado

Conpes 3854, Departamento Nacional de Planeación, Republica de Colombia. "Política Nacional de Seguridad Digital" Bogotá D.C. abril 11 de 2016.

DALTABIT GODAS Enrique, VASQUEZ, José. "La Seguridad de la Información" Limusa Noriega Editores, 2007. Pág. 215.

DEJAN, Kosutic. la importancia de la declaración de aplicabilidad para la norma ISO 27001, 2015. Disponible en: https://advisera.com/27001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/

Dirección General de Modernización Administrativa, P. e. MAGERIT –versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, octubre de 2012, Libro II. Madrid: © Ministerio de Hacienda y Administraciones Pública.

Estándares y Normas de seguridad. Recuperado de; http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf

Fortalecimiento de la gestión TI en el estado {En línea} disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelode-Seguridad/
GÓMEZ VIEITES, Álvaro. Enciclopedia de la seguridad informática, 2 ed. México: Alfaomega, 2011.

GUINDEL, Esmeralda. Calidad y seguridad de la información y auditoría informática, calidad y seguridad de la informacion,2010, Trabajo de grado (ingeniería técnica de informática de gestión), Universidad Carlos III de Madrid Disponible en: http://e-archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf?sequence.

Gobierno de Colombia (2018). 7. Estructura general del modelo nacional de gestión de riesgos de seguridad digital.

HERNÁNDEZ SAMPIERI, C. Roberto; FERNÁNDEZ COLLADO, Carlos y BAPTISTA, pilar. Metodología de la investigación, Bogotá D.C: Editorial Mcgraw-Hill. Panamericana, 1997

INTECO, Implantación de un SGSI en la empresa. Plan avanza2. Pág. 22.

INTERPOLADOS. (2018). MAGERIT V.3: metodología de análisis y gestión de riesgos de los sistemas de información. 2018, octubre 2, de INTERPOLADOS

Recuperado de https://interpolados.wordpress.com/2018/10/02/magerit-v-3-metodologia-de-analisis-y-gestion-de-riesgos-de-los-sistemas-de-informacion/

ICONTEC, NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001{En línea} disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

ISOTools Excellence. ISO 27001: ¿Cuál es la estructura de la nueva norma ISO 27001 2013
{En línea} disponible en(https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/).)

ISOTools Excellence. ISO 27001: ¿Qué significa la Seguridad de la Información? {En línea} disponible en:(http://www.pmgssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion).

JAUREZ, Hector. (08 de noviembre de 2011) ISO-27001: ¿Qué es y para qué sirve? [en línea] -http://www.magazcitum.com.mx/?p=1574#.Vyfm6fnhCM8

LÓPEZ MATACHANA, Yansenis, Los virus informáticos: una amenaza para la sociedad, Cuba: Editorial Universitaria, 2009.

LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. El portal de ISO 27001 en español, ISO 27000. Disponible en: http://www.iso27000.es/index.html

Magerit v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [On line]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VRMl5_yG8ms.

Manual de diagnóstico y prevención de vulnerabilidades de datos para pymes {En línea} disponible en: https://repository.unad.edu.co/bitstream/handle/10596/15026/80225921.pdf?sequence=1&isAllowed=y

MENDOZA, Miguel. Identificación y análisis a la gestión de riesgos de seguridad, Gestión de riesgos de seguridad, 2015, Welyvetsecurity, Disponible en: http://www.welivesecurity.com/la-es/2015/07/16/analisis-gestion-de-riesgos-seguridad.

MINTIC. República de Colombia. Modelo de seguridad de la información. Sitio web: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf Notas de la versión de Nessus. Seguridad de red sostenible.

MINTIC, Republica de Colombia. Modelo de Seguridad y Privacidad de la Información. “G7 – Guía de gestión de riesgos” 2016.

MINTIC, Republica de Colombia. Modelo de Seguridad y Privacidad de la Información. “G2 – Guía elaboración de la política general de seguridad y privacidad de la información” 2016.

R. Alexandra, O. Zulima. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios, Ingeniería 16(2), 56-66

RAMIREZ, G. y CONSTAIN, G. Modelos y estándares de seguridad informática. UNAD, febrero de 2012.

RUBEN, A. Kali Linux. Recuperado de: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671. 2016.

SEAQ. Acunetix Web Vulnerability Scanner. Recuperado de: https://www.seaq.co/acunetix.html, mayo de 2018.

Seguridad 7” A” Metodología NIST SP 800-30 (National Institute of Standards and Technology), [On line]. Disponible en: http://seguridades7a.blogspot.com/p/nist-sp-800-30.html

TECCELAYA. Norma, Estándar, http://equipoteccelaya.blogspot.es/1234029360/

Telefónica, F. "Ciberseguridad, la protección de la información en un mundo digital" Editorial Ariel, S.A, 2016

Tenable. La familia Nessus. {En línea} disponible en: https://es-la.tenable.com/products/nessus

UNIR, Políticas de Seguridad Informática. Unir Revista en línea. Mayo 14 de 2014: https://www.unir.net/ingenieria/revista/noticias/politicas-seguridad-informatica/549204996232/

UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme? [En línea]. Marzo, 2018. Disponible en internet: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

UNIVERSIDAD LIBRE. Seguridad de la Información. [En línea]. Disponible en internet: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

UNIVERSIDAD VERACRUZANA. Introducción a la seguridad de la información. [En línea]. Disponible en internet: https://www.uv.mx/celulaode/seguridad-info/tema1.html

ZAMORA, Julián. Cyber Security. “Gestión de Ciber Riesgos” 2020.