DISEÑO SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA ORIENT

MACEDONIO NAVARRO BAHAMON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2020

DISEÑO SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA ORIENT

MACEDONIO NAVARRO BAHAMON

Proyecto de grado para optar al título de Especialista en Seguridad Informática

CESAR ENRIQUE SILVA
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ibagué, Diciembre del 2020.

DEDICATORIA

Este proyecto lo dedico primero a Dios, quien nos brinda a diario sabiduría y discernimiento para tomar adecuadas decisiones, de igual forma se lo dedico a mi familia quienes siempre están para apoyarme en cada una de las circunstancias de mi vida y junto a mi celebran cada meta propuesta.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia por la oportunidad de ingresar en la especialización de seguridad Informática, también a los tutores: Cesar Enrique Silva por su valiosa colaboración, tiempo y dedicación, a las dudas e inquietudes que he tenido a la hora empezar a desarrollar el diseño del sistema de gestión de seguridad de la información para la joyería Orient en Colombia.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZA: Posibilidad que suceda cualquier eventualidad terminando en algún daño del bien o servicio dentro en la empresa.

ANALISIS DE RIESGO: Proceso que permite comprender la naturaleza del riesgo actual en la joyería Orient, además de medir o determinar el nivel de riesgo al que se encuentra expuesta.

ATAQUE: Cualquier tipo de intento de afectar de manera negativa cualquier activo en la empresa.

BORRADO SEGURO: Proceso por el cual se asegura la eliminación de archivos contenidos en una base de datos o sistema, bajo un proceso documentado.

BSI: British Standards Institution, la entidad de normalización del Reino Unido, responsable en su día de la publicación de la norma BS 7799, origen de ISO 27001. Su función como entidad de normalización es comparable a la de AENOR en España.[1]

CIBERDELITO: La ejecución de un delito por medio de una medio informático o digital el cual conlleve a un daño, perdida o cualquier modificación no autorizada en el sistema.

CONFIDENCIALIDAD: Es un determinante fundamental en el funcionamiento de cada proceso en la empresa, siempre protegiendo la Información o datos de acuerdo al privilegio del usuario.

CONTROL: Son todos aquellos procesos o buenas practicas que puedan llegar a minimizar o proteger un activo de un amenaza o riesgo dentro de la empresa, algunos sinónimos para este son salvaguardas o contramedida.

DISPONIBILIDAD: para poder cumplir con los estándares requeridos de servicio en la empresa es fundamental tener la disponibilidad de la información y recursos necesarios para poder ejecutar cualquier proceso o acción en la empresa.

ESTÁNDARES DE SEGURIDAD: La gestión de los activos de la empresa y para garantizar la rentabilidad de la misma, la empresa ha intentado estructurar los lineamientos técnico necesarios para proteger los activos y siempre en la búsqueda de mejorar y estar a la vanguardia.

[1] ISO27000.ES. 2020. Disponible en: https://www.iso27000.es/glosario.html.

FUGA DE DATOS: La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.[2]

GESTION DE CLAVES: Son todos aquellos controles que se pueden gestionar referentes al proceso de criptográfica en relación a llaves de acceso a la información en la empresa.

GESTIÓN DE RIESGOS: En la gestión del riesgo en la Orient, siempre ha sido dirigido hacia la mitigación de las acciones que puedan generar algún tipo de riesgo o amenaza a la misma, en la actualidad se están tomando en consideración a la información como uno de los activos más importantes de la misma.

IMPACTO: Es lo que puede llegar afectar para la empresa un incidente, se ha positivo o negativo y en diferentes escalas acorde a la implicación en este caso de la seguridad y el riesgo para la empresa.

INTEGRIDAD: En la Joyería Orient la integridad de la información y de los procesos permite garantizar a los accionistas y usuarios que los procesos son de alta calidad y la información es veraz.

LA INFORMACIÓN: Considerado el recurso estratégico más importante de la empresa, dicho recurso permite producir movimientos bursátiles, con le fin de originar reestructuraciones sectoriales, por lo que disminuye la importancia de la mano de obra y del capital como motor económico; sentando las bases de una nueva tecnología de la información en las empresas, instituciones de todo tipo y en la sociedad en general, cuyo símbolo más representativo es el fenómeno de Internet[3].

MODELO DE SEGURIDAD: Estructura o modelo por el cual se trabajan las políticas de seguridad, de la gestión del riesgo y la valoración de activos; siendo un modelo evolutivo y cambiante el cual busca mitigar riesgos para mantener el control de la empresa; En la actualidad se encuentran el proceso de valorar la información y datos como uno de los activos más valiosos de la misma por lo cual el modelo de seguridad debe empezar a actualizarse.

---

[2] INSTITUTO DE CIBERSEGURIDAD - INCIBE. Glosario de términos de ciberseguridad. Una guia de apoximacion para el empresario. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

[3] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES COLOMBIANAS. Seguridad y privacidad de la información. Rols y responsabilidades. Guia No. 4. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf.

PHPMYADMIN: Ha Permitido gestionar y administrar las bases de datos de los equipos remotos a través del navegador Web.

POLÍTICAS DE SEGURIDAD: en este caso la empresa ha sido consciente del riesgo que tiene, constantemente lo cual ha ocasionado que la misma mantenga en constante evolución de los lineamientos para asegurar la seguridad de los activos y hoy en día por esta razón también la información en una empresa.

POSTGRESQL: Es el gestor de base de datos en el que toda una comunidad de la empresa actualmente trabaja para el funcionamiento de los diferentes servicios ofrecidos.

RIESGO: En la empresa la probabilidad de algún daño o amenaza es alta ya que el valor individual de los activos es alto en el mercado y por eso cualquier acción o proceso tiene un riesgo alto en referencia al impacto.

RESUMEN

De acuerdo a la preocupación actual que se presenta en el mundo y en Colombia frente a los riesgos, vulnerabilidades y peligros que influyen en la seguridad de los datos de la información para el funcionamiento de una empresa, la presente propuesta tiene como objetivo realizar el diseño del SGSI para la Joyería Orient en Colombia, por medio de un análisis y valoración del riesgo de activos, lo cual permitirá implementar controles y políticas en la seguridad de la información, así mismo, de manera transversal permitirá conocer el estado actual del sistema de gestión de seguridad de la información en base al Anexo A ISO 27001-2013, identificar los posibles activos de la información y riesgos de la Joyería Orient, teniendo en cuenta la metodología MAGERIT y finalmente definir las políticas de seguridad y los controles necesarios para mejorar el sistema de gestión de seguridad de la información. Dicho proceso, podrá ser aplicado a todos los funcionarios operativos, administrativos, pasantes o contratistas que utilicen los recursos, sistemas de información o infraestructura de comunicaciones y tecnologías de la información en la Joyería Orient y sus sedes. Todo esto con el fin de fortalecer la seguridad de la información en la empresa.

Palabras clave: Amenazas, Controles, Magerit, Políticas, Riesgos, Salvaguardas, Seguridad Informática, Servicios, Sistema De Gestión.

ABSTRACT

According to the current concern that exists in the world and Colombia regarding the risks, vulnerabilities and dangers that influence the security of information data, for the operation of a company, this proposal aims to carry out the design of the ISMS for Orient Jewelery in Colombia, through an analysis and assessment of the risk of assets, which will allow to implement controls and policies on information security, likewise, in a cross-sectional way will allow to know the current state of the management system of information security based on Annex A ISO 27001-2013, identify the possible information assets and risks of Orient jewelry, taking into account the MAGERIT methodology and finally define the security policies and controls necessary to improve the system of information security management. Said process may be applied to all operational, administrative, intern or contractor officials who use the resources, information systems or communications infrastructure and information technologies in Orient jewelry and its headquarters. All this in order to strengthen the security of information in the company.

Keywords: Computer Security, Controls, Threats, Magerit, Management System, Policies, Risks, Safeguards, Services.

INTRODUCCIÓN

La finalidad de crear un diseño de sistema de seguridad informático va acorde a la necesidad de la protección de los datos, el cual hace parte de los activos valiosos de los procesos corporativos; dado el crecimiento mundial en el procesamiento y traslado de la información, vs la necesidad de Colombia en ir acorde a la evolución digital, lo cual permitiría brindar respuestas concretas a las grandes industrias. Por ello se inicia con el diseño de un sistema de gestión de seguridad de la información para una mediana empresa, lo cual podría ser un modelo para ser implementado en las grandes corporaciones de acuerdo con la evolución de las diferentes etapas del proyecto.

Actualmente las medianas empresas se han caracterizado por no brindar mayor importancia, y mucho menos por contar con sistemas de información acordes a las necesidades inmediatas el cual les permita contar con datos protegidos, actualizados y adquirirlos de forma rápida, sencilla, según los procesos y necesidades corporativos. A pesar de la normatividad existente, pocas empresas han logrado desarrollar de forma esperada; la adecuada gestión de la seguridad informática, por lo que a las que no lo han implementado les acarrea problemas de ejecución y calidad de los procesos, haciendo que estos sean extensos y poco seguros para los usuarios y proveedores.

Para ello se plantea el diseño de sistema de seguridad informático para la Pyme Joyería Orient, aplicando el anexo A de la ISO 27001, con el fin de determinar el estado de madurez de la seguridad de la información de la misma, y evaluando las necesidades corporativas en cuanto al manejo de la información y le flujo del mismo dentro de la Joyería; mediante un análisis de vulnerabilidad, identificación de activos, verificar la necesidad de la creación de controles y políticas que aseguren la protección de datos, así como la prevención de ataques cibernéticos, estructurales o funcionales que llegaran afectar el funcionamiento y productividad de la empresa[4].

Esto se realizará mediante la inclusión de un especialista en seguridad informática, donde de acuerdo con la evaluación realizada, diseñe el sistema de gestión de seguridad de la información y realice un plan de acción para el mejoramiento inmediato, fortaleciendo el mismo y asegurando que la Joyería Orient pueda estandarizar la calidad de los servicios y la información, como valor agregado y así proyectarse a ser más competitivos en el mercado.

[4] COBIT-MODELO-DE-MADUREZ. Ipmoguide. 2019. Disponible en: https://ipmoguide.com/cobit-modelo-de-madurez/.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La Joyería Orient es una empresa familiar y tradicional de la ciudad de Ibagué desde 1947, y durante toda su trayectoria sus únicos activos eran los productos que comercializan, como lo son joyas, relojes, artículos y accesorios exclusivos para caballeros y damas, siempre estando a la vanguardia de los cambios comerciales y adaptándose poco a poco a los cambios tecnológicos es por eso que hasta hace poco pudieron percibir que la información es uno de los activos más valiosos para una empresa tanto para controles dentro de la compañía, como para generar estrategias de mercado, por tal razón las directivas de la empresa han requerido el asesoramiento en el diseño de un sistema de seguridad de la información el cual les permita reconocer los activos, identificar vulnerabilidades, gestionar una matriz de riesgo definiendo los controles para minimizar riesgos, gestionar políticas de seguridad de la información todo esto para asegurar y proteger la confidencialidad, disponibilidad e integridad de los datos de sus sistemas de información, y así mismo prevenir ataques a sus servidores o fallas en sus sistemas de información[5].

Teniendo en cuenta que las falencias informáticas, es importante buscar una ayuda que le permita a la Joyería Orient tomar las decisiones correctas, adecuadas y afortunadas con respecto a la seguridad de los datos, como lo indica el rápido avance de los marcos de datos en todo el mundo y de esta manera convertirse en una Contribución vital para garantizar la infraestructura y los procedimientos, a la luz de las mejores prácticas de flujo y reflujo. Para abordar este problema para la Orient, es importante tener el asesoramiento y acompañamiento sobre modelos de seguridad de la información que deben incorporar modificaciones y actualizaciones a los acuerdos, directrices, métodos, medidas, y además exposiciones para todos los clientes de la organización.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es la pertinencia de un diseño del sistema de gestión de seguridad de la información para la Joyería Orient?

[5] JOYERIA ORIENT. Disponible en: https://www.joyeriaorient.com/sobre-nosotros/.

2. JUSTIFICACIÓN

Los procesos empresariales y el desarrollo de los mismos han generado la importancia de los sistemas de información en las compañías, así mismo se ha identificado que a pesar de ser uno de los activos más importantes para las mismas, es uno de los factores más vulnerables; por ende la seguridad de la información brinda no solo a las empresas, si no que a todos los procesos que maneje datos contar con un blindaje de los mismos, eficiente, confidencial y permanente en el tiempo, de acuerdo a las necesidades inmediatas.

De acuerdo a lo anterior, se logra identificar que la seguridad de la información para las compañías no es un factor relevante de prestar atención, ya que este no es visto como un generador de ingresos tangibles; de igual forma el desconocimiento de los diferentes factores que influyen a nivel de la seguridad de la información y la inexperiencia de los riesgos a los que están expuestos, podrían generar pérdidas en tiempo y recursos; por lo que este tipo de temas no han sido relevante para las mismas, generando en un futuro el deterioro o afectación en el manejo de los datos.

Por ende, es importante que las empresas cuenten con conocimiento de los beneficios de un sistema de seguridad de información que les brinde protección, accesos autorizados a los datos confidenciales y permanencia de estos; así como metodologías, normas y procesos que permitan la eficiencia del almacenamiento, protección y acceso a los datos; procediendo a la mitigación de los riegos y amenazas asociadas a una inadecuada administración de los sistemas de la información.

Para ello, un diseño de SGSI define una serie de respuestas a las necesidades propias corporativas como lo son: la estandarización de la estructura de la información acorde a los requerimientos internacionales, contar con normas y políticas de adecuado al tratamiento de la información, optimizar costos y tiempos en la búsqueda de activos, confianza y efectividad a los requerimientos de los clientes, además del cambio de enfoque respecto a la importancia de un adecuado SGSI.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar el SGSI a partir de un análisis y valoración del riesgo de los activos, basado en la evaluación diagnostica de la situación actual de la Joyería Orient en Colombia.

3.2 OBJETIVOS ESPECÍFICOS

- Determinar el estado actual del sistema de gestión de seguridad de la información mediante el Anexo A ISO 27001:2013.

- Identificar los posibles activos de la información y riesgos de la joyería Orient, teniendo en cuenta la metodología MAGERIT.

- Definir las políticas de seguridad y los controles necesarios para mejorar el sistema de gestión de seguridad de la información en la Joyería Orient.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La Joyería Orient en Colombia, actualmente ha tenido en cuenta que la información es uno de los activos más importante dentro de una compañía; y por esta razón se determina un análisis informático, el cual les permita conocer el estado actual de seguridad de la información, la valoración de activos y los posibles controles para minimizar cualquier riesgo, lo cual, les va a permitir tener una rentabilidad mayor a los nuevos retos en la actualidad, evitando así futuros ataques cibernéticos.

Por esta razón en el desarrollo del proyecto se implementará un proceso de análisis y gestión que son fundamentales para la protección de la organización, ya que es el proceso más sensible y con mayor destreza en un SGSI, por lo cual es un proceso en el cual debemos conocer el funcionamiento global de la organización, identificando los siguientes pasos:

- Identificar activos, procesos
- Identificar la relación y el funcionamiento de los activos
- Identificar las vulnerabilidades de estos
- Valorar activos, procesos
- Valorar el impacto de dichas vulnerabilidades de acuerdo con el valor del activo o proceso
- Diseñar los debidos controles para mitigar dichas vulnerabilidades
- Realizar un seguimiento continuo del funcionamiento de la organización y sus vulnerabilidades

Lo anterior son normalmente los pasos requeridos para la implementación de un SGSI en una organización, para ello existen varias metodologías las cuales ayudan a establecer parámetros o normas, que permiten llevar a cabo los procesos. Dentro de las diferentes metodologías con mayor relevancia a nivel mundial se encuentran la MAGERIT, OCTAVE o la EBIOS, debido al gran impacto positivo en las organizaciones.

Durante los procesos de Análisis y Gestión de riesgos se debe tener claro que la información tiene tres aspectos fundamentales: Disponibilidad, Integridad y Autenticidad de la información; por ende, es que se realiza la implementación de SGSI, para poder llevar a estos procesos y un análisis exitoso. Para ello la

aplicación de un sistema de gestión de seguridad de la información en base a una norma como la ISO 27001:2013, le permitirá a la empresa tener un modelo de buenas prácticas conocido a nivel mundial y esto generará a la organización estar a la vanguardia en la seguridad de sus activos de la información[6].

Es así que lo largo del trabajo de grado se utilizarán diferentes conceptos, algunos los encontraremos definidos en el 4.3 MARCO CONCEPTUAL, los cuales permitirán contextualizar aún más el fundamento del proyecto.

4.2 ANTECEDENTES

De acuerdo con las diferentes investigaciones llevadas a cabo respecto SGSI y la protección de los sistemas de información para evitar futuros ataques cibernéticos, se toma como punto de referencia algunos proyectos encaminados en el área:

Para el año 2016 en el Proyecto de grado nombrado Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 para positiva compañía de seguros S.A. en la ciudad de Bogotá[7]; donde se propuso Diseñar un SGSI para la empresa en mención; a través una investigación exploratoria, por lo que el diseño brindo a la compañía la sensibilización con el envío de alertas de seguridad informática, así como alertas emitidas en cuanto a cualquier situación cibernética pueda generar fraudes y colocar en riesgo la compañía.

En el Proyecto de grado aplicado nombrado Análisis de seguridad al sistema de la Registraduría nacional de Colombia[8] en el 2018; donde se propuso identificar vulnerabilidades para actualizar el SGSI en la empresa en cuestión, mediante una investigación exploratoria, donde se logró preparar la protección del sistema y de sus activos de información, contra posibles ataques y amenazas, teniendo en cuenta que la defensa debe estar alineada al MSPI (Modelo de Seguridad y Privacidad de la Información)

[6] GÓMEZ VIEITES, Álvaro. Anexo III Análisis y Gestión de Riesgos en un Sistema Informático. Disponible en: https://www.academia.edu/5971566/Anexo_III_An%C3%A1lisis_y_Gesti%C3%B3n_de_Riesgos_en_un_Sistema_Inform%C3%A1tico.

[7] ARDILA NAVARRETE, Julián Andrés. Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para Positiva Compañía de Seguros SA en la ciudad de Bogotá. Universidad Nacional Abierta y a Distancia. Bogotá, 2016. Disponible en: file:///C:/Users/Usuario/Downloads/79218306.pdf

[8] NAVARRO BAHAMON, Macedonio y TRUJILLO HERNÁNDEZ, Carla Patricia. Análisis de seguridad al sistema de la Registraduría Nacional de Colombia. 2018.

Para el año 2011 en el Proyecto de Grado nombrado Diseño del sistema de gestión de seguridad de la información en angelcom S.A.[9] Busca evidenciar el proceso de transformación de la seguridad en la información de Angelcom S. A., con el fin de aumentar su competitividad dentro de un lineamiento de proveedor confiable para operar como concesión en la explotación económica del Recaudo del Sistema TransMilenio S.A. por lo que identificaron en la compañía la necesidad de la definición de funciones, y responsabilidades mediante la implementación de medidas como lo son la valides jurídica de las evidencias, implantación de medidas por medio de la comunicación de información con terceros, garantizar la información de las contrataciones con terceros, concientización por parte de la empresa en fundamentar sus procedimientos de acuerdo a las normas estipuladas.

Al evidenciar investigaciones precedentes, permiten ampliar el espectro de la estructura, formulación y desarrollo del proyecto, brindando claridad en el desarrollo de los objetivos y el diseño de un sistema de gestión de seguridad de la información.

4.3 MARCO CONCEPTUAL

4.3.1 Seguridad Informática. Área encargada de la protección de los sistemas informáticos por medio de algunas prácticas ejecutadas, la cual se logra con la implementación de políticas diseñadas para proteger un bien o un servicio, haciendo uso de herramientas de defensa como lo son: Antivirus, Firewalls, Detección de anomalías, entre otros[10].

4.3.2 Norma ISO/IEC 27001-2013. Normatividad por la cual se registran y se establecen los requisitos fundamentales y acciones para la implementación y diseño de un Sistema de Gestión de Seguridad de la Información, mediante la puesta en marcha de políticas y el uso del ciclo PVHA (Planear, Hacer, Verificar y Actuar)

La norma esta dividía en dos secciones para su aplicabilidad la primera consta de 10 ítems, los cuales deben ser tratados o tomados en cuento al momento en cuanto al conocimiento de la funcionalidad de la empresa, como lo son: Objeto y campo de aplicación, referencias normativas, Términos y Definiciones, Contexto de la organización, Liderazgo, Planificación, Soporte, Operación, Evaluación de desempeño y mejora.

[9] HERNÁNDEZ MEDINA, Diana Carolina. Diseño del sistema de gestión de seguridad de la información en Angelcom S.A. Universidad Libre. Bogotá, D.C. 2011. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/9097/PROYECTO%20FINAL.pdf?sequence=1&isAllowed=y

[10] GÓMEZ VIEITES, Álvaro. Seguridad en equipos informáticos. ProQuest Ebook Central. 2014. Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3229330

Y la segunda parte se encuentra apoyada por medio el anexo A o ISO 27002:2013[11] la cual es una guía de buenas prácticas basada en dominios, objetivos de control y controles, en la cual se encuentran parámetros establecidos de acuerdo al dominio que afecte el proceso en la empresa; una vez definido el mismo se tendrán las pautas requeridas para implementar los controles requeridos en los procesos y funcionalidades de los activos, por esa razón al tener una organización clara de acuerdo al activo y su rango o área de actuación; se pueden definir claramente el mejor control que mitigue el riesgo presente en el activo.

Dentro los 14 Dominios encontramos desde la gestión de activos, recursos humanos, cifrado de información, control de acceso, seguridad física y ambiental, entre otros; a su vez los controles correspondientes a cada uno de los dominios poseen una correlación entre ellos, ya que al hablar de ellos, encontramos el funcionamiento de una empresa en la cual los procesos referentes al manejo de información van relacionados entre sí por ejemplo al momento de organizar controles de criptografía, debemos tener en cuenta el control cese o cambio de puesto de trabajo en el dominio de seguridad de los recursos humanos donde se asigna las responsabilidades y roles, lo cual hace parte vital del conjunto de políticas para la seguridad en la información, que a su vez están contemplados dentro de los controles del dominio políticas de seguridad[12].

4.3.3 Análisis de Brecha (GAP). Método empleado para conocer el estado de "Madures" entre la actualidad de un sistema y el esperado del mismo, donde se evalúan las diferencias de rendimiento y si ella cumplen los requisitos del negocio, permitiendo conocer que hace falta y los recursos para alcanzarlo.

4.3.4 Seguridad de la Información. Basada en la estructura de las medidas preventivas para garantizar la disponibilidad, confidencialidad e integridad de la información. En la misma se podrán encontrar todas las buenas prácticas de los procesos tecnológicos gestionados en la empresa, enfocados en mitigar los riesgos y amenazas de la información en la empresa

4.3.5 Implementación SGSI. De acuerdo a lo planteado en la ISO 27001, la Seguridad de la información, reside en la preservación de la confidencialidad,

[11] ISOTOOLS EXCELLENCE. Norma-ISO-27002-control-de-accesos. Disponible en: https://www.pmg-ssi.com/2017/08/norma-iso-27002-control-de-accesos/.

[12] IBM. Utilización de listas de control de acceso de bases de datos para la identificación y autenticación. Disponible en: https://www.ibm.com/support/knowledgecenter/es/SSKTXQ_9.0.0/admin/config/st_adm_security_useridauth_c.html.

Integridad y disponibilidad de los datos, así como los sistemas comprometidos en su tratamiento.[13]

4.3.6 Paso para Implementar un SGSI. Como se mencionó anteriormente para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información basado en la ISO 27001, se utiliza el ciclo continuo PHVA[14].

Se contemplan las fases descritas a continuación:

4.3.6.1 La Fase "Plan" (Planificación). Establece los objetivos de la seguridad de la información y selección de los controles adecuados de seguridad.

4.3.6.2 La Fase "Hacer" (Implementación). La fase de la ejecución de todo lo estructurado en la fase anterior. Dando las indicaciones pertinentes de cómo se debe manejar el sistema en pro de las políticas, controles y procedimientos correspondientes.

4.3.6.3 La Fase "Verificar" (Revisión). En esta fase se realiza el seguimiento de la implementación del SGSI mediante diversos "conductos", siempre verificando que los resultados cumplen los objetivos establecidos.

4.3.6.4 La Fase "Actuar" Mantenimiento y Mejora. Es la realización de todas las acciones de prevención y corrección del SGSI, con el fin de garantizar la mejora continua del mismo.

4.4. FASES DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.4.1 Fase Diagnóstico. En la cual se busca conocer el estado de la empresa actual, identificando adecuadamente activos, procesos y sus riesgos asociados

4.4.1.1 Fase Planificación, para lo cual la Empresa Determina

- Grupos de trabajo (de acuerdo a cada uno de los procesos determinar el personal encargado del mismo de acuerdo a su cargo y área de trabajo)

- Plan de Trabajo (Metodología donde se identifique las actividades a realizar, plazos e interrelación entre las mismas, todo esto de acuerdo al grupo que lo vaya a realizar)

[13] INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá. El Instituto, 2013. 37 p.

[14] GONZALEZ, Frank. Diagnóstico y Actualización del Sistema de Gestión de Seguridad de la Información (SGSI) para Ventas y Servicios S.A. Trabajo de grado para Ingeniero de Sistemas. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p.

- Asignación de Responsabilidades (se especifica límites y compromisos de acuerdo al grupo de trabajo)

4.4.1.2 Fase Implementación. Cumplimiento de los objetivos establecidos, realizando una comparación entre lo obtenido y lo planificado)

4.4.1.3 Evaluación y Monitoreo. Se evalúan los resultados obtenidos una vez se haya culminado la fase de implementación del SGSI y en base de esta se diseña un programa o cronograma de seguimiento de las mejoras y resultados obtenidos.

4.4.2 Identificación de Vulnerabilidades. Es la fase donde se contempla el uso de herramientas y listas de verificación para determinar las amenazas que puedan convertirse en vulnerabilidades para el sistema, teniendo en cuenta vulnerabilidades en la seguridad física, seguridad de infraestructura, seguridad en conexiones, servicios y funciones.

4.4.3 Determinación de las Amenazas. Por medio de la metodología de análisis y gestión, se busca establecer cuáles son las probabilidades que suceda un evento que llegue a causar un daño sobre el funcionamiento del sistema, para lo cual existen 4 tipos de orígenes de las amenazas según la metodología de análisis y gestión de riesgos MAGERIT Vr 3.0[15], como lo son:

- Origen Natural: Desastres Naturales

- Origen Industrial: Corte en el suministro de energía, fallo en servicios de comunicaciones, emanaciones electromagnéticas, entre otros

- Errores y Fallos no intencionales: errores de configuración, errores del administrador o usuarios, deficiencias de la organización, destrucción de la información, errores de mantenimiento, perdida de equipo, entre otros.

- Ataques Intencionados: Manipulación de Registros de actividad, suplantación de la identidad del usuario, difusión de software dañino, acceso no autorizado, análisis de tráfico, robo, ataque destructivo, entre otros.

[15] GOBIERNO DE ESPAÑA. MAGERIT V3. 2012. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XW_f3ChKjIU.

4.5 MARCO HISTÓRICO

4.5.1 Sistemas Gestión de la Seguridad en la Información. El concepto SGSI surge desde hace 5000 años, donde se inician a tomar los primeros conceptos de seguridad; esto basado en los hallazgos arqueológicos, como las pirámides egipcias, pirámides mayas, palacios y templos, los cuales su fundamento era el de protección de una amenaza, lo cual ha tenido una constante evolución en el trascurso de la historia

Es así como el concepto de seguridad ha seguido un continuo proceso evolutivo entre las organizaciones sociales; y es ahí donde se evidencia que gracias a la historia el primer sistema de seguridad, apareció en la republica romana e iniciando la seguridad externa y seguridad interna de una sociedad.

Procediendo un poco más en la historia, en la revolución industrial se origina la seguridad moderna teniendo como fundamento combatir los delitos y movimientos laborales, la cual fue concebida por Henry Fayol en 1919, donde identifica a la seguridad como una de las funciones empresariales, teniendo en cuenta esto Fayol deriva sus medidas a la seguridad de los activos físicos de la instalación, el cual en su momento ponía al mismo por encima de los empleados[16].

Hacia principios de los años noventa en Inglaterra, se empieza a conocer y desarrollar un modelo el cual denominan "Sistema de Gestión de Seguridad de Información", en 1995 se lanza por primera vez como norma inglesa la BSI; para 1998 se lanzan los requisitos de su certificación y en el 2000 fue aprobada como la parte 1 de la ISO 17799, pero es hasta el 2005 donde su promotor el British Standars Institute logra oficializar una norma conocida como la ISO 27001:2005, la cual se reconocen las metodologías y buenas prácticas; para poder garantizar la confidencialidad, integridad y disponibilidad de la información, siendo exigida en los mercados internacionales para que las empresas respondan con un sistema de planificación en la continuidad del negocio.

En Colombia esta norma se suma a las certificaciones de los sistemas de gestión de calidad, tales como la norma ISO 9001:2008 y NTC GP 1000:2004, por lo cual establece un avance significativo a las compañías certificadas para una competitividad en el mercado global, permitiéndole hoy en día las empresas enfocar parte de su atención a los activos de la información y su protección.

4.5.2 La Joyería Orient en Colombia. La historia de Joyería Orient se empezó a escribir en 1945, con la apertura de la primera joyería en el centro de Ibagué, la cual contaba con un orfebre, un relojero y dos ayudantes más.

[16] DE LA CRUZ GARCÍA, Juan Manuel. Delitos informáticos. El Cid Editor. 2009.

A finales de los años 70 se da la apertura de la segunda joyería ubicada en el Centro Comercial Combeima. Años más tarde, en 1986, se constituyó la sociedad García Varela Ltda con el nombre comercial Joyería Orient.

Durante los 90, se vivió un periodo de crecimiento importante, se abrieron nuevos puntos de venta en la ciudad de Ibagué, se incorporaron cerca de 20 ayudantes más, se amplío el taller de manufactura con cuatro orfebres y se tercerizó el taller de relojería.

En agosto de 2012 se crea la joyería Time City, dedicada a un público más joven.
Durante los primeros años del presente siglo, Joyería Orient aumentó su alcance geográfico con la apertura de puntos de venta en la ciudad de Bogotá, Pereira, Medellín, Neiva y se abrieron nuevas joyerías Time City en las ciudades de Neiva, Medellín e Ibagué.
Actualmente, se adelantan los estudios pertinentes para entrar en la ciudad de Manizales.

“Joyas que dan valor a tu vida”

Es una empresa familiar del sector joyero, fundada en 1945, miembro del círculo colombiano de joyerías; la cual se dedica a la compra, importación, producción, venta y prestación de servicios técnicos de joyería, y relojería.

Brinda a sus clientes soluciones personalizadas a las necesidades de belleza, vanidad y medición del tiempo, están respaldados por un excelente servicio postventa, todo esto gracias al apoyo de personas capacitadas en el sector de joyería y relojería; quiénes están comprometidos a ofrecer un excelente servicio al cliente y al desarrollo de la empresa y el progreso de Colombia. (Joyeria Orient)

- Visión

Satisfacer las necesidades y expectativas de vanidad, belleza y medición del tiempo de los clientes, con productos de joyería de alta calidad, con precios justos y un excelente servicio.

- Misión

Siempre estará a la vanguardia para ofrecer sus productos y servicios haciendo presencia en los puntos estratégicos de desarrollo del comercio en la ciudad de Ibagué e incursionará en los mercados del centro del país.

4.6 MARCO CIENTÍFICO O TECNOLÓGICO

4.6.1 Línea y Tipo de Investigación. La metodología a usar en el desarrollo de este proceso será un enfoque mixto entre metodología cualitativa y cuantitativa,

siendo que se pretende realizar un estudio desde la parte cuantitativa, mediante la identificación de variables, instrumentación y medición para determinar la vulnerabilidad, fallas y demás. También se empleará desde la metodología cualitativa el análisis del funcionamiento de la empresa; complementando ambas metodologías, para crear un sistema de gestión confiable de acuerdo con la realidad de la empresa y su funcionamiento.

4.6.2 Tipo de Investigación

4.6.2.1 Investigación Descriptiva. Permite delimitar los hechos que conforman el problema de investigación, como lo son:

- Establecer la descripción propia como unidad de investigación (Cantidad de equipo, usuarios, procesos, etc.) en la joyería Orient.
- Encontrar y comprobar las posibles asociaciones relacionadas en los procesos o variables de investigación.

4.6.2.2 Investigación Exploratoria. Por medio de la observación y la entrevista se pretende levantar datos para el diagnóstico inicial sobre el tratamiento de la información en la Joyería Orient.

4.6.3 Área de Investigación. La propuesta se enmarca dentro del área de conocimiento: Gestión de la Seguridad Informática, específicamente en el diseño del sistema de gestión de seguridad de la información y gestión del riesgo informático.

4.6.3.1 La Gestión del Riesgo. Contempla el análisis, valoración y clasificación del riesgo con el fin de hallar los controles apropiados para contrarrestarlos[17]

Este método sigue cuatro pasos, como lo son:

- Análisis: Mediante esta acción es posible establecer que partes del sistema necesitan protección, además, identificar cuáles son las vulnerabilidades y amenazas y reconocer el grado de riesgo al que se enfrentan.

- Clasificación: Se categoriza el riesgo y el nivel de aceptación.

- Reducción y control: corresponde a labores de sensibilización del usuario y al análisis de la efectividad de las medidas seleccionadas[18]

[17] AGUILERA, Purificación. Seguridad Informática: Ciclos Formativos. México: Editex, 2010, p.9.

[18] SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA. Seguridad de la Información. En: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, 2014, No. 1, p 15-16

4.6.4 Técnicas e Instrumentos de Recolección de Información. Para el presente proyecto, se hará uso de las fuentes bibliográficas requeridas para el diseño del sistema de gestión de seguridad de la información, con el fin de establecer antecedentes necesarios que soporten y sustenten la investigación.

Las técnicas de recolección de datos para el desarrollo de la investigación son: La Entrevista y la Observación.

- Observación: por medio de esta técnica podemos deducir y conocer los procedimientos reales dentro de la empresa.

- Entrevista: Mediante esta técnica podemos conocer y socializar el punto de vista de las diferentes partes involucradas en el desarrollo de los procesos de la empresa.

4.6.5 Población y Muestra

4.6.5.1 Población. El proyecto involucra la oficina administrativa de la joyería ubicada en la sede de Ibagué, teniendo en cuenta que es allí donde se centraliza la mayoría de los procesos de la misma; respecto a las sedes en las demás ciudades, se contempla mediante un manejo administrativo.

4.6.5.2 Muestra. Para el estudio en referencia se incluirán 14 funcionarios o usuarios de los sistemas informáticos de la empresa (Base de datos, equipo de cómputo), teniendo en cuenta procedimientos y procesos operativos como administrativos de la compañía.

4.7 MARCO LEGAL

Al momento que una organización toma la decisión de realizar la implementación de un SGSI, se deben tomar en cuenta las implicaciones que con lleva este y entre ellas esta las implicaciones legales, en el caso del SGSI de la Joyeria Orient, este marco legal permitirá conocer que leyes pueden soportar y aportar a las diferentes políticas o controles del sistema, ya que al momento de incumplimiento de un control o política puede estar cometiendo un delito regido en las regulaciones legales colombianas.

- Decreto 1747 de 2000, que reglamenta parcialmente la ley 527 de 1999, con lo relacionado a las entidades de certificación, los certificados y las firmas digitales[19], en la estructura de las políticas de la empresa se regula el control de

[19] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Decreto ley 19 de 2012. Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. 2012. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/decreto_0019_2012.html

acceso de manera individual, por lo cual, cualquier tipo de suplantación o derivados se vería acogido bajo este decreto para la debida sanción.

- Ley Estatutaria 1266 de 2008, que establece las disposiciones generales del habeas data y regula el manejo de la información que se contiene en las bases de datos personales, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países[20], esta regulación permitirá dar soporte a las diferentes políticas de manejo de la información contempladas en la 6.4.3

- Ley 1273 de 2009, con la que se modifica el código penal, se crea un nuevo bien jurídico denominado "de la protección de la información y los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de información y de comunicación[21], esta ley establece las regulaciones legales en el marco colombiano que contempla la seguridad e integridad de la información, lo cual nos permite soportar el incumplimiento de las políticas y controles estipulados en la 6.3 y las debidas consecuencias del incumplimiento del mismo[22].

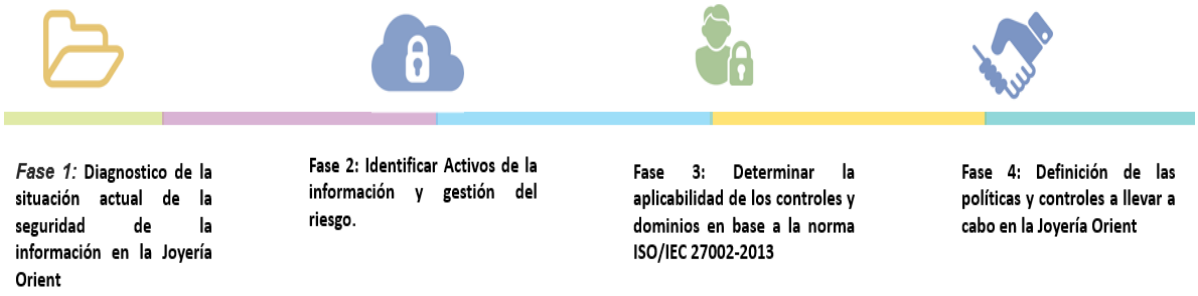
[20] UNIVERSIDAD NACIONAL DE COLOMBIA. Oficina Jurídica Nacional. Disponible en:http://www.legal.unal.edu.co/sisjurun/normas/Norma1.jsp?i=42011

[21] DELTA ASESORES. Ley de delitos informáticos en Colombia. 2014. Disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

[22] CONGRESO DE LA REPÚBLICA. 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. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

5. DISEÑO METODOLÓGICO

Figura 1. Diseño metodológico (ampliar información)



Fuente: Elaboración propia

En la figura anterior, podemos ver la línea de continuidad de las 4 fases a desarrollar en el diseño metodológico del proyecto

5.1 DIAGNOSTICO DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA JOYERÍA ORIENT

Es necesario Identificar y reconocer las disposiciones establecidas al interior de la empresa en materia de seguridad de la información, para lo cual se propone:

- Realizar una consulta a la documentación existente relacionada a la estructura procedimental de la empresa
- Entrevistar a los administradores de punto, y líderes de área para establecer y conocer los procesos actuales.
- Observación de la forma de manejo de la información sensible
- Realizar un Modelo de madurez para conocer el estado actual en relación a dónde estamos y adonde se quiere llegar.

5.2 IDENTIFICAR ACTIVOS DE INFORMACIÓN Y GESTIÓN DEL RIESGO

De acuerdo a lo antes descrito, se debe realizar el inventario de activos de la información para la empresa, lo cual permitirá que dominios descritos en el anexo A de la norma ISO/IEC 27001-2013, se aplicaran en la evaluación de riesgos, con el fin de minimizarlos, para lo cual se realiza:

Visita de reconocimiento a la oficina administrativa y entrevista con el depto. De informática con el fin de identificar y relacionar el tipo de activos informáticos.

5.3 DETERMINAR LA APLICABILIDAD DE LOS CONTROLES Y DOMINIOS EN BASE A LA NORMA ISO/IEC 27002-2013

Una vez realizado el análisis de riesgo, vulnerabilidades y amenazas se pretende realizar un comparativo el nivel de cumplimiento de los requerimientos establecidos en los dominios de la ISO/IEC 27002-2013, con el objetivo de identificar las deficiencias presentadas por la Joyería Orient.

5.4 DEFINICIÓN DE LAS POLÍTICAS Y CONTROLES A LLEVAR A CABO EN LA JOYERÍA ORIENT

Socializar con el equipo administrativo lo encontrado ante las deficiencias de la empresa, los escenarios de riesgo y los controles a llevar a cabo junto con las políticas para mitigar los riesgos en el manejo de la información.

6. DESARROLLO DE LOS OBJETIVOS

6.1 CONOCER EL ESTADO ACTUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN BASE AL ANEXO A ISO 27001-2013

Teniendo en cuenta el cumplimiento o diagnostico actual de acuerdo con los controles del Anexo A, se determina que la madurez de la protección o seguridad de la información está en un 35% de estado inicial, por lo que refiere que existen algunos controles o salvaguardas, mas no ejecución por parte del personal de la empresa. De igual forma hay un 32% de inexistentes, los cuales la empresa no tiene ningún tipo de control en el proceso; el 12% del estado administrado refiere a los procesos que actualmente se encuentran documentados y formalizados.

Actualmente solo se tiene un 10% del estado definido, acorde a los procesos documentados, pero que están pendiente de aprobación por parte de las directivas de la empresa; tan solo, un 2% de los procesos evaluados tiene un control o salvaguarda que está siendo utilizado por parte de los funcionarios de la empresa.

Este diagnóstico inicial, nos deja evidenciar que actualmente la empresa se encuentra en un estado crítico de seguridad de la información, con un 67% en controles inexistentes o no empleados por parte del personal de la empresa y proveedores.

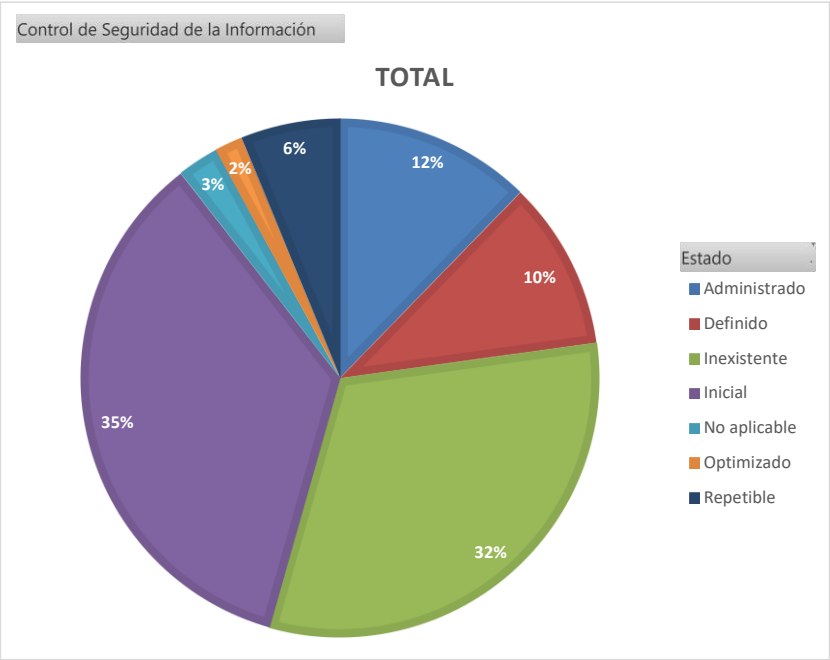
La información del diagnóstico resumida se evidencia en la Tabla 2 y figura 2.

Tabla 1. Estado actual del estado de la seguridad

Estado	Control de Seguridad de la Información
Administrado	12%
Definido	10%
Inexistente	32%
Inicial	35%
No aplicable	3%
Optimizado	2%
Repetible	6%
Total general	100%

Fuente: Elaboración propia

Figura 2. Estado actual de la seguridad de la información



Fuente: Elaboración propia

6.2 IDENTIFICAR LOS POSIBLES ACTIVOS DE LA INFORMACION Y GESTION DEL RIESGOS DE LA JOYERIA ORIENT, TENIENDO EN CUENTA LA METODOLOGIA MAGERIT

Acorde a los lineamientos establecidos, se clasificaron los activos de TI, al igual que los recursos de o activos de la información de la empresa, permitiendo el análisis de gestión del riesgo MAGERIT, en la cual desarrollaremos los siguientes pasos

- Establecer un inventario de activos
- Agrupar activos acordes a su área de funcionalidad en el sistema de información
- Establecer la medición de riesgo
- Identificar los riesgos
- Identificar los posibles escenarios de amenaza
- Realizar el debido análisis del riesgo

6.2.1 Activos de Joyería Orient. Los activos son los componentes o funcionalidades de un sistema de información: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humano.

Software

- Base de datos clientes
- Aplicaciones comerciales
- Sistema operativo
- Correo Corporativo
- Navegador web
- Red telefónica

Hardware

- Servidores
- Planillas de pagos
- Equipos (Computadores de oficina, impresoras, Monitores, teclados).
- Manuales
- Firewall Fortinet

6.2.2 Inventario de Activos. En la tabla 2, se relacionan los activos de la joyería Orient en Colombia clasificado bajo la nomenclatura de la metodología magerit para el posterior análisis de riesgos.

Tabla 2. Inventario de activos

Código	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
D1	Archivo Contabilidad_D	Archivo digital con información contable de la empresa.	Dpto. Contable	Datos(Digital)	Servidor Local BD	SI

Código	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
D2	Archivo Usuarios_D	Archivos digitales con información de clientes de la empresa.	Dpto. Contable	Datos(Digital)	Servidor Local BD	SI
D3	Archivos Proveedores_D	Archivos digitales con información de Proveedores de la empresa.	Dpto. Contable	Datos(Digital)	Servidor Local BD	SI
D4	Archivos Corporativos_D	Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de Administración)	Dpto. Administrativo Legal	Datos(Digital)	Servidor Local BD	SI
D5	Archivo Corportaivo_F	Archivos físicos con información corporativa.	Dpto. Administrativo Legal	Datos(Físico)	Oficina Administrativa	SI
D6	Archivo Usuarios_F	Archivos físicos de clientes de la empresa.	Dpto. Contable	Datos(Físico)	Oficina Administrativa	SI
D7	Archivos Proveedores_F	Archivos físicos de Proveedores de la empresa.	Dpto. Contable	Datos(Físico)	Oficina Administrativa	SI
D8	Archivo Contabilidad_F	Archivos físicos de respaldo de la contabilidad. (Libros contables)	Dpto. Contable	Datos(Físico)	Oficina Administrativa	SI
K1	Claves Criptograficas	Login y contraseñas de usuarios	Dpto. Informática.	Claves(Digital)	Oficina Administrativa	SI
S1	Página web	Página web	Dpto. Informática.	Servicios(Digital)	Oficina Administrativa	SI
S2	Correo corporativo.	Correo corporativo.	Dpto. Informática.	Servicios(Digital)	CPD Externo	NO
S3	Compras de Joyas	Compras de Joyas	Dpto. Comercial	Servicios(Físicos)	Puntos de Venta	NO
S4	Compra de Relojes	Compra de Relojes	Dpto. Comercial	Servicios(Físicos)	Puntos de Venta	SI
S5	Compra de Accesorios	Compra de Accesorios	Dpto. Comercial	Servicios(Físicos)	Puntos de Venta	SI
S6	Venta de Joyas	Venta de Joyas	Dpto. Comercial	Servicios(Físicos)	Puntos de Venta	SI
S7	Venta de Relojes	Venta de Relojes	Dpto. Comercial	Servicios(Físicos)	Puntos de Venta	SI
S8	Venta de Accesorios	Venta de Accesorios	Dpto. Comercial	Servicios(Físicos)	Puntos de Venta	SI
S9	Seguridad en el trabajo	Auditoria y seguimiento a políticas internas	Dpto. SG-SST	Servicio(Físicos)	Oficina Administrativa	SI
SW1	Software Correo corporativo.	Software de correo corporativo. Gmail	Dpto. Informática.	Software(Digital)	CPD Externo	NO
SW1	Sistema Operativo	Sistema operativo de los equipos de cómputo - Windows 10	Dpto. Informática.	Software(Digital)	CPD Externo	NO

Código	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
SW3	Herramienta Ofimática	Suite Office 365	Dpto. Informática.	Software(Digital)	CPD Externo	NO
SW4	Software Cámaras de Seguridad	Software de Seguridad - HIKVISION	Dpto. Informática.	Software(Digital)	Oficina Administrativa	NO
SW5	Antivirus	Software antivirus - Karpesky	Dpto. Informática.	Software(Digital)	CPD Externo	SI
SW6	Software Financiero y Contable	Software financiero y Contable - ISIIGO	Dpto. Informática.	Software(Digital)	Servidor Local BD	SI
SW7	Software Logístico	Software Logístico - ICG	Dpto. Informática.	Software(Digital)	Servidor Local BD	SI
SW8	Software Crediticio	Software Crediticio - KAIOWA	Dpto. Informática.	Software(Digital)	CPD Externo	SI
SW9	Navegador Web	Navegador Chrome - Mozilla	Dpto. Informática.	Software(Digital)	CPD Externo	NO
SW10	Licenciamiento ISIIGO	Licenciamiento ISIIGO	Dpto. Informática.	Software(Digital)	CPD Externo	SI
SW11	Gestor Base de datos	MySQL	Dpto. Informática.	Software(Digital)	Servidor Local BD	NO
SW12	Gestor Web	PHP 5.6.30	Dpto. Informática.	Software(Digital)	Servidor Local BD	NO
SW13	Servidor Web	Apache 2.4.25	Dpto. Informática.	Software(Digital)	Servidor Local BD	NO
HW1	Switch 01 (Contable)	Switch Contable	Director Administrativo	Hardware(Físico)	Ofi. Administrativa_Salon01	SI
HW2	Switch 02 (Administrativo)	Switch Administrativo	Director Administrativo	Hardware(Físico)	Ofi. Administrativa_Salon01	SI
HW3	Switch 03 (Informático)	Switch Informático	Dpto. Informática.	Hardware(Físico)	Ofi. Administrativa_Salon02	SI
HW4	Computador 01 (Contable)	Computador Contador	Director Administrativo	Hardware(Físico)	Ofi. Administrativa_Salon01	SI
HW5	Computador 02 (Contable)	Computador Aux Contable	Director Administrativo	Hardware(Físico)	Ofi. Administrativa_Salon01	SI
HW6	Computador 03 (Cartera)	Computador Cartera	Director Administrativo	Hardware(Físico)	Ofi. Administrativa_Salon01	NO
HW7	Computador 04 (Legal)	Computador Área Legal	Dpto. Administrativo Legal	Hardware(Físico)	Ofi. Administrativa_Salon02	NO
HW8	Computador 05 (SG-SST)	Computador SG-SST	Dpto. SG-SST	Hardware(Físico)	Ofi. Administrativa_Salon02	NO
HW9	Computador 06 (Informática)	Computador Área Informática	Dpto. Informática.	Hardware(Físico)	Oficina Administrativa	SI
HW10	Impresora 01	Impresora/Scanner Oficina Administrativa	Director Administrativo	Hardware(Físico)	Oficina Administrativa	SI
HW11	Cámaras de Seguridad	Cámaras de Seguridad	Administrador Punto de Venta	Hardware(Físico)	Puntos de Venta	NO
HW12	Servidor 01 BackUp	Servidor Local BackUp	Dpto. Informática.	Hardware(Físico)	Oficina Administrativa	SI

Código	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
HW13	Servidor 02 Seguridad, Aplicaciones	Servidor de Seguridad, Aplicaciones - Dell T440	Dpto. Informática.	Hardware(Físico)	Oficina Administrativa	SI
HW14	Firewall	FireWall - Cisco ASA	Dpto. Informática.	Hardware(Físico)	Oficina Administrativa	SI
HW15	Computador 07 (Combeima)	Equipo de cómputo CC COMBEIMA	Administrador Punto de Venta	Hardware(Físico)	CC. Combeima - Ibagué	SI
HW16	Computador 08 (Estación)	Equipo de cómputo CC LA ESTACION	Administrador Punto de Venta	Hardware(Físico)	CC La Estación - Ibagué	SI
HW17	Computador 09 (Multicentro)	Equipo de cómputo CC MULTICENTRO	Administrador Punto de Venta	Hardware(Físico)	CC Multicentro - Ibagué	SI
HW18	Computador 10 (Aqua)	Equipo de cómputo CC AQCUA	Administrador Punto de Venta	Hardware(Físico)	CC Acqua -Ibagué	SI
HW19	Computador 11 (San Pedro01)	Equipo de cómputo CC SAN PEDRO PISO1	Administrador Punto de Venta	Hardware(Físico)	CC. San Pedro - Neiva	SI
HW20	Computador 12 (San Pedro02)	Equipo de cómputo CC SAN PEDRO PISO2	Administrador Punto de Venta	Hardware(Físico)	CC. San Pedro - Neiva	SI
HW21	Computador 13 (Stn Lucia)	Equipo de cómputo CC SANTA LUCIA	Administrador Punto de Venta	Hardware(Físico)	C.C. Santa Lucia - Neiva	SI
HW22	Computador 14 (Arboleda)	Equipo de cómputo CC ARBOLEDA	Administrador Punto de Venta	Hardware(Físico)	C.C. Arboleda - Pereira	SI
HW23	Computador 15 (Unicentro)	Equipo de cómputo CC UNICENTRO	Administrador Punto de Venta	Hardware(Físico)	C.C. Unicentro - Pereira	SI
HW24	Computador 16 (Andino)	Equipo de cómputo CC ANDINO	Administrador Punto de Venta	Hardware(Físico)	C.C. Andino - Bogotá	SI
HW25	Computador 17 (Medellin)	Equipo de cómputo CC Santa Fe	Administrador Punto de Venta	Hardware(Físico)	C.C. Santa Fe - Medellín	SI
HW26	Servidor 03 BD	Servidor Local Base de datos	Dpto. Informática.	Hardware(Físico)	Oficina Administrativa	SI
HW27	UPS	UPS	Dpto. Informática.	Hardware(Físico)	Oficina Administrativa	NO
COM1	Celular Corporativo 01	Celulares Corp. Contabilidad	Dpto. Contable	Disp. Comunicación (Físico)	Oficina Administrativa	SI
COM2	Celular Corporativo 02	Celulares Corp. Cartera	Dpto. Cartera	Disp. Comunicación (Físico)	Oficina Administrativa	NO
COM3	Celular Corporativo 03	Celulares Corp. Dpto. Legal	Dpto. Administrativo Legal	Disp. Comunicación (Físico)	Oficina Administrativa	SI
COM4	Celular Corporativo 04	Celulares Corp. SG-SST	Dpto. SG-SST	Disp. Comunicación (Físico)	Oficina Administrativa	NO
COM5	Celular Corporativo 05	Celulares Corp. C.C. Combeima	Administrador Punto de Venta	Disp. Comunicación (Físico)	CC. Combeima - Ibagué	NO

Código	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
COM6	Celular Corporativo 06	Celulares Corp. C.C. Estación	Administrador Punto de Venta	Disp. Comunicación (Físico)	CC La Estación - Ibagué	NO
COM7	Celular Corporativo 07	Celulares Corp. C.C. Acqua	Administrador Punto de Venta	Disp. Comunicación (Físico)	CC Acqua -Ibagué	NO
COM8	Celular Corporativo 08	Celulares Corp. C.C. Multicentro	Administrador Punto de Venta	Disp. Comunicación (Físico)	CC Multicentro - Ibagué	NO
COM9	Celular Corporativo 09	Celulares Corp. C.C. San Pedro 1	Administrador Punto de Venta	Disp. Comunicación (Físico)	CC. San Pedro - Neiva	NO
COM10	Celular Corporativo 10	Celulares Corp. C.C. San Pedro 2	Administrador Punto de Venta	Disp. Comunicación (Físico)	CC. San Pedro - Neiva	NO
COM11	Celular Corporativo 11	Celulares Corp. C.C. Santa Lucia	Administrador Punto de Venta	Disp. Comunicación (Físico)	C.C. Santa Lucia - Neiva	NO
COM12	Celular Corporativo 12	Celulares Corp. C.C. Arboleda	Administrador Punto de Venta	Disp. Comunicación (Físico)	C.C. Arboleda - Pereira	NO
COM13	Celular Corporativo 13	Celulares Corp. C.C. Unicentro	Administrador Punto de Venta	Disp. Comunicación (Físico)	C.C. Unicentro - Pereira	NO
COM14	Celular Corporativo 14	Celulares Corp. C.C. Andino	Administrador Punto de Venta	Disp. Comunicación (Físico)	C.C. Andino - Bogotá	NO
COM15	Celular Corporativo 15	Celulares Corp. C.C. Santa Fe	Administrador Punto de Venta	Disp. Comunicación (Físico)	C.C. Santa Fe - Medellín	NO
COM16	Celular Corporativo 16	Celulares Corp. Directora Administrativa	Director Administrativo	Disp. Comunicación (Físico)	Oficina Administrativa	SI
COM17	Punto HUB	Puntos de acceso HUB)	Dpto. Informática.	Disp. Comunicación (Físico)	Oficina Administrativa	SI
COM18	Teléfono IP	Teléfonos IP	Dpto. Contable	Disp. Comunicación (Físico)	Oficina Administrativa	SI
COM19	VPN Administrativo	VPN.	Dpto. Informática.	Disp. Comunicación (Físico)	Oficina Administrativa	SI
P1	Gerente General	Gerente General	Gerente General	Persona (Físico)	Oficina Administrativa	SI
P2	Director Administrativo	Director Administrativo	Director Administrativo	Persona (Físico)	Oficina Administrativa	SI
P3	Administrador de Punto 01	Administrador de Punto C.C. Combeima	Administrador Punto de Venta	Persona (Físico)	CC. Combeima - Ibagué	NO
P4	Administrador de Punto 02	Administrador de Punto C.C. Estación	Administrador Punto de Venta	Persona (Físico)	CC La Estación - Ibagué	SI
P5	Administrador de Punto 03	Administrador de Punto C.C. Acqua	Administrador Punto de Venta	Persona (Físico)	CC Acqua -Ibagué	SI
P6	Administrador de Punto 04	Administrador de Punto C.C. Multicentro	Administrador Punto de Venta	Persona (Físico)	CC Multicentro - Ibagué	SI

Código	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
P7	Administrador de Punto 05	Administrador de Punto C.C. San Pedro 01	Administrador Punto de Venta	Persona (Físico)	CC. San Pedro - Neiva	SI
P8	Administrador de Punto 06	Administrador de Punto C.C. San Pedro 02	Administrador Punto de Venta	Persona (Físico)	CC. San Pedro - Neiva	SI
P9	Administrador de Punto 07	Administrador de Punto C.C. Santa Lucia	Administrador Punto de Venta	Persona (Físico)	C.C. Santa Lucia - Neiva	SI
P10	Administrador de Punto 08	Administrador de Punto C.C. Arboleda	Administrador Punto de Venta	Persona (Físico)	C.C. Arboleda - Pereira	SI
P11	Administrador de Punto 09	Administrador de Punto C.C. Unicentro	Administrador Punto de Venta	Persona (Físico)	C.C. Unicentro - Pereira	SI
P12	Administrador de Punto 10	Administrador de Punto C.C. Andino	Administrador Punto de Venta	Persona (Físico)	C.C. Andino - Bogotá	SI
	Administrador de Punto 11	Administrador de Punto C.C. Santa Fe	Administrador Punto de Venta	Persona (Físico)	C.C. Santa Fe - Medellín	SI
P13	Contador	Contador	Dept. Contable	Persona (Físico)	Oficina Administrativa	SI
P14	Auxiliar Contable	Auxiliar Contable	Dept Contable	Persona (Físico)	Oficina Administrativa	NO
P15	Funcionario Cartera	Funcionario Cartera	Dept. Cartera	Persona (Físico)	Oficina Administrativa	NO
P16	Ingeniero de Sistemas	Ingeniero de Sistemas	Dpto. Informática.	Persona (Físico)	Oficina Administrativa	SI
P17	Auxiliar de SG-ST	Auxiliar de SG-ST	Dpto. SG-SST	Persona (Físico)	Oficina Administrativa	NO
P18	Vendedores	Vendedores	Dept. Comercial	Persona (Físico)	Puntos de Venta	SI
P19	Contratistas externos	Contratistas externos	Director Administrativo	Persona (Físico)	Equipo Externo	NO
AUX1	Cajas de seguridad.	Cajas de seguridad.	Administrador Punto de Venta	Equipo Auxiliar (Físico)	Puntos de Venta	SI
AUX2	Bóvedas de Seguridad	Bóvedas de Seguridad	Administrador Punto de Venta	Equipo Auxiliar (Físico)	Puntos de Venta	SI
AUX3	Acetas.	Acetas.	Dept Contable	Equipo Auxiliar (Físico)	Oficina Administrativa	NO
Media1	USB.	USB.	Dept. Informático	Sop. de Información(Físico)	Oficina Administrativa	NO
Media2	CD.	CD.	Dept. Informático	Sop. de Información(Físico)	Oficina Administrativa	NO
Media3	Acetas para información contable.	Acetas para información contable.	Dept Contable	Sop. de Información(Físico)	Oficina Administrativa	NO
Media4	Acetas para Registro y Control de inventarios	Acetas para Registro y Control de inventarios	Dept Contable	Sop. de Información(Físico)	Oficina Administrativa	NO
Media5	Acetas con información de proveedores	Acetas con información de proveedores	Dept Contable, Cartera	Sop. de Información(Físico)	Oficina Administrativa	NO
Media7	Servidor Local BackUp	Servidor Local BackUp	Dpto. Informática.	Locación (Físico)	Oficina Administrativa	NO

Código	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
L1	Instalación 01	Joyería CC Combeima	Administrador Punto de Venta	Locación (Físico)	CC. Combeima - Ibagué	SI
L2	Instalación 02	Joyería CC Multicentro	Administrador Punto de Venta	Locación (Físico)	CC Multicentro - Ibagué	SI
L3	Instalación 03	Joyería CC Estación	Administrador Punto de Venta	Locación (Físico)	CC La Estación - Ibagué	SI
L4	Instalación 04	Joyería CC Acqua	Administrador Punto de Venta	Locación (Físico)	CC Acqua -Ibagué	SI
L5	Instalación 05	Joyería C.C San Pedro Piso 1 - Neiva	Administrador Punto de Venta	Locación (Físico)	CC. San Pedro - Neiva	SI
L6	Instalación 06	Joyería C.C. San Pedro Piso 2 Neiva	Administrador Punto de Venta	Locación (Físico)	CC. San Pedro - Neiva	SI
L7	Instalación 07	Joyería C.C. Santa Lucia Neiva	Administrador Punto de Venta	Locación (Físico)	C.C. Santa Lucia - Neiva	SI
L8	Instalación 08	Joyería C.C. Arboleda Pereira	Administrador Punto de Venta	Locación (Físico)	C.C. Arboleda - Pereira	SI
L9	Instalación 09	Joyería C.C. Unicentro Pereira	Administrador Punto de Venta	Locación (Físico)	C.C. Unicentro - Pereira	SI
L10	Instalación 10	Joyería C.C Andino Bogota	Administrador Punto de Venta	Locación (Físico)	C.C. Andino - Bogotá	SI
L11	Instalación 11	Joyería C.C. Santa Fe	Administrador Punto de Venta	Locación (Físico)	CC. Santa Fe- Medellín	SI
L12	Instalación 12	Oficina Administrativa Cr 3 # 13-01 piso 3 y 4	Director Administrativo	Locación (Físico)	Oficina Administrativa Ibagué	SI

Fuente: Elaboración propia”

En el anexo B. Especificaciones técnicas de activos (hardware) encontraran las especificaciones de los activos anteriores.

6.2.3 Análisis de Riesgos. El análisis de riesgo tiene la función de exponer los riesgos que enfrenta una organización. La metodología Magerit propone las siguientes pautas[23]:

- Determinación de los activos importantes de la organización, su interrelación y su valor.
- Determinación de la amenaza a la que están expuesta dichos activos.
- Determinación de salvaguardas hay disponible y evaluación de su eficiencia.
- Estimación del impacto del daño.

[23] DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA. Método de analisis de riesgos. MAGERIT - Version 3.0 Metodología de Análisis y Gestión Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012, pág. 22.

- Estimaciones de riesgo,

Para empezar con el debido análisis, debemos tener en cuenta algunos aspectos como lo son, la determinación de los diferentes tipos de amenaza a los que se puede enfrentar un activo, los cuales están representados en la TABLA 5 MATRIZ DE AMENAZAS POR TIPOS

Tabla 3. Matriz de Amenazas por tipos

Origen	Amenazas	Tipos de activos
Desastres naturales	Fuego	Equipos de computo
		Red de comunicación
		Documentación
	Daños por agua	Equipos de computo
		Red de comunicación
		Documentación
	Desastres naturales	Equipos de computo
		Red de comunicación
		Documentación
Industrial	Fuego	Equipos informáticos
		Red de comunicación
		Documentación
	Daños por agua	Equipos informáticos
		Red de comunicación
		Documentación
Errores y fallos no intencionados	Errores de los usuarios	Base de datos
		Información Financiera
	Escape de información	Base de datos
		Información Financiera
Ataques intencionados	Manipulación de los registros de activad (log)	Bases de datos
		Recursos Humano
		Información financiera
	Difusión de software dañino	Red de comunicación
		Equipos de computo
		Base de datos
		Red de comunicación
		Sistema Operativos
	Acceso no autorizado	Bases de datos
		Información Financiera
		Sistemas operativos
		Recursos Humano

Fuente:[24]

El impacto que con lleva el activo dentro de la organización, hace referencia a la afectación de la continuidad del negocio lo cual está representado en la TABLA 6 VALORACION DEL IMPACTO

Tabla 4. Valoración de Impacto

Impacto		
Valor	**Nivel**	**Descripción**
5	**Critico**	El impacto representa pérdidas importantes que detengan en su totalidad procesos relevantes
4	**Grave**	El impacto puede representar perdidas mayores que aborten procesos importantes
3	**Considerable**	El impacto puede representar perdidas que generen daños en procesos importantes
2	**Leve**	El Impacto no representa pérdidas significativas
1	**Despreciable**	El Impacto no representa perjuicios para la empresa

Fuente: Elaboración propia

En esta misma relación la probabilidad de que se materialice dicha amenaza está representado en la TABLA 7 VALORACIÓN DE LA PROBABILIDAD

Tabla 5. Valoración de la probabilidad

Probabilidad		
Valor	**Nivel**	**Descripción**
5	**Regular**	Evento que ocurre con mucha frecuencia
4	**Probable**	Evento que puede ocurrir, pero no con frecuencia.
3	**Ocasional**	Eventos que han presentado antecedentes, pero no en el corto plazo
2	**Poco frecuente**	Evento que ocurre con una periodicidad baja
1	**Improbable**	Eventos que suceden de forma esporádica

Fuente: Elaboración propia

Una vez descrita la importancia de un activo en la compañía, es medido por el nivel de confidencialidad que contenga, el cual está representado en la TABLA 8 VALORACION DE LA CONFIDENCIALIDAD

[24] CEDEÑO VALAREZO, Luis Cristóbal., MORALES CARRILLO, Jessica Johanna., DÁVILA MUÑOZ, Mayra Alejandra y PÁRRAGA ANDRADE, Gema Vanessa. Análisis de Riesgos tecnológicos en la cooperativa de ahorro y crédito Calceta Limitada. Revista Tecnológica-ESPOL, 2016, 29(1). Disponible en: http://rte.espol.edu.ec/index.php/tecnologica/article/view/492/329

Tabla 6. Valoración de la confidencialidad

Confidencialidad		
Valor	**Nivel**	**Descripción**
5	**Confidencial**	Información clasificada solo accesible por un grupo selecto de empleados.
4	**Acceso autorizado**	Información que es accesible por trabajadores que se les permite acceder por la alta gerencia
3	**Restringida**	Información dispuesta solo para personal de la empresa
2	**Privada**	Información que es accesible por todo el personal de la empresa, pero nadie externo a ella
1	**Publico**	Información mostrada al público que no representa mayor impacto para la organización

Fuente: Elaboración propia

En el proceso de realizar un detallado análisis del activo debemos tener claro en qué porcentaje de disponibilidad podemos tener un equipo, esto en base de cuánto tiempo puede dejar de estar disponible, este activo en relación a la continuidad laboral.

Tabla 7. Valoración de la Disponibilidad

Valor	Disponibilidad	Descripción
5	100 %	0.088 horas Down time al año
4	99.900 %	8.8 horas Down time al año
3	99.000 %	88 horas Down time al año
2	98.000 %	175 horas Down time al año
1	95.000 %	438 horas Down time al año

Fuente:[25]

La integridad de la información es uno de los tres aspectos fundamentales, por lo cual es determinante para determinar el valor de un activo en una organización, lo cual se ha determinado en la TABLA 10 VALORACIÓN DE LA INTEGRIDAD

[25] GARCIA, Miguel Angel. Calculando la disponibilidad de sistemas complejos. 2015. Disponible en: https://magmax.org/blog/en-busca-de-los-cinco-9s/.

Tabla 8. Valoración de la Integridad (Perdida en Complejidad y Exactitud)

Valor	Nivel	Descripción
5	**Alta**	**Perdidas Severas**
3	**Media**	**Perdidas moderadas**
2	**Baja**	**Impacto no significativo**

Fuente: Elaboración propia

6.2.4 Valoración del Impacto en el Activo. Para determinar la importancia de un activo con relación a la continuidad del negocio debemos poder valorar a un activo bajo los tres aspectos fundamentales, como lo son la confidencialidad, integridad y disponibilidad, teniendo en cuenta el impacto que puede causar el mismo en el funcionamiento de la empresa, esto se ve referenciado en la tabla 11 valoración del activo.

Esta Valoración del activo permitirá a la empresa realizar un análisis del nivel de riesgo en base de los escenarios que se puedan presentar, algunos de ellos en base al funcionamiento actual de la empresa están evidenciados en el 6.2.5 ESCENARIOS

Nivel Riesgo: Impacto X Probabilidad

Tabla 9. Valoración del activo

Código	Confidencialidad	Integridad	Disponibilidad	Impacto
D1	5	5	5	5
D2	5	5	4	5
D3	5	5	4	5
D4	5	5	3	4
D5	5	5	4	4
D6	5	5	4	4
D7	5	5	4	4
D8	5	5	4	4
K1	5	5	5	5
S1	1	5	3	3
S2	4	5	4	3

Código	Confidencialidad	Integridad	Disponibilidad	Impacto
S3	5	5	4	5
S4	5	5	4	5
S5	5	5	4	5
S6	5	5	3	5
S7	5	5	3	5
S8	5	5	3	5
S9	3	5	4	3
SW1	4	5	3	3
SW1	4	5	4	3
SW3	3	3	3	3
SW4	5	5	5	5
SW5	4	3	4	5
SW6	5	5	5	5
SW7	5	5	5	5
SW8	5	5	5	5
SW9	3	3	5	4
SW10	4	5	5	5
SW11	4	5	4	3
SW12	4	5	4	3
SW13	4	5	4	3
HW1	5	5	5	5
HW2	5	5	5	5
HW3	5	5	5	5
HW4	5	5	5	5
HW5	5	5	5	5
HW6	5	5	5	5
HW7	5	5	5	3
HW8	5	5	5	3
HW9	5	5	5	5
HW10	4	3	3	3
HW11	4	3	3	2
HW12	5	5	5	5
HW13	5	5	5	5
HW14	5	5	5	5

Código	Confidencialidad	Integridad	Disponibilidad	Impacto
HW15	5	5	5	5
HW16	4	5	4	4
HW17	4	5	4	4
HW18	4	5	4	4
HW19	4	5	4	4
HW20	4	5	4	4
HW21	4	5	4	4
HW22	4	5	4	4
HW23	4	5	4	4
HW24	4	5	4	4
HW25	4	5	4	4
HW26	4	5	4	4
HW27	5	5	4	5
COM1	5	5	3	3
COM2	5	5	3	3
COM3	5	5	3	3
COM4	5	5	3	3
COM5	5	5	3	3
COM6	5	5	3	3
COM7	5	5	3	3
COM8	5	5	3	3
COM9	5	5	3	3
COM10	5	5	3	3
COM11	5	5	3	3
COM12	5	5	3	3
COM13	5	5	3	3
COM14	5	5	3	3
COM15	5	5	3	3
COM16	5	5	3	3
COM17	5	5	4	4
COM18	4	5	3	3
COM19	4	5	3	3
P1	5	5	5	4
P2	5	5	4	5

Código	Confidencialidad	Integridad	Disponibilidad	Impacto
P3	5	3	5	4
P4	5	3	5	4
P5	5	3	5	4
P6	5	3	5	4
P7	5	3	5	4
P8	5	3	5	4
P9	5	3	5	4
P10	5	3	5	4
P11	5	3	5	4
P12	5	3	5	4
P13	5	3	5	4
P14	5	3	5	4
P15	5	3	5	3
P16	5	5	4	5
P17	5	5	3	4
P18	4	3	4	4
P19	4	3	2	3
P20	3	3	4	4
AUX1	5	5	5	4
AUX2	5	5	5	4
AUX3	5	5	4	4
Media1	5	5	3	4
Media2	5	5	3	4
Media3	5	5	4	3
Media4	5	5	4	3
Media5	4	5	4	3
Media7	5	5	5	5
L1	1	3	2	3
L2	1	3	2	3
L3	1	3	2	3
L4	1	3	2	3
L5	1	3	2	3
L6	1	3	2	3
L7	1	3	2	3

Código	Confidencialidad	Integridad	Disponibilidad	Impacto
L8	1	3	2	3
L9	1	3	2	3
L10	1	3	2	3
L11	1	3	2	3
L12	1	5	4	5

Fuente: Elaboración propia

6.2.5 Escenarios

- **Escenario1**

Probabilidad: 3

Dado que la mayoría de los archivos físicos están disponibles para todos los empleados de la empresa, se pueden presentar casos de alteración, eliminación y robo de información.

Vulnerabilidad: Archivos físicos desprotegidos, con acceso por parte de funcionarios de la empresa

Amenaza: Adulteración, robo del contenido del archivo

Activos afectados: Datos – D4, D5, D6.

- **Escenario 2**

Probabilidad: 4

Dado que la empresa no tiene políticas claras acerca del manejo de las contraseñas, se presenta que entre ellos se compartan sus contraseñas para acceso al sistema integrado u otros servicios, que puede generar adulteración o manipulación de información y datos dentro del mismo

Vulnerabilidad: Acceso a los datos del sistema financiero, por medio de contraseñas compartidas

Amenaza: Adulteración o robo de información, suplantación de permisos del funcionario

Activos afectados: Software – SW6, SW7, SW8.

- **Escenario 3**

Probabilidad: 5

Dado que la Joyería Orient no tiene implementado un área de sistemas definida dentro de la estructura de la empresa. No hay centralización de los servicios tecnológicos ni procedimientos adecuados.

Vulnerabilidad: Falta de punto de referencia en aspectos tecnológicos
Amenaza: Ausencia de políticas en seguridad informática, procedimientos no aplicados adecuadamente.

Activos afectados: Software – SW5, SW6, SW7, SW8, SW9, SW10, SW11, SW12, SW13. Hardware – HW1, HW2, HW3, HW4, HW5, HW6, HW7, HW8, HW9, HW10, HW11, HW12, HW13, HW14, HW15, HW16, HW17, HW18, HW19, HW20, HW21, HW22, HW23, HW24, HW25, HW26

- **Escenario 4**

Probabilidad: 4

Dado a que los empleados no conocen todas las políticas en seguridad de la información y/o no aplican los debidos procedimientos, formatos correspondientes, se han presentado demoras en los procesos y potencial pérdida de información.

Vulnerabilidad:

Demora en los procesos, inconformidad en los servicios

Amenaza: Pérdida de información, procesos con retrasos

Activos afectados: Servicios, Personas – S3, S4, S5, S6, S7, S8, S9, P4, P5, P10, P11.

- **Escenario 5**

Probabilidad: 3

Dado que el software logístico y contable no se ha terminado de implementar en todos los puntos se ha presentado fallas al generar reportes, back Ups y otros tipos de requerimientos solicitados por los directivos.

Vulnerabilidad: Falencias en los requerimientos funcionales del aplicativo, Falta de soporte eficiente en los puntos por parte del proveedor del software.
Amenaza: Retrasos en los procesos, falta de disponibilidad de la información.
Activos afectados: Software – SW6, SW7.

- **Escenario 6**

Probabilidad: 4

La Dirección Administrativa, empleados de contabilidad, administradores de punto, al ser la cabeza de la empresa y/o empleados de manejo información sensible, están expuestos a todo tipo de situaciones perjudiciales para la empresa.

Vulnerabilidad: Falta de políticas de manejo adecuado de información personal.

Amenaza: Extorsión, robo

Activos afectados: Personas – P1, P2, P3, P4, P5, P6, P7, P8, P9, P10, P11, P12, P13, P14, P15, P16

- **Escenario 7**

Amenaza: Eliminación, modificación, robo del contenido del archivo

Activos afectados: Equipo Auxiliar, Soporte de Información – AUX3, Media4, Media5, Media6, Media 7.

- **Escenario 8**

Probabilidad: 4

A pesar que en su mayoría todas las instalaciones se encuentran dentro de centros comerciales y teniendo en cuenta lo ya acontecido en dos de las instalaciones no existen mayores controles de ingreso a las mismas, lo cual puede presentar intrusiones de personas no autorizadas, que generan situaciones inesperadas y posible robo de información.

Vulnerabilidad: Información física de algunos procesos no resguardada apropiadamente.

Amenaza: Alteración del orden en las instalaciones, robo de información.

Activos afectados: Soporte de información, Instalaciones – Media1, Media 2, Media 3, Media 4, Media 5, Media 6, Media 7, L1, L2, L3, L4, L5, L6, L7, L8, L9, L10, L11, L12.

- **Escenario 9**

Probabilidad: 4

No existen los procedimientos debidamente documentados para la realización de los procesos de copias de seguridad, restauración de backups, ni los usuarios responsables de los mismos procesos, medios de almacenamiento backups.

Vulnerabilidad:

Falta de conocimiento en caso de presentarse un evento que requiera restaurar inmediatamente una copia de seguridad y no exista documentación.

Amenaza: caída de los servicios de la empresa y falta de disponibilidad de la información.

Activos afectados: Hardware – HW13, HW26

- **Escenario 10**

Probabilidad: 4

Existe las copias de seguridad de las principales bases de datos de la empresa, pero no existe ninguna copia espejo de los sistemas operativos Windows server y Linux de los servidores.

Vulnerabilidad: Falta plan acción de contingencia en caso de presentarse fallas en los servicios o errores en los sistemas operativos de los servidores.

Amenaza: Inoperatividad de la empresa y algunos servicios generando falta de disponibilidad de la información.

Activos afectados: Software – SW6, SW7, SW8, Soporte de información – HW13, HW26.

- **Escenario 11**

Probabilidad: 4

Dado de que no existe un medio de almacenamiento de backups alterno al servidor local de backups. Puede presentarse inconvenientes si el servidor local de backups presenta alguna falla.

Vulnerabilidad: Falta de medio de almacenamiento de backups alterno al servidor local de backups.

Amenaza: Inoperatividad del instituto y los servicios, Perdida de información, falta de disponibilidad.

Activos afectados: Hardware, Soporte de Información – HW12, HW13, HW26, Media7.

- **Escenario 12**

Probabilidad: 4

Dado que las oficinas principales no tienen un sistema de resguardo para la ausencia de energía eléctrica, se ha ocasionado que al momento de ausencia del servicio eléctrico, se ha perdido información.

Vulnerabilidad: Falta de una red de contingencia eléctrica.

Amenaza: Perdida de información.

Activos afectados: Hardware – HW1, HW2, HW3, HW4, HW5, HW6, HW7, HW8, HW9, HW10, HW11, HW12, HW13, HW14.

- **Escenario 13**

Probabilidad: 4

Actualmente la empresa no tiene una política del manejo y creación de usuarios y contraseñas, se ha presentado que entre los mismos compañeros se adivinen las contraseñas e ingresen al usuario de los demás.

Vulnerabilidad: Acceso a los datos del sistema Contable, logístico, Crediticio y equipos de cómputo.

Amenaza: Adulteración o robo de información, suplantación de permisos del funcionario.

Activos afectados: Claves Criptográficas**,** Software – SW6, SW7, SW8, K1.

6.3 DEFINIR LAS POLITICAS DE SEGURIDAD Y LOS CONTROLES NECESARIOS PARA MEJORAR EL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN LA JOYERIA

6.3.1 Controles. Teniendo en cuenta el proceso de seguridad de la empresa y los actuales escenarios, que presenta la empresa se han gestionado los diferentes controles para mejorar la seguridad de los diferentes activos y procesos, teniendo en cuenta el tipo de control a ejercer y su efectividad, como están a continuación en la tabla 12 controles.

Tabla 10. Controles

Código	Escenario	Tipo Control	Control	Efectividad
ESC1	Escenario 1	Correctivo	Protección de archivos y soportes de información físicos, por medio de archivos y en cuartos bajo llave, cámara de seguridad y/o protección de los funcionarios de la entidad	Reducción de la vulnerabilidad de un 60 a 80%
ESC2	Escenario 2	Preventivo	Implementación de políticas en seguridad de la información, referentes al manejo de las contraseñas por parte de los funcionarios de la entidad	Reducción de la vulnerabilidad de un 60 a 80%
ESC3	Escenario 3	Correctivo	Creación del área de un área de sistema para la empresa, de acuerdo a las estructuras de los gobiernos TI, actualmente existe un ingeniero que se encarga del soporte de los equipos y conoce el funcionamiento de la estructura, se recomienda que deba ser él, el líder del área.	Reducción de la vulnerabilidad de un 80 a 100%
ESC4	Escenario 4	Correctivo	Definir las políticas en seguridad de la información e implementarlas en el día a día de los funcionarios, a través de capacitaciones,	Reducción de la vulnerabilidad de un 80 a 100%

Código	Escenario	Tipo Control	Control	Efectividad
			afiches y demás comunicaciones corporativas	
ESC5	Escenario 5	Preventivo	Realizar un cronograma establecido para la implementación total de las herramientas contables y logísticas, ajustando los requerimientos que sean identificados e incluyendo los necesarios.	Reducción de la vulnerabilidad de un 60 a 80%
ESC6	Escenario 6	Preventivo	Apoyo en seguridad para las personas que posean información clasificada como confidencial o equipos con información de la misma índole, los cuales son esenciales para el normal funcionamiento de la entidad.	Reducción de la vulnerabilidad de un 30 a 60%
ESC7	Escenario 7	Preventivo	Creación de políticas acerca del resguardo de los archivos físicos con clasificación crítica de la empresa, en lugares con la protección adecuada y control permanente.	Reducción de la vulnerabilidad de un 30 a 60%
ESC8	Escenario 8	Preventivo	Aplicar los controles en seguridad básicos a los visitantes y demás personas que se encuentren en la empresa, además de implementar un mejor servicio de alarma en las instalaciones.	Reducción de la vulnerabilidad de un 80 a 100%
ESC9	Escenario 9	Correctivo	Definir los empleados o usuarios responsables del proceso de backups, implementando un plan de acción debidamente documentado por escrito sobre el proceso de	Reducción de la vulnerabilidad de un 80 a 100%

Código	Escenario	Tipo Control	Control	Efectividad
			creación y restauración de Backups	
ESC10	Escenario 10	Preventivo	Incluir en los procedimiento de backups de los servidores, la creación de copias espejo de los S.O. Windows Server y Linux.	Reducción de la vulnerabilidad de un 60 a 80%
ESC11	Escenario 11	Preventivo	Definir un medio de almacenamiento de backups alterno al servidor local, ya sea almacenamiento en un servidor web o través de un disco duro externo, el cual debe ser resguardado por personal autorizado en una ubicación segura.	Reducción de la vulnerabilidad de un 60 a 80%
ESC12	Escenario 12	Preventivo	Instalar una red de alimentación estable por medio de UPS o una planta eléctrica, para toda la infraestructura ya que por el momento solamente los servidores tienen este servicio.	Reducción de la vulnerabilidad de un 80 a 100%
ESC13	Escenario 13	Preventivo	Implementar una política de seguridad donde se establezca La longitud de las contraseñas debe ser de mínimo de ocho caracteres alfanuméricos (mayúsculas, minúsculas, números, símbolos), no deben parecerse a su nombre de usuario ni a su contraseña anterior y la caducidad de las contraseñas debe ser de 45 días	Reducción de la vulnerabilidad de un 60 a 80%

Fuente: Elaboración propia

6.4 POLÍTICAS GENERALES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.4.1 Regulación de los Controles Criptográficos. El área de tic debe estipular el sistema y técnicas criptográficas a implementar en la empresa siendo así el caso o la funcionalidad del mismo, estipulando el valor del activo y su impacto en la empresa, asegurando la integridad, confidencialidad de la información, este tipo de controles se deben tener en cuenta al momento de gestionar contraseñas, trasmitir información y salvaguardarla, para lo cual debemos estipular el tipo de cifrado, firma digital, servicios de no repudio entre otros.

Directriz:

- Se deben cifrar todos los discos duros de los equipos del personal de la empresa que contengan información privada de la misma.

- El manejo de las llaves, se debe llevar acorde a la **GESTION DE CONTRASEÑAS.**

- Todo aquel sistema de información con el cual se requiera, tener comunicación o transmisión de información, deben garantizar los mecanismos de cifrado entre ambos.

- Todos los documentos lógicos que contengan información pública reservada o clasificada se deben cifrar.

- Toda Base de datos e información que contenga información de contraseñas o claves, no deberá ser almacenada bajo texto, debe ser cifrada por mecanismos criptográficos.

6.4.2 Medio Extraíbles (CD – USB – Disco Duro Extraíbles)

Directriz

- El uso de medios extraíbles solo estará permitido de acuerdo a su rol y responsabilidad.

- Se deben cifrar todos los documentos o información por medio de la herramienta designada por la empresa antes de ser guardados en el medio extraíbles designado.

- La clave del cifrado debe ser compartida por un medio diferente del por qué se va a transportar la información.

- Debe quedar en el acta establecida, la información requerido, tal como responsable de la información, medio que se empleara, titulo de los documentos o archivos, cantidad y clave de cifrado.

- El funcionario será el único responsable de la información una vez se ha copiada al medio extraíble, por lo cual cualquier tipo de suceso que afecte la confidencialidad e integridad de la información será considerado como una falta a las normas de seguridad de la empresa y tendrá que someterse al consejo disciplinario de la empresa.

Esta política se ve respaldada por la política de **Gestión de soportes para medios extraíbles** en el ítem 6.4.4

6.4.3 Políticas y Procedimientos de Intercambio de Información. El área de tic debe estipular los reglamentos, métodos y técnicas a implementar en la transmisión o intercambio de información entre dos puntos de acuerdo a la sensibilidad de la misma.

Directriz

Intercambio de información:

- Toda información de la empresa considerada como sensible en la evaluación de activos, debe ser cifrada por medio de la herramienta estipulada en el manual de uso, la cual cumpla con las garantías para la protección de la integridad y confidencialidad de la misma.

- Cualquier tipo de intercambio de información debe quedar en el acta bajo la supervisión del área encargada por la empresa.

- La información no puede ser eliminada ni modificada bajo el proceso y de acuerdo lo estipule su rol y función

- Se deben ajustar las los controles de autenticación para la transmisión de la información, tarea solicitada al área de TI

- Cada funcionario será responsable por la información en caso de un incidente.

- La llave de cifrado debe ser entregada por un medio diferente al receptor.

6.4.3.1 Restricción del Acceso a la Información. Esta política complementa a las condiciones de roles y privilegios ya que por esta, el área de TIC se encarga de reglamentar de acuerdo a su perfil los acceso debidos de la información, esto estipulando reglas o condiciones para el mismo, lo cual proporciona que los usuarios deban cumplir ciertos requerimientos de cada aplicación o sistema a participar para tener acceso a la información.

Directriz

- El acceso acorde al rol o perfil de seguridad, determina si puede Modificar, Crear, Ver o no tener acceso a la información
- Todo acceso a la información debe ser en los equipos autorizados de la empresa.
- No debe estar habilitado la opción “Recordar clave en este equipo”
- No se debe enviar la contraseña por correo electrónico
- La clave del cifrado debe ser compartida por un medio diferente del por qué se va a transportar la información.
- Debe quedar en el acta establecida, la información requerido, tal como responsable de la información, medio que se empleara, titulo de los documentos o archivos, cantidad y clave de cifrado

6.4.4 Gestión de Soportes para Medios Extraíbles

Directriz

- Gestionar por medio de un directorio activo y reglas de un firewall, los permisos de acceso de plataformas y de recursos de la entidad.
- Solo los usuarios que requieren permisos podrán trabajar con medios extraíbles como USB, DVD, entre otros
- Todos los equipos tendrán bloqueado los dispositivos periféricos para el manejo de medios extraíbles.

6.4.5 Soporte Físico e Información en Tránsito. El área tic es responsable de salvaguardar la información crítica de la organización de una manera segura, a través de métodos de cifrado robustos que garanticen la disponibilidad, integridad y confidencialidad de los datos ante una eventual falla en los sistemas informáticos, debe de salvaguardar esta información en diferentes medios de almacenamiento como pueden ser, discos externos, tapes, o servidores externos para back up**.**

6.4.6 Política para la Gestión de Contraseñas. El área tic debe garantizar la seguridad en el acceso a la información, implementando políticas de acceso seguro a través de contraseñas robustas, las cuales deben de cumplir con los siguientes parámetros:

- La longitud de las contraseñas debe ser de mínimo de ocho caracteres alfanuméricos (mayúsculas, minúsculas, números, símbolos), no deben parecerse a su nombre de usuario ni a su contraseña anterior.

- La caducidad de las contraseñas debe ser de 45 días

- La caducidad de las contraseñas de Administrador de los diferentes sistemas debe ser 60 días.

7. CONCLUSIONES

De acuerdo a los objetivos planteados en el proyecto, se planteó el desarrollo del proceso de diagnóstico en la Joyeria Orient Colombia, allí se determinó la ausencia de las políticas de seguridad de la información, lineamientos y la aplicación de controles; con el fin de evitar y mitigar los posibles riesgos o amenazas, a los que se encuentran expuestos los activos de la información de la empresa; donde actualmente se encuentran en un 35% de no aplicar los controles actuales, un 32% de no tener controles o salvaguardas, de acuerdo al anexo 1, por lo que le permitirá a las directivas conocer el estado actual de la seguridad de la información de la empresa, así logrando reconocer la importancia de la implementación de un sistema de gestión de seguridad de la información.

Para llevar a cabo el segundo objetivo, se fundamentó en la identificación de activos y la importancia de los mismos en base a la rentabilidad de la empresa, este proceso permite a la misma poder identificar algunos activos los cuales desconocían la importancia de estos, llevando a tomar las medidas necesarias para la protección de ellos.

De igual forma, para llevar a cabo el segundo objetivo se planteó la aplicación de la metodología MAGERIT, permitiendo a la empresa identificar, valorar oportunamente el impacto y la probabilidad que se materialice una amenaza sobre cualquier activo de la información relacionado en el proceso, también se establecieron los posibles escenarios que dieran como resultado la pérdida o daño de los activos, esto para poder conocer aún más el proceso de la empresa, permitiendo establecer los controles apropiados para mitigar dicho daño.

RECOMENDACIONES

Los resultados esperados en el desarrollo del presente proyecto, son correspondientes a la concientización de las directivas y administradores de la joyería en base a la importancia que se tiene en el diseño e implementación de un SGSI con el fin de proteger uno de los activos más importantes, como lo es la información.

Esto debido a que lo encontrado en el estado actual de la seguridad de la información, desarrollado en el objetivo 1, nos brinda una señal de alerta al nivel alto de falencias en la protección de la información actual, por lo cual como primera media se recomienda la creación de un área de Infraestructura de Tecnología que permita la administración de los activos y la gestión de protección de los mismos.

Partiendo de ahí se recomienda la realización del Diseño de sistema de gestión de seguridad de la información para la empresa basado en un estándar ISO/IEC 27001:2013, que permita gestionar de una manera eficiente todos los activos de la información y la gestión del riesgo pertinente.

Teniendo en cuenta que para esto se requiere el compromiso por parte de las directivas para la puesta en marcha en la implementación del SGSI, para el fortalecimiento de la cultura de seguridad en la información es fundamental para la protección de la entidad.

BIBLIOGRAFÍA

AGUILERA, Purificación. Seguridad Informática: Ciclos Formativos. México: Editex, 2010, p.9.

ARDILA NAVARRETE, Julián Andrés. Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para Positiva Compañía de Seguros SA en la ciudad de Bogotá. Universidad Nacional Abierta y a Distancia. Bogotá, 2016. Disponible en: file:///C:/Users/Usuario/Downloads/79218306.pdf

CEDEÑO VALAREZO, Luis Cristóbal., MORALES CARRILLO, Jessica Johanna., DÁVILA MUÑOZ, Mayra Alejandra y PÁRRAGA ANDRADE, Gema Vanessa. Análisis de Riesgos tecnológicos en la cooperativa de ahorro y crédito Calceta Limitada. Revista Tecnológica-ESPOL, 2016, 29(1). Disponible en: http://rte.espol.edu.ec/index.php/tecnologica/article/view/492/329

COBIT-MODELO-DE-MADUREZ. Ipmoguide. 2019. Disponible en: https://ipmoguide.com/cobit-modelo-de-madurez/.

CONGRESO DE LA REPÚBLICA. 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. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

DE LA CRUZ GARCÍA, Juan Manuel. Delitos informáticos. El Cid Editor. 2009.

DELTA ASESORES. Ley de delitos informáticos en Colombia. 2014. Disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Decreto ley 19 de 2012. Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. 2012. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/decreto_0019_2012.html

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA. Método de analisis de riesgos. MAGERIT - Version 3.0 Metodología de Análisis y Gestión Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012, pág. 22.

GARCIA, Miguel Angel. Calculando la disponibilidad de sistemas complejos. 2015. Disponible en: https://magmax.org/blog/en-busca-de-los-cinco-9s/.

GOBIERNO DE ESPAÑA. MAGERIT V3. 2012. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XW_f3ChKjIU.

GÓMEZ VIEITES, Álvaro. Anexo III Análisis y Gestión de Riesgos en un Sistema Informático. Disponible en: https://www.academia.edu/5971566/Anexo_III_An%C3%A1lisis_y_Gesti%C3%B3n_de_Riesgos_en_un_Sistema_Inform%C3%A1tico.

GÓMEZ VIEITES, Álvaro. Seguridad en equipos informáticos. ProQuest Ebook Central. 2014. Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3229330

GONZALEZ, Frank. Diagnóstico y Actualización del Sistema de Gestión de Seguridad de la Información (SGSI) para Ventas y Servicios S.A. Trabajo de grado para Ingeniero de Sistemas. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p.

HERNÁNDEZ MEDINA, Diana Carolina. Diseño del sistema de gestión de seguridad de la información en Angelcom S.A. Universidad Libre. Bogotá, D.C. 2011. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/9097/PROYECTO%20FINAL.pdf?sequence=1&isAllowed=y

IBM. Utilización de listas de control de acceso de bases de datos para la identificación y autenticación. Disponible en: https://www.ibm.com/support/knowledgecenter/es/SSKTXQ_9.0.0/admin/config/st_adm_security_useridauth_c.html.

ISO27000.ES. 2020. Disponible en: https://www.iso27000.es/glosario.html.

ISOTOOLS EXCELLENCE. Norma-ISO-27002-control-de-accesos. Disponible en: https://www.pmg-ssi.com/2017/08/norma-iso-27002-control-de-accesos/.

INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá.: El Instituto, 2013. 37 p.

INSTITUTO DE CIBERSEGURIDAD - INCIBE. Glosario de términos de ciberseguridad. Una guia de apoximacion para el empresario. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

JOYERIA ORIENT. Disponible en: https://www.joyeriaorient.com/sobre-nosotros/.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES COLOMBIANAS. Seguridad y privacidad de la información. Rols y responsabilidades. Guia No. 4. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf.

NAVARRO BAHAMON, Macedonio y TRUJILLO HERNÁNDEZ, Carla Patricia. Análisis de seguridad al sistema de la Registraduría Nacional de Colombia. 2018.

RAMIÓ AGUIRRE, Jorge. Introducción a la seguridad informática y criptografía clásica. Universidad Politécnica de Madrid. 2016. Disponible en: http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion1.html

SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA. Seguridad de la Información. En: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, 2014, No. 1, p 15-16

UNIVERSIDAD NACIONAL DE COLOMBIA. Oficina Jurídica Nacional. Disponible en:http://www.legal.unal.edu.co/sisjurun/normas/Norma1.jsp?i=42011

ANEXOS

Anexo A. ISO 27002

De acuerdo a la Información recolectada se determina con el Anexo a o ISO 27002 que controles están implantados y cuáles no.

Tabla 1. Métrica ISO 27002

Estado	Significado
? Desconocido	No ha sido verificado
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Tabla 2. ISO 27002

Sección	Controles de Seguridad de la Información	Estado
A5	**Políticas de seguridad de la información**	
A5.1	**Directrices de gestión de la seguridad de la información**	
A5.1.1	Políticas para la seguridad de la información	Inicial
A5.1.2	Revisión de las políticas para la seguridad de la información	Repetible
A6	**Organización de la seguridad de la información**	
A6.1	**Organización interna**	
A6.1.1	Roles y responsabilidades en seguridad de la información	Inicial
A6.1.2	Segregación de tareas	Repetible
A6.1.3	Contacto con las autoridades	Definido
A6.1.4	Contacto con grupos de interés especial	Inexistente
A6.1.5	Seguridad de la información en la gestión de proyectos	Inexistente
A6.2	**Los dispositivos móviles y el teletrabajo**	
A6.2.1	Política de dispositivos móviles	Inexistente
A6.2.2	Teletrabajo	Inicial
A7	**Seguridad relativa a los recursos humanos**	
A7.1	**Antes del empleo**	
A7.1.1	Investigación de antecedentes	Administrado
A7.1.2	Términos y condiciones del empleo	Administrado
A7.2	**Durante el empleo**	
A7.2.1	Responsabilidades de gestión	Inicial
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inicial
A7.2.3	Proceso disciplinario	Inicial
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**	
A7.3.1	Responsabilidades ante la finalización o cambio	Definido
A8	**Gestión de activos**	
A8.1	**Responsabilidad sobre los activos**	
A8.1.1	Inventario de activos	Definido
A8.1.2	Propiedad de los activos	Definido
A8.1.3	Uso aceptable de los activos	Inicial
A8.1.4	Devolución de activos	Inexistente

Sección	Controles de Seguridad de la Información	Estado
A8.2	**Clasificación de la información**	
A8.2.1	Clasificación de la información	Inicial
A8.2.2	Etiquetado de la información	Inicial
A8.2.3	Manipulado de la información	Inicial
A8.3	**Manipulación de los soportes**	
A8.3.1	Gestión de soportes extraíbles	Repetible
A8.3.2	Eliminación de soportes	Inexistente
A8.3.3	Soportes físicos en tránsito	Inicial
A9	**Control de acceso**	
A9.1	**Requisitos de negocio para el control de acceso**	
A9.1.1	Política de control de acceso	Inicial
A9.1.2	Acceso a las redes y a los servicios de red	Inicial
A9.2	**Gestión de acceso de usuario**	
A9.2.1	Registro y baja de usuario	Administrado
A9.2.2	Provisión de acceso de usuario	Administrado
A9.2.3	Gestión de privilegios de acceso	Inicial
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Administrado
A9.2.5	Revisión de los derechos de acceso de usuario	Definido
A9.2.6	Retirada o reasignación de los derechos de acceso	Definido
A9.3	**Responsabilidades del usuario**	
A9.3.1	Uso de la información secreta de autenticación	Inicial
A9.4	**Control de acceso a sistemas y aplicaciones**	
A9.4.1	Restricción del acceso a la información	Administrado
A9.4.2	Procedimientos seguros de inicio de sesión	Administrado
A9.4.3	Sistema de gestión de contraseñas	Administrado
A9.4.4	Uso de utilidades con privilegios del sistema	Administrado
A9.4.5	Control de acceso al código fuente de los programas	Administrado
A10	**Criptografía**	
A10.1	**Controles criptográficos**	
A10.1.1	Política de uso de los controles criptográficos	Inexistente
A10.1.2	Gestión de claves	Inicial
A11	**Seguridad física y del entorno**	
A11.1	**Áreas seguras**	
A11.1.1	Perímetro de seguridad física	Inexistente

Sección	Controles de Seguridad de la Información	Estado
A11.1.2	Controles físicos de entrada	Inicial
A11.1.3	Seguridad de oficinas, despachos y recursos	Inicial
A11.1.4	Protección contra las amenazas externas y ambientales	Inicial
A11.1.5	El trabajo en áreas seguras	Administrado
A11.1.6	Áreas de carga y descarga	No aplicable
A11.2	**Seguridad de los equipos**	
A11.2.1	Emplazamiento y protección de equipos	Inexistente
A11.2.2	Instalaciones de suministro	Inexistente
A11.2.3	Seguridad del cableado	Inexistente
A11.2.4	Mantenimiento de los equipos	Inicial
A11.2.5	Retirada de materiales propiedad de la empresa	Inicial
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Inexistente
A11.2.7	Reutilización o eliminación segura de equipos	No aplicable
A11.2.8	Equipo de usuario desatendido	Inexistente
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Inicial
A12	**Seguridad de las operaciones**	
A12.1	**Procedimientos y responsabilidades operacionales**	
A12.1.1	Documentación de procedimientos operacionales	Definido
A12.1.2	Gestión de cambios	Inexistente
A12.1.3	Gestión de capacidades	Inexistente
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	No aplicable
A12.2	**Protección contra el software malicioso (malware)**	
A12.2.1	Controles contra el código malicioso	Definido
A12.3	**Copias de seguridad**	
A12.3.1	Copias de seguridad de la información	Definido
A12.4	**Registros y supervisión**	
A12.4.1	Registro de eventos	Inicial
A12.4.2	Protección de la información del registro	Definido
A12.4.3	Registros de administración y operación	Definido
A12.4.4	Sincronización del reloj	Inexistente
A12.5	**Control del software en explotación**	
A12.5.1	Instalación del software en explotación	Inexistente
A12.6	**Gestión de la vulnerabilidad técnica**	
A12.6.1	Gestión de las vulnerabilidades técnicas	Inicial
A12.6.2	Restricción en la instalación de software	Inicial

Sección	Controles de Seguridad de la Información	Estado
A12.7	**Consideraciones sobre la auditoria de sistemas de información**	
A12.7.1	Controles de auditoría de sistemas de información	Inexistente
A13	**Seguridad de las comunicaciones**	
A13.1	**Gestión de la seguridad de las redes**	
A13.1.1	Controles de red	Repetible
A13.1.2	Seguridad de los servicios de red	Repetible
A13.1.3	Segregación en redes	Inexistente
A13.2	**Intercambio de información**	
A13.2.1	Políticas y procedimientos de intercambio de información	Inicial
A13.2.2	Acuerdos de intercambio de información	Inicial
A13.2.3	Mensajería electrónica	Definido
A13.2.4	Acuerdos de confidencialidad o no revelación	Inicial
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	
A14.1	**Requisitos de seguridad en los sistemas de información**	
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Inexistente
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Inexistente
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Inexistente
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**	
A14.2.1	Política de desarrollo seguro	Inexistente
A14.2.2	Procedimiento de control de cambios en sistemas	Inexistente
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Inexistente
A14.2.4	Restricciones a los cambios en los paquetes de software	Inexistente
A14.2.5	Principios de ingeniería de sistemas seguros	Inexistente
A14.2.6	Entorno de desarrollo seguro	Inexistente
A14.2.7	Externalización del desarrollo de software	Inexistente
A14.2.8	Pruebas funcionales de seguridad de sistemas	Inexistente
A14.2.9	Pruebas de aceptación de sistemas	Inexistente
A14.3	**Datos de prueba**	
A14.3.1	Protección de los datos de prueba	Inexistente
A15	**Relación con proveedores**	

Sección	Controles de Seguridad de la Información	Estado
A15.1	**Seguridad en las relaciones con proveedores**	
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Administrado
A15.1.2	Requisitos de seguridad en contratos con terceros	Administrado
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Repetible
A15.2	**Gestión de la provisión de servicios del proveedor**	
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Optimizado
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Optimizado
A16	**Gestión de incidentes de seguridad de la información**	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**	
A16.1.1	Responsabilidades y procedimientos	Inicial
A16.1.2	Notificación de los eventos de seguridad de la información	Inicial
A16.1.3	Notificación de puntos débiles de la seguridad	Inicial
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Inicial
A16.1.5	Respuesta a incidentes de seguridad de la información	Inicial
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inexistente
A16.1.7	Recopilación de evidencias	Inexistente
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**	
A17.1	**Continuidad de la seguridad de la información**	
A17.1.1	Planificación de la continuidad de la seguridad de la información	Administrado
A17.1.2	Implementar la continuidad de la seguridad de la información	Inicial
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Inicial
A17.2	**Redundancias**	
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Repetible
A18	**Cumplimiento**	
A18.1	**Cumplimiento de los requisitos legales y contractuales**	

Sección	Controles de Seguridad de la Información	Estado
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Inexistente
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Inexistente
A18.1.3	Protección de los registros de la organización	Inexistente
A18.1.4	Protección y privacidad de la información de carácter personal	Inicial
A18.1.5	Regulación de los controles criptográficos	Inicial
A18.2	**Revisiones de la seguridad de la información**	
A18.2.1	Revisión independiente de la seguridad de la información	Inicial
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Inicial
A18.2.3	Comprobación del cumplimiento técnico	Inicial

Anexo B. Especificaciones técnicas de activos (hardware)

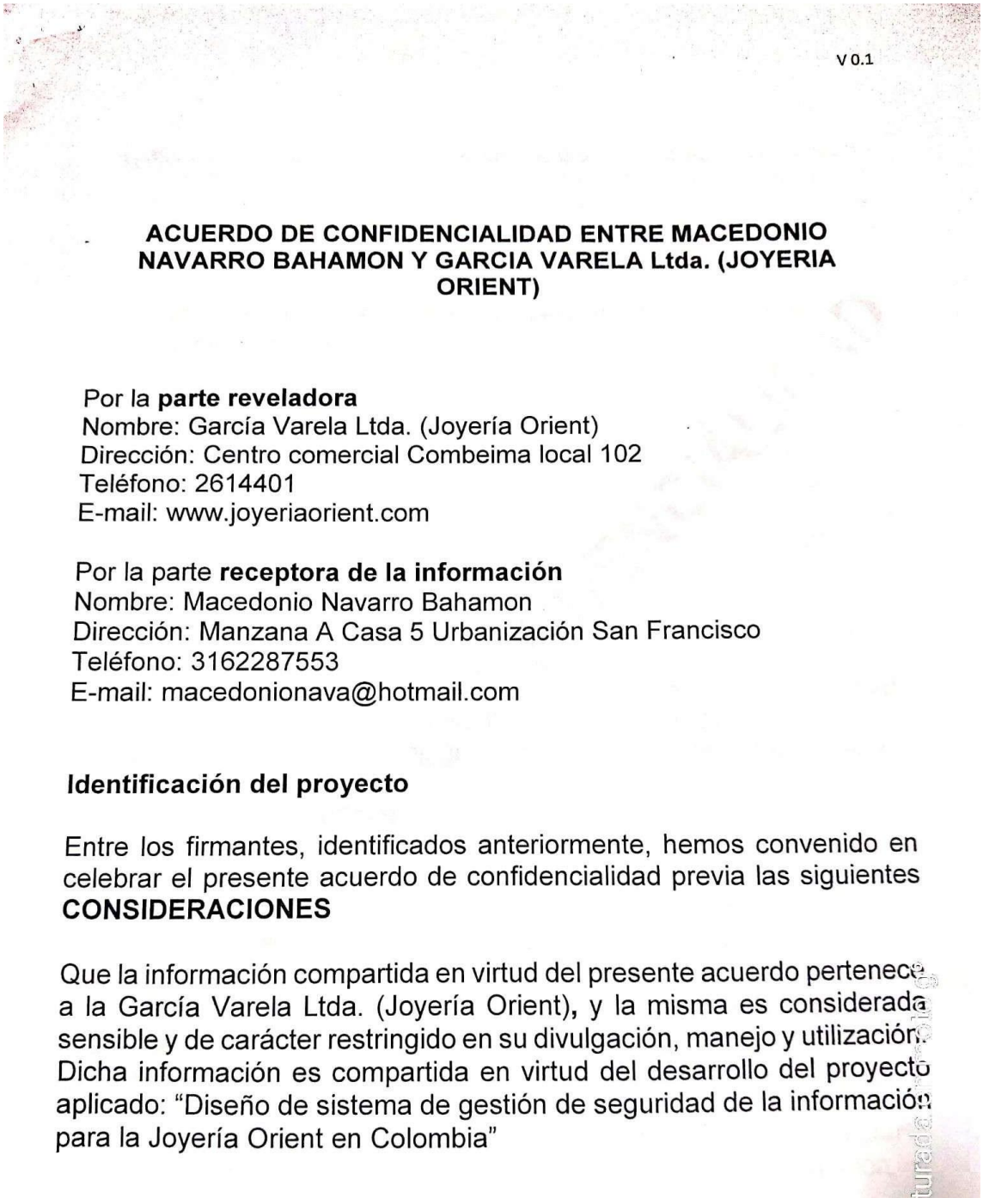
Taba 1. Especificación técnica de activos - hardware

Activo	Dispositivo	Característica
HW1,HW2,HW3	Marca	Tp-link
	Modelo	Tl-sg1024d
	Estándares Y Protocolos	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab , IEEE 802.3x
	Interfaz 24	10/100/1000Mbps RJ45 Ports
	Medios De Red	cable 3, 4 5, 10BASE-T: categoría UTP
	Fuente De Alimentación	100-240VAC, 50/60Hz
	Consumo De Energía Maximum	13.1W (220V/50Hz)
	Dimensiones	(W X D X H) 11.6*7.1*1.7 pulgadas (294*180*44 mm)
HW4, HW5, HW6, HW7, HW8	Marca	Lenovo
	Modelo	M72e
	Sistema Operativo	Windows 10 Home
	Procesador	Intel Core i5-3470S 2.90GHz
	Disco Duro	1 Tb
	Memoria RAM	4 GB
	Antivirus	Karpesky
	Firewall	Windows 10 Home
HW9	Marca	Lenovo
	Modelo	Windows 10 Home
	Sistema Operativo	Windows 10 Home
	Procesador	AMD Ryzen 5 Pro 3500U (2,10GHz)
	Disco Duro	500GB SSD
	Memoria RAM	8.0GB DDR4
	Antivirus	Karpesky
	Firewall	Windows 10 Home
HW10	Marca	HP

Activo	Dispositivo	Característica
	Modelo	Mfp 137
	Tipo	Multifunción
	Línea	LaserJet
	Conectividad	USB, WIFI
HW11	Marca	Hikvision
	Modelo	DS-2CE56H0T-IRMMF
	Imagen	5 Mpx
	Output	Analog HD output
HW12,HW26	Marca	DELL
	Modelo	PowerEdge T140
	Procesador	Intel® Xeon® E-2124, 3.3 GHz
	RAM	8 GB
	Disco Duro	5 TB
HW13	Marca	DELL
	Modelo	PowerEdge T440
	Procesador	Intel Xeon 3106 1.70GHz
	RAM	8 GB
	Disco Duro	2 TB
HW15,HW16,HW17,HW18,HW19,HW20,HW21,HW22,HW23,HW24,HW25	Marca	HP
	Modelo	20-C217
	Sistema Operativo	Windows 10 Home
	Procesador	Intel Celeron J6030
	Disco Duro	500 GB
	Memoria RAM	4 GB
	Antivirus	Karpesky
	Firewall	Windows 10 Home

Fuente: Elaboración propia

Anexo C. Acuerdo de confidencialidad



V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE MACEDONIO NAVARRO BAHAMON Y GARCIA VARELA Ltda. (JOYERIA ORIENT)

Por la **parte reveladora**
Nombre: García Varela Ltda. (Joyería Orient)
Dirección: Centro comercial Combeima local 102
Teléfono: 2614401
E-mail: www.joyeriaorient.com

Por la parte **receptora de la información**
Nombre: Macedonio Navarro Bahamon
Dirección: Manzana A Casa 5 Urbanización San Francisco
Teléfono: 3162287553
E-mail: macedonionava@hotmail.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

Que la información compartida en virtud del presente acuerdo pertenece a la García Varela Ltda. (Joyería Orient), y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto aplicado: "Diseño de sistema de gestión de seguridad de la información para la Joyería Orient en Colombia"

1. Que la información de propiedad de García Varela Ltda. (Joyería Orient) ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

   único y confidencial, o que es objeto de protección a título de secreto industrial.

Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación "Diseño de sistema de gestión de seguridad de la información para la Joyería Orient en Colombia", Macedonio Navarro Bahamon que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de García Varela Ltda. (Joyería Orient).

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al García Varela Ltda. (Joyería Orient), así como también a no utilizar dicha

Información en beneficio propio ni de terceros, sólo con fines estadisticos y de mejoramiento de la García Varela Ltda. (Joyería Orient).

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,

   modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto "Diseño de sistema de gestión de seguridad de la información para la Joyería Orient en Colombia" lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma García Varela Ltda. (Joyería Orient), restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de García Varela Ltda. (Joyería Orient).

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: *Describir la información que se tomará en el proyecto para su desarrollo, deben tener en cuenta que si existe información como nombre, apellido, cédula, teléfono estas deben ser amparadas por la ley 1581 de 2012 y no puede ser revelada en el documento final del proyecto.*

10. La información capturada por la **parte receptora** se observará como *cifras para estudio estadístico, en la generación del modelo MAGERIT, información cuantitativa*, no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad toda la persona García Varela Ltda. (Joyería Orient)no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de García Varela Ltda. (Joyería Orient), ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante Macedonio Navarro Bahamon se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa García Varela Ltda. (Joyería Orient) para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el respositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la emresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo**. La **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes (Macedonio Navarro Bahamon - García Varela Ltda. (Joyería Orient)) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las clausulas del presente acuerdo de confidencialidad por parte de Macedonio Navarro Bahamon.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Ibagué -Tolima, a los (24) días del mes de (Abril) de 2020

Como Parte Receptora:

MACEDONIO NAVARRO B.
Macedonio Navarro Bahamon
Estudiante UNAD.
C.C. No. 1110467462 de Ibagué

Por la parte reveladora:

Sherina E Granados G
Sherina Granados García
García Varela Ltda.-Joyería Orient
C.C. No. 65.773.100 de Ibagué

Anexo D. Autorización a ejecución de proyecto

V0.1

Ibagué, 24 de Abril de 2020

Señora:
SHERINA GRANADOS GARCÍA
Directora Administrativa

Asunto: Autorización para la ejecución del proyecto titulado: "Diseño de sistema de gestión de seguridad de la información para la Joyería Orient en Colombia".

Cordial saludo estimada Directora,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a García Varela Ltda. (Joyería Orient), de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: "Diseño de sistema de gestión de seguridad de la información para la Joyería Orient en Colombia" el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

- El proyecto en su objetivo general describe lo siguiente: Realizar el diseño del SGSI, por medio de un análisis y valoración del riesgo de activos, lo cual permitirá poder implementar controles y políticas en la seguridad de la información de la Joyería Orient en Colombia; al mismo tiempo será apoyado por los objetivos específicos: Conocer el estado actual del sistema de gestión de

seguridad de la información en base al Anexo A ISO 27001-2013, identificar los posibles activos de la información y riesgos de la joyería Orient, teniendo en cuenta la metodología MAGERIT y definir las políticas de seguridad y los controles necesarios para mejorar el sistema de gestión de seguridad de la información[cs1] en la Joyería Orient[MJMH2], para obtener como resultado un alto impacto en la seguridad de la empresa García Varela Ltda. (Joyería Orient).

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por García Varela Ltda. (Joyería Orient).
- La empresa García Varela Ltda. (Joyería Orient) deberá establecer qué tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El dcumento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados

el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en Ibagué, a los (24) días del mes de (Abril) de 2020

Cordialmente,

Macedonio Navarro B.

Macedonio Navarro Bahamon
Estudiante UNAD.

Sherina E Granados G

Sherina Granados García
Directora Administrativa