DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO LOS LINEAMIENTOS DEL ESTANDAR ISO/IEC 27001:2013 PARA LA NOTARÍA ÚNICA DE LA CIUDAD DE DOSQUEBRADAS (RISARALDA)

OCTAVIO DE JESÚS PULGARÍN GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2023

DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO LOS LINEAMIENTOS DEL ESTANDAR ISO/IEC 27001:2013 PARA LA NOTARÍA ÚNICA DE LA CIUDAD DE DOSQUEBRADAS (RISARALDA)

OCTAVIO DE JESÚS PULGARÍN GARCÍA

Proyecto de Grado – Trabajo aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

EDGAR ROBERTO DULCE VILLARREAL
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Este trabajo está dedicado a todas las personas que directa e indirectamente me han acompañado en todos los momentos de mi vida en especial a la ayuda espiritual de mi madre Adela a mi hermana Gloria Inés y a Gloria Mercedes que ha sido una brújula importante para guiarme en momentos donde estoy perdiendo el norte.

AGRADECIMIENTOS

Agradezco especialmente a Carolina Marín del Rio gerente de la Notaría Única de la ciudad de Dosquebradas, de igual forma al Dr. Javier Cano Ramírez notario único del círculo de Dosquebradas que permitieron mi formación, a mis tutores de la Universidad Abierta y a Distancia UNAD por su acompañamiento en este trabajo.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

Activos TI: Son todos los bienes o recursos que posee una organización para el tratamiento de la información, de su uso adecuado dependerá en gran medida el cumplimento de los objetivos de la organizacionales[1].

ISO 27001: Estándar enfocado en procesos adoptando el modelo PDCA (Planear, Hacer, Verificar y Actuar) este modelo aporta al estándar la identificación de procesos en una organización y su mejora continua[2].

ISO: Su significado se refiere a International Organization for Standardization es la organización encargada de generar estándares internacionales; desde sus inicios en los años 40 a la fecha, han generado más de 23.000 estándares en diferentes áreas que han permitido el establecimiento de patrones y la mejora continua de los procesos organizacionales[3].

Mejora continua: En las organizaciones cualquiera que sea su naturaleza existen procesos, estar revisando su forma de operar, productividad y problemas y estar mejorándolos en función de hacerlos óptimos y seguros es el enfoque de este proceso[4].

---

[1] TECNOLOGÍAS INFORMACION, Integridad de datos. [Sitio Web]. [Consulta: 18 de marzo de 2022]. Disponible en: https://www.tecnologias-informacion.com/integridaddatos.html
UNIR, Claves de las políticas de seguridad informática. [Sitio Web]. La Rioja [Consulta: 19 de marzo de 2022]. Disponible en: unir.net/ingenieria/revista/politicas-seguridad-informatica/

[2] GLOBAL SUITE, ¿Cuál es el objetivo fundamental de las normas ISO? [Sitio Web]. [Consulta: 18 de marzo de 2022]. Disponible en: https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:~:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.

[3] 27001 ACADEMY, ¿Qué es norma ISO 27001? [Sitio Web]. Zagreb. [Consulta: 18 de marzo de 2022]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

[4] HEFLO. Mejora continua. [Sitio Web]. Brasil. [Consulta: 19 de marzo de 2022]. Disponible en: https://www.heflo.com/es/definiciones/mejora-continua/

Políticas de Seguridad: Normas que establece una organización para que la información conserve su integridad, disponibilidad e integridad y que permite mitigar las vulnerabilidades presentes en los sistemas de información.

Procedimientos de seguridad: Permiten definir de forma específica, las políticas de seguridad de una organización en estos se definen los paso a paso a seguir para un uso adecuado de los recursos tecnológicos[5].

Riesgo de la seguridad de la información: Es la probabilidad de que ocurra un suceso que vulnere la seguridad de los sistemas informáticos de una organización valiéndose de sus debilidades[6].

Seguridad de la información: Conjunto de políticas utilizadas para proteger la seguridad de los datos de una organización, estas políticas están en procura de preservar la disponibilidad, integridad y confidencialidad[7].

Vulnerabilidad de la información: Es la debilidad que se encuentra en un sistema de información y es aprovechada para dañar o robar la información, esta puede encontrarse en los equipos, programas, procesos, personas y todo el universo organizacional[8].

---

[5] FRESHSERVICE, Gestión de activos de TI. [Sitio Web]. [Consulta: 18 de marzo de 2022]. Disponible en: https://freshservice.com/latam/it-asset-management-software/

[6] BANCO SANTANDER, ¿Qué es una vulnerabilidad informática? [Sitio Web]. [Consulta: 18 de marzo de 2022]. Disponible en: CONEXIÓN ESAN, Las cuatro etapas para la mejora continua en la organización. [Sitio Web]. Monterico. [Consulta: 17 de marzo de 2022]. Disponible en: https://www.esan.edu.pe/conexion-esan/las-cuatro-etapas-para-la-mejora-continua-en-la-organizacion#:~:text=El%20nombre%20del%20ciclo%20PDCA,etapas%20en%20el%20siguiente%20art%C3%ADculo

[7] LD GRUPO, Ciberseguridad. [Sitio Web]. Lima, Breña [Consulta: 19 de marzo de 2022]. Disponible en: https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/

[8] UNIR, Claves de las políticas de seguridad informática. [Sitio Web]. La Rioja [Consulta: 19 de marzo de 2022]. Disponible en: unir.net/ingenieria/revista/politicas-seguridad-informatica/

RESUMEN

Las Notarías en Colombia son lugares donde un notario (nombrado por el estado para ejercer funciones públicas) se encarga de dar fe pública sobre las voluntades de los ciudadanos y documentos, en la actualidad existen alrededor de 924 Notarías en todo el territorio nacional a enero del 2023 según datos de la Superintendencia de Notariado y Registro ente encargado de su vigilancia.

Para cumplir con su ejercicio, el notario contrata un personal idóneo que se encarga de la atención al público en los servicios notariales de autenticaciones, declaraciones, escrituración, registro civil, asesorías jurídicas entre otros servicios. Cada uno de estos procesos internos se encarga de gestionar diferente información física y digital en sus instalaciones ubicadas en la ciudad de Dosquebradas Risaralda.

En el siguiente trabajo aplicado abordaremos el diseño del sistema de gestión SGSI bajo el estándar ISO 27001:2013 para la notaría Única de la ciudad de Dosquebradas permitiendo identificar cada uno de los activos con que cuenta la organización, categorizarlos y definir el nivel de criticidad entre alto, medio o bajo. Con estos criterios definidos entre medio y alto como factor para hallar las debilidades se realizaron diferentes consultas en fuentes y repositorios en la web, destacando los CVE y CWE. Con las vulnerabilidades detectadas se definieron según el anexo A del estándar los diferentes controles a aplicar para que los procesos si así lo definen la organización gestionen de forma segura la información dentro de sus procesos internos.

Palabras claves: Activos, controles, información, ISO/IEC 27001, mejora continua, notaría, políticas, procesos, Seguridad de la información, Sistema de Gestión, vulnerabilidad.

ABSTRACT

Notaries in Colombia are places where a notary (appointed by the state to exercise public functions) is in charge of giving public faith on the wills of citizens and documents, there are currently around 904 Notaries throughout the national territory as of March 2022 according to data from the Superintendence of Notaries and Registration, the entity in charge of its surveillance.

In order to carry out his exercise, the notary hires suitable personnel who are in charge of serving the public in the notarial services of authentications, declarations, deeds, civil registration, legal advice, among other services. Each of these internal processes is responsible for managing different physical and digital information at its facilities located in the city of Dosquebradas Risaralda.

In the following applied work, we will address the design of the ISMS management system under the ISO 27001:2013 standard for the Sole Notary of the city of Dosquebradas, allowing the identification of each of the assets that the organization has, categorize them and define the level of criticality between them. high, medium or low. With the criteria defined between medium and high as a factor to find weaknesses, different queries were made in sources and repositories, highlighting the CVE and CWE. With the vulnerabilities detected, according to Annex A of the standard, the different controls to be applied were defined so that the processes, if so, defined by the organization, can safely manage the information within their internal processes.

Keywords: Assets, controls, information, ISO/IEC 27001, continuous improvement, notary, policies, processes, Information Security, Management System, vulnerability.

INTRODUCCIÓN

Las organizaciones cuando se conforman van en busca de cumplir objetivos, unas se crean con una visión clara de lo que quieren hacer o cual será su nicho de mercado; otras en cambio, nacen como una idea de negocio que se van organizando a medida que la normatividad lo exige o el nivel de crecimiento que se espera lograr.

A medida que las organizaciones evolucionan, crecen factores como el recurso humano, la tecnología, sus clientes entre otros recursos que se hacen importantes para el día a día del negocio. Indiscutiblemente todos los recursos en una organización tienen que ver con uno de los activos más importantes, se trata de la información; de cómo se gestione, cuide o se tenga disponible este activo va a definir en gran medida la permanencia en el tiempo de una empresa.

Cuando la organización comprende la importancia de la información que genera, consultan o procesan surge la necesidad de protegerla, es allí donde estándares como el ISO/IEC 27001:2013 aporta de manera importante a las organizaciones el mantener este activo bajo condiciones seguras.

En el siguiente trabajo abordaremos el diseño del sistema de Gestión de la seguridad de la información para la Notaría Única de la Ciudad de Dosquebradas identificando los activos con que cuentan, sus procesos internos y sus vulnerabilidades, definiendo el alcance del sistema y proponiendo las políticas para brindar seguridad a este activo tan valioso para la organización.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La problemática de seguridad de la información que nace del crecimiento de una organización no es solo de entidades publico privadas como la Notará Única de la ciudad de Dosquebradas, se convierte en un problema propio de cada sector productivo que necesite gestionar la información de forma rápida y segura.

El enfoque tecnológico de la Notaría Única de Dosquebradas se ha basado en mantener la información disponible para ser gestionada por sus colaboradores, esto ha llevado a que la integridad y confidencialidad de la información no sean factores críticos; si bien se han implementado métodos de protección como Firewall o antivirus, aun no se cuentan con políticas de seguridad que ayuden a encontrar un balance entre la confidencialidad, integridad y disponibilidad generando una protección proactiva que evite pérdidas o daños de la información.

1.2 DESCRIPCIÓN DEL PROBLEMA

El constante cambio en las políticas de Estado que obligan a las organizaciones a realizar un uso adecuado de los datos personales, las responsabilidades de las organizaciones publico privadas en salvaguardar la información y en especial las Notarías en guardar y conservar la información contenida en los diferentes actos notariales, los constantes ataques cibernéticos a los que se está expuestas las organizaciones cuando utilizan los servicio de internet deben llevar a las organizaciones a preparasen ante posibles ataques y/o perdidas de información.

La Notaría Única de la ciudad de Dosquebradas no cuenta en este momento con políticas, procedimientos o controles de seguridad de la información para garantizar su disponibilidad, confiabilidad e integridad ni tampoco con un inventario de sus activos tecnológicos encargados de procesar la información y mucho menos se han evaluado las vulnerabilidades a las que está expuesta la información.

Revisando este panorama actual en el que se encuentra la Notaría Única de la ciudad de Dosquebradas podemos observar que se encuentra muy expuesta a la pérdida o mala manipulación de la información.

1.3 FORMULACIÓN DEL PROBLEMA

¿El diseño de un sistema de gestión bajo el estándar ISO 27001:2013 permitirá mejorar la seguridad de la información en la Notaría Única de la ciudad de Dosquebradas (Risaralda)?

2 JUSTIFICACIÓN

Para las organizaciones es de vital importancia contar con políticas, procedimientos y/o controles que ayuden a salvaguardar la seguridad de la información en sus procesos, ya que de no existir generarían una gran exposición a daños o ataques que se traducen en un alto costo en tiempo y dinero en su recuperación si esta fuera posible recuperarla.

Una guía para lograr procesos seguros en torno a la información es la norma ISO 27001:2013 que pertenece a la familia de las norma ISO 27000, esta norma define los requisitos para implementar el SGSI (Sistema de Gestión de la Seguridad de la Información) esta puede ser aplicada a organizaciones públicas, privadas o mixtas sin importar su tamaño; se enfoca en el ciclo de mejora continua o circulo Deming (Planear, Hacer, Verificar y Actuar) PHVA por su siglas en español y permite a la organización identificar los riesgos o ataques que pueden afectar la información y por ende la operación.

El estándar tiene la característica que puede ser certificado permitiendo generar confianza entre los usuarios internos y externos en torno al manejo seguro de la información; otra de sus características, es que no solo está enfocada en los equipos o proceso del área de TI, sino que aborda la Notaría desde sus diferentes procesos (autenticaciones, declaraciones, escrituración, registro civil, registro, rentas, contabilidad y administración).

En temas legales las Notarías deben asegurar que en materia de seguridad de la información se cumplan los parámetros establecidos por la Superintendencia de Notariado y Registro, contar con el diseño de las políticas y controles aseguran que el marco legal se encuentra cubierto permitiendo a la organización su cumplimiento.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar el sistema de gestión bajo el estándar ISO 27001:2013 para mejorar la seguridad de la información en la Notaría Única de la ciudad de Dosquebradas (Risaralda).

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos con que cuenta la Notaría Única de la ciudad de Dosquebradas (Risaralda) para el manejo de la información bajo el estándar ISO/IEC 27001:2013.

- Definir el alcance del diseño del sistema de gestión de la seguridad de la información según los parámetros del estándar ISO/IEC 27001:2013.

- Identificar las vulnerabilidades para los activos de la Notaría Única de la ciudad de Dosquebradas (Risaralda).

- Proponer el diseño de las políticas de seguridad de la información bajo los lineamientos el estándar ISO/IEC 27001:2013.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Sistema de gestión de la seguridad de la información

Un sistema de gestión de la seguridad de la información ayuda a conocer el riesgo al que se encuentra expuesta la información en una organización, esta herramienta permite reducir el nivel de riesgo y se convierte en un canal de comunicación eficiente entre los responsables de la gestión de la información.

Uno de los estándares más utilizados en esta materia es la norma ISO/IEC 27001 que pertenece a la familia de normas ISO 27000 enfocadas en la seguridad de la información.

Según Icontec ente certificador de esta norma dentro de sus beneficios se encuentran:

- Habilitar y potencializar el uso de herramientas de gestión para proteger la confidencialidad, integridad y disponibilidad de la información.
- Prevenir y reducir el nivel de riesgo mediante la implementación de controles.
- Permitir a la gerencia gestionar de forma adecuada los recursos que se necesitan para mantener la seguridad de la información.
- Generar en los colaboradores la importancia de la seguridad de la información en la organización[9].

[9] ICONTEC, Certificación ISO 27001, Sistemas de Gestión de seguridad de la información. [Sitio Web]. Bogotá. [Consultado: 17 de abril de 2022]. Disponible en: https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/

4.1.2 ISO/IEC 27001:2013

En busca de que se conserven los tres pilares de la seguridad de la información en una organización; en términos generales hablamos de la confidencialidad, integridad y disponibilidad existe el estándar ISO/IEC 27001:2013 enfocado en la implementación de procesos de gestión del riesgo al interior de una organización a través de controles que ayudan a generar conciencia en la importancia de la seguridad de la información; los elementos de este estándar deben hacer parte fundamental de la cultura organizacional siendo una ventaja de este estándar la adaptación a las necesidades en materia de protección de la seguridad de la información[10].

4.1.3 CICLO PHVA

También conocido como ciclo Deming es una herramienta fundamental para los sistemas de gestión, basado en las etapas de Planear, Hacer, Verificar y Actuar permitiendo a las organizaciones mejorar continuamente sus procesos.

4.1.4 PLANEAR

Es aquí donde se conciben los objetivos articulándolos a los procesos internos de la organización haciendo participes del proceso de la gestión a los responsables de cada proceso, es la etapa inicial y una de las más importantes porque de su buen diagnóstico dependerá el éxito de la siguiente fase.

---

[10] ACADEMIA, Norma ISO NTC-ISO-IEC 27001. [En línea] [Consultado: 17 de abril de 2022]. Disponible en: https://www.academia.edu/40913480/NORMA_T%C3%89CNICA_NTC_ISO_IEC_COLOMBIANA_27001_TECNOLOG%C3%8DA_DE_LA_INFORMACI%C3%93N_T%C3%89CNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTI%C3%93N_DE_LA_SEGURIDAD_DE_LA_INFORMACI%C3%93N_REQUISITOS

4.1.4.1 HACER

En esta fase se lleva a cabo la ejecución de los objetivos anteriormente identificados, en esta etapa se detectan los diferentes problemas de implementación y se pueden determinar los ajustes al proceso.

4.1.4.2 VERIFICAR

Como su nombre lo indica en esta etapa se verifica que lo que se está ejecutando es acorde a lo que se definió en la primera etapa (Planear).

4.1.4.3 ACTUAR

Este punto del ciclo ayuda a que los proceso evolucionen ayudando a mitigar las desviaciones que se puedan presentar determinando como se le debe hacer seguimiento a lo implementado[11].

Si bien el ciclo PHVA consta de estas 4 fases este proyecto se enfocará en la primera fase donde se determinaron los objetivos trazados por la organización para salvaguardar la información.

[11] GERENCIE, Ciclo PHVA. [En línea] [Consultado: 17 de abril de 2022]. Disponible en: https://www.gerencie.com/ciclo-phva.html

4.2 MARCO CONCEPTUAL

4.2.1 Seguridad de la información

Cuando hablamos de seguridad de la información nos referimos a todo el conjunto de medidas necesarias implementadas por una organización para asegurar que los datos se encuentren debidamente protegidos.

Toda organización sin importar su tamaño dentro de sus procesos va a manipular datos, en esta manipulación propia del proceso se deben garantizar tres aspectos indispensables: Integridad, confidencialidad y disponibilidad[12].

4.2.1.1 Confidencialidad

No toda la información almacenada en una organización puede ser consultada por todos los que hacen parte de ella, esta propiedad permite que los datos sean consultados por las personas adecuadas y que no sean propagados sin la debida autorización[13].

4.2.1.2 Disponibilidad

[12] AYUDALEY, Seguridad de la información: Aspectos para tener en cuenta. [En línea] [Consultado: 17 de abril de 2022]. Disponible en: https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/

[13] ISOTOOLS, ¿Qué es la seguridad de la información y cuantos tipos hay? [Sitio Web]. Santiago. [Consulta: 18 de marzo de 2022]. Disponible en: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Asegurar que la información se pueda consultar en el momento que se necesita y generar los diferentes medios para que esta pueda ser consultada es la capacidad que nos brinda este servicio[14].

4.2.1.3 Integridad

hablamos de integridad cuando la información no ha sufrido ninguna alteración y son fiel copia de los que reposan en la base de datos de una organización, este proceso evita que los datos no estén duplicados, incorrectos o que sean alterados[15].

4.2.1.4 Servicios Notariales

Los servicios públicos notariales son aquellos prestados por los notarios donde implica dar autenticidad pública de los documentos o hechos presentados ante él (Articulo 1 ley 588 de 2000)[16].

4.2.1.5 Documento digital

[14] Ibid., p. 1.

[15] Ibid., p. 1.

[16] SNR, Boceto Manual Preguntas Frecuentes Servicio Notarial. [Sitio Web]. Bogotá. [Consulta: 26 de mayo de 2022]. Disponible en: https://www.supernotariado.gov.co/files/portal/66.Ley%20de%20Trasparencia-66.2.Informacion%20de%20Interes/3.Boceto%20Manual%20Preguntas%20Frecuentes%20Servicio%20Notarial%20B.pdf

Representa un documento digital que se encuentra almacenado en bits (0,1) de un documento físico, su codificación permite el almacenamiento y visualización en dispositivos electrónicos[17].

4.2.1.6 Escritura pública

Documento que contiene la declaración de voluntad de una o varias partes interesadas en hacer una negociación o delegar un derecho, este documento es presentado ante el notario quien da la plena autenticidad de la voluntad de la parte o partes interesadas. Consta de 4 etapas:

- Recepción de las voluntades de las partes interesadas.
- Redacción y escritura de las voluntades.
- Firma del documento por parte de los interesados en expresar su voluntad.
- Firma por parte del Notario y que le da el estatus de Escritura pública[18].

4.2.1.7 Notario

Persona natural quien es delegado por el estado colombiano mediante el Decreto Ley 960 de 1970 para ejercer la función pública notarial sin que esta delegación lo convierta en empleado público, encargado de dar autenticidad pública de las

[17] SECRETARÍA DISTRITAL, Documento digital. [Sitio Web]. Bogotá. [Consulta: 26 de mayo de 2022]. Disponible en: https://www.sdp.gov.co/transparencia/informacion-interes/glosario/documento-digital

[18] SNR, Boceto Manual Preguntas Frecuentes Servicio Notarial. [Sitio Web]. Bogotá. [Consulta: 26 de mayo de 2022]. Disponible en: https://www.supernotariado.gov.co/files/portal/66.Ley%20de%20Trasparencia-66.2.Informacion%20de%20Interes/3.Boceto%20Manual%20Preguntas%20Frecuentes%20Servicio%20Notarial%20B.pdf

diligencias y trámites presentadas ante él; el notario es vigilado por la Superintendencia de Notariado y Registro ente que supervisa el estricto cumplimiento de sus funciones[19].

4.2.1.8 Protocolista

Persona técnica con conocimiento normativo notarial encargado de la realización escrita de las voluntades de los ciudadanos, con su experticia tiene la capacidad de plasmar en un documento que posteriormente se convertirá en una escritura pública que esta cumpla con la normatividad legal vigente.

4.2.1.9 Protocolo

El protocolo es el archivo físico donde se encuentran alojadas las escrituras públicas, estas deben estar en el lugar de despacho del notario y son de consulta pública[20].

4.2.1.10 Declaraciones extra-proceso

[19] Ibid., p. 8.

[20] SNR, Boceto Manual Preguntas Frecuentes Servicio Notarial. [Sitio Web]. Bogotá. [Consulta: 26 de mayo de 2022]. Disponible en: https://www.supernotariado.gov.co/files/portal/66.Ley%20de%20Trasparencia-66.2.Informacion%20de%20Interes/3.Boceto%20Manual%20Preguntas%20Frecuentes%20Servicio%20Notarial%20B.pdf

Las declaraciones extra-proceso también llamadas declaraciones extrajuicio son aquellas manifestaciones que realizan los ciudadanos de forma libre y sin ninguna presión donde manifiesta el testimonio de un hecho en particular ante un notario[21].

[21] NOTARIA 32 BOGOTÁ, Declaraciones extrajuicio. [Sitio Web]. Bogotá. [Consulta: 26 de mayo de 2022]. Disponible en: https://www.notaria32bogota.com.co/sitio/tramites-y-servicios/declaraciones-extrajuicio

5 DISEÑO METODOLÓGICO

Para el diseño de gestión de la seguridad de informática bajo la norma ISO 27001:2013 se tendrán en cuenta su fase de planeación que consta del establecimiento del Sistema de Gestión de la seguridad de la información:

- Identificar las necesidades y expectativas de las partes interesadas.
- Identificar los activos de información.
- Categorizar los activos de información según su criticidad.
- Identificar vulnerabilidades de las categorías identificadas.
- Aplicar controles a las categorías identificadas y a su vez a los activos de información.

6 IDENTIFICAR LOS ACTIVOS CON QUE CUENTA LA NOTARÍA ÚNICA DE LA CIUDAD DE DOSQUEBRADAS (RISARALDA) PARA EL MANEJO DE LA INFORMACIÓN BAJO EL ESTÁNDAR ISO/IEC 27001:2013

Para una organización sin importar su tamaño es muy importante contar con un inventario de activos donde se gestiona la información; para la Notaría Única de la ciudad de Dosquebradas este panorama no debe ser indiferente ya que tenerlo es la base para gestionar su seguridad según la norma ISO/IEC 2007:2013.

Para desarrollar este punto se tendrá en cuenta el anexo A *Objetivos de control y controles de referencia* en su numeral A.8 Gestión de Activos de la norma ISO/IEC 2007:2013.

En esta gestión es importante Identificar los activos, identificar un propietario clasificarlo, definir su criticidad, impacto ante su perdida y compromiso de la organización.

- **Identificar Activos**: El proceso de identificar qué activos directa o indirectamente procesan, mantienen y custodian la información de la Notaría Única de Dosquebradas es de vital importancia; para realizar esta identificación se tendrán en cuenta los procesos internos que son: Autenticaciones, Registro y Rentas, Protocolo, Recursos humanos, Gerencia, Contabilidad, Jurídica y Sistemas.
- **Identificar propietario**: Es la persona en la organización líder del proceso interno de la Notaría, cada proceso cuenta con un responsable nombrado desde la Gerencia y se convierte en un activo del recurso humano.
- **Clasificación**: Este parámetro define el tipo al que pertenece el activo, bajo los parámetros: Software, Hardware, Información, Servicio y Otros; estos últimos son activos que no aplican dentro de ninguna clasificación anterior.

- **Criticidad**: Determinar el valor de un activo según su Disponibilidad, integridad y confidencialidad; siendo Alta, media y baja el criterio de valoración que el activo debe mantener como se muestra en el cuadro 1.

Cuadro 1. Valor de criticidad del activo

ALTA	Activos que deben conservar la integridad, disponibilidad y confidencialidad
MEDIA	Activos que deben conservar 2 valores entre la integridad, disponibilidad y confidencialidad
BAJA	Activos donde la integridad, disponibilidad y confidebcialidad es baja

Fuente: Elaboración propia

- **Ubicación**: Se refiere a la ubicación física o digital donde se encuentra almacenada la información, la Notaría Única de Dosquebradas cuenta con una sede física con 3 pisos, aquí se distribuyen los activos y procesos para la operación.

6.1 ACTIVOS POR PROCESO

La Notaría Única de la ciudad de Dosquebradas Cuenta con los procesos de Gerencia, sistemas, contabilidad, jurídica, autenticaciones, declaraciones, protocolo, recursos humanos, registro y rentas; estos procesos se encargan de tramitar los diferentes servicios notariales, cada uno de los procesos identificados genera y procesa un volumen considerable de información; a continuación, se detallan los activos con que cuenta cada proceso identificando su ubicación, clasificación y criticidad.

6.1.1 GERENCIA

La gerencia es el lugar estratégico de la Notaría, es el proceso donde se toman las decisiones administrativas; si bien, los lineamientos de los servicios a prestar son impartidos por el Superintendencia de Notariado y Registro, desde la gerencia se toman las decisiones que se trasladaran a las demás áreas misionales de la organización en procura de brindar un servicio ágil y confiable, está área cuenta con 2 funcionarios (Notario, Gerente) cada uno con su equipo de cómputo y una impresora. Los cambios operacionales de personal y en instalaciones físicas son realizados en esta área; los datos generados son de alta criticidad, en el cuadro 2 se identifican los activos que hacen parte de esta área donde los datos, las instalaciones físicas y la caja fuerte son de alta criticidad.

Cuadro 2. Activos identificados área de Gerencia

PROCESO		GERENCIA		
RESPONSABLE		CAROLINA MARIN		
ID	NOMBRE DE ACTIVO	UBICACIÓN	CLASIFICACIÓN	CRITICIDAD
1	Pc Escritorio Notario	1 PISO	Hardware	MEDIA
2	Pc Gerente	2 PISO	Hardware	MEDIA
3	Impresora epson L3110	2 PISO	Hardware	BAJA
4	Datos proceso	DIGITAL	Información	ALTA
5	Instalaciones fisicas	FISICA	Otros	ALTA
6	Caja fuerte	FISICA	Otros	ALTA

Fuente: Elaboración propia

6.1.2 SISTEMAS

Esta área se encarga de todos los activos tecnológicos de la organización, es el área de apoyo tecnológico de los demás procesos de la organización, encargada del óptimo desempeño de los equipos, su mantenimiento preventivo, correctivo y de la administración de los servidores de datos, firewall, video vigilancia, página

web, servidor de telefonía. Cuenta con un funcionario encargado de su gestión. En el cuadro 3 se identifican los activos de esta área su clasificación y criticidad, destacando las cámaras IP, el panel de la alarma, la Ups, el servidor de datos, el swicth de 48 puertos, el dvr, el servicio de internet, el firewall y los datos del proceso con alta criticidad.

Cuadro 3. Activos identificados área Sistemas

PROCESO		SISTEMAS		
RESPONSABLE		OCTAVIO PULGARIN		
ID	NOMBRE DE ACTIVO	UBICACIÓN	CLASIFICACIÓN	CRITICIDAD
7	Extensor Tenda Wiffi	1 PISO	Hardware	BAJA
8	Camaras Ip Dahua	UBICACIÓN	Hardware	ALTA
9	Panel de alarma Honewall	1 PISO	Hardware	ALTA
10	Sensores de Humo	UBICACIÓN	Hardware	MEDIA
11	UPS 10 KVA	2 PISO	Hardware	ALTA
12	Servidor datos	2 PISO	Hardware	ALTA
13	Swicth 48 puertos	2 PISO	Hardware	MEDIA
14	Swicth 24 puertos	2 PISO	Hardware	MEDIA
15	Dvr dahua	2 PISO	Hardware	ALTA
16	Servidor Telefonía	2 PISO	Hardware	MEDIA
17	UAP Tenda	2 PISO	Hardware	BAJA
18	Pc Sistemas	3 PISO	Hardware	MEDIA
19	Swicth 24 puertos	3 PISO	Hardware	MEDIA
20	Pagina web	DIGITAL	Software	MEDIA
21	Servicio Internet	DIGITAL	Servicio	ALTA
22	Firewall Pfsense	2 PISO	Hardware	ALTA
23	Datos proceso	DIGITAL	Información	ALTA

Fuente: Elaboración propia

6.1.3 CONTABILIDAD

El área contable se encarga de llevar todo lo concerniente al manejo del dinero, las cuentas por cobrar, cuentas por pagar, informes contables, pagos de nómina,

reportes de impuestos; esta dependencia cuenta con un profesional en el área contable como responsable del proceso, un auxiliar contable es el encargado de ingresar las diferentes facturas y genera los reportes correspondientes y dos auxiliares de caja son los encargados del recaudo de los cánones de escrituración, pago por autenticaciones y demás servicios que genera el ejercicio notarial; para la gestión el área se apoya en un software contable. En el cuadro 4 se identifican los activos de esta área su clasificación y criticidad, destacando las facturas físicas y digitales, los datos de los empleados y del proceso con una alta criticidad.

Cuadro 4. Activos identificados área de Contabilidad

PROCESO		CONTABILIDAD		
RESPONSABLE		CAROLINA ZAPATA		
ID	NOMBRE DE ACTIVO	UBICACIÓN	CLASIFICACIÓN	CRITICIDAD
24	Pc Escritorio Caja	1 PISO	Hardware	MEDIA
25	Pc Escritorio Caja 2	1 PISO	Hardware	MEDIA
26	Impresora Kyocera M3550	1 PISO	Hardware	BAJA
27	Impresora POS Epson	1 PISO	Hardware	BAJA
28	Pc Contabilidad	2 PISO	Hardware	MEDIA
29	Facturas Digitales-Fisicas	FISICA-DIGITAL	Información	ALTA
30	Datos empleados	DIGITAL	Información	ALTA
31	Software mekano	DIGITAL	Software	MEDIA
32	Datos proceso	DIGITAL	Información	ALTA

Fuente: Elaboración propia

6.1.4 JURÍDICA

El área jurídica de la notaría es la encargada de la revisión de todos los temas legales, es allí donde se verifican que todos los trámites cumplan con lo establecido en la normatividad colombiana y que las escrituras elaboradas lleguen a la oficina de registro sin errores, evitando devoluciones y retrasos en la entrega de las escrituras registradas a los clientes; igualmente, se encarga de resolver las

inquietudes jurídicas de los ciudadanos. Esta área cuenta como líder con un profesional en derecho y tres colaboradores igualmente capacitados. En el cuadro 5 se identifican los activos de esta área su clasificación y criticidad donde los datos del proceso son considerados de alta criticidad.

Cuadro 5. Activos identificados área Jurídica

PROCESO		JURIDICA		
RESPONSABLE		VALENTINA OSPINA		
ID	NOMBRE DE ACTIVO	UBICACIÓN	CLASIFICACIÓN	CRITICIDAD
33	Pc Escritorio Juridica	1 PISO	Hardware	MEDIA
34	Pc Registro Civil	2 PISO	Hardware	MEDIA
35	Impredora Hp	2 PISO	Hardware	BAJA
36	Pc Revision 1	3 PISO	Hardware	MEDIA
37	Pc Revision 2	3 PISO	Hardware	MEDIA
38	Pc Revision 3	3 PISO	Hardware	MEDIA
39	Lector biometrico huella	1 PISO	Hardware	BAJA
40	Software juridica	DIGITAL	Software	MEDIA
41	Software Index	DIGITAL	Software	MEDIA
42	Datos proceso	DIGITAL	Información	ALTA

Fuente: Elaboración propia

6.1.5 AUTENTICACIONES Y DECLARACIONES

La autenticaciones son los documentos donde el Notario da fe que las firmas que contienen los documentos son de los ciudadanos que acreditan ser, para esta revisión el notario se apoya en un equipo humano conformado por dos personas que reciben el documento y ellos a su vez se apoyan en un software biométrico para la lectura de su documento de identidad (cédula) y de sus huellas dactilares; igualmente, el responsable de esta área se encarga de la coordinación de los documentos privados (declaraciones, apostillas, certificados de tradición), para llevar a cabo esta labor cuenta con 5 colaboradores. En el cuadro 6 se identifican

los activos de esta área su clasificación y criticidad donde el software de identificación biométrica y los datos del proceso son considerados de alta criticidad.

Cuadro 6. Activos identificados área de Autenticaciones

PROCESO		AUTENTICACIONES		
RESPONSABLE		KARINA ESPINOZA		
ID	NOMBRE DE ACTIVO	UBICACIÓN	CLASIFICACIÓN	CRITICIDAD
43	Equipo Intel Nuc Aplicación turnero	1 PISO	Hardware	BAJA
44	Pc Escritorio autenticacion 1	1 PISO	Hardware	MEDIA
45	Pc Escritorio autenticacion 2	1 PISO	Hardware	MEDIA
46	Pc Declaraciones 1	2 PISO	Hardware	MEDIA
47	Pc Declaraciones 2	2 PISO	Hardware	MEDIA
48	Pc Declaraciones 3	2 PISO	Hardware	MEDIA
49	Televisores LG	1 PISO	Hardware	BAJA
50	Impresora Kyocera M3660	1 PISO	Hardware	BAJA
51	Impresora POS TCS	1 PISO	Hardware	BAJA
52	Impresora POS ZEBRA	1 PISO	Hardware	BAJA
53	Impresora epson l5120	1 PISO	Hardware	BAJA
54	Lector de Cédulas Motorola	1 PISO	Hardware	BAJA
55	Lector de Cédulas Honewall	2 PISO	Hardware	BAJA
56	Lector biometrico huella	1 PISO	Hardware	BAJA
57	Camara usb Microsoft	1 PISO	Hardware	BAJA
58	Software Identificate	DIGITAL	Software	ALTA
59	Datos proceso	DIGITAL	Información	ALTA

Fuente: Elaboración propia

6.1.6 PROTOCOLO Y RECURSOS HUMANOS

El área de protocolo es la encargada de la recepción de los documentos para posteriormente elaborar las escrituras públicas si todo está en regla, cuenta como recurso humano con 12 colaboradores que generan los documentos que posteriormente serán revisados por el área jurídica; por disposición del área gerencial, el líder de este proceso también se encarga de coordinar todo lo

concerniente al recurso humano, de llevar estadísticas y dar cumplimiento a lo establecido en la normatividad colombiana en cuanto a seguridad y salud en el trabajo de los colaboradores y visitantes. En el cuadro 7 se identifican los activos de esta área su clasificación y criticidad donde las escrituras, los datos personales de los usuarios, empleados y los datos del proceso son considerados de alta criticidad.

Cuadro 7. Activos identificados área de protocolo y recursos humanos

PROCESO		PROTOCOLO-RECURSOS HUMANOS		
RESPONSABLE		DANIELA VALENCIA		
ID	NOMBRE DE ACTIVO	UBICACIÓN	CLASIFICACIÓN	CRITICIDAD
60	Pc Escritorio Recepcion 2	1 PISO	Hardware	MEDIA
61	Pc Escritorio Recepcion 3	1 PISO	Hardware	MEDIA
62	Pc Escritorio Recepcion 4	1 PISO	Hardware	MEDIA
63	Pc Escritorio Recepcion 5	1 PISO	Hardware	MEDIA
64	Pc Recepcion 6	2 PISO	Hardware	MEDIA
65	Pc Cierre	2 PISO	Hardware	MEDIA
66	Pc Escrrituracion	2 PISO	Hardware	MEDIA
67	Pc Elaboracion 1	2 PISO	Hardware	MEDIA
68	Pc elaboración 2	2 PISO	Hardware	MEDIA
69	Impresora Kyocera m3660	2 PISO	Hardware	BAJA
70	Pc Elaboracion 3	3 PISO	Hardware	MEDIA
71	pc elaboracion 4	3 PISO	Hardware	MEDIA
72	Lector de Cédulas Honewall	2 PISO	Hardware	BAJA
73	Lector biometrico huella	2 PISO	Hardware	BAJA
74	Camara usb Microsoft	1 PISO	Hardware	BAJA
75	Escrituras en elaboración	FISICA-DIGITAL	Información	ALTA
76	Datos personales usuarios	FISICA-DIGITAL	Información	ALTA
77	Software protocolo	DIGITAL	Software	MEDIA
78	minutos celulares	DIGITAL	Servicio	BAJA
79	Software Identificate	DIGITAL	Software	ALTA
80	Software Tecnoturnos	DIGITAL	Software	MEDIA
81	Datos Sistema gestión	FISICA-DIGITAL	Información	ALTA
82	Datos proceso	DIGITAL	Información	ALTA

Fuente: Elaboración propia

6.1.7 REGISTRO Y RENTAS

Cuando las escrituras públicas son debidamente elaboradas y revisadas por el área jurídica, el área de registro y rentas es la encargada del envío y radicado de

estos documentos de forma digital y física en la oficina de registro e instrumentos públicos; igualmente, del pago de impuestos a la gobernación departamental y posterior entrega a los usuarios cuando la escritura pública ha sido registrada. Está área es coordinada por un profesional con experiencia en trámites de registro y 4 colaboradores. En el cuadro 8 se identifican los activos de esta área su clasificación y criticidad identificando las escrituras físicas y los datos del proceso como de alta criticidad.

Cuadro 8. Activos identificados área de Registro y Rentas

PROCESO		REGISTRO Y RENTAS		
RESPONSABLE		JULIANA GIRALDO		
ID	NOMBRE DE ACTIVO	UBICACIÓN	CLASIFICACIÓN	CRITICIDAD
83	Pc Escritorio Copias 1	1 PISO	Hardware	MEDIA
84	Pc Escritorio copias 2	1 PISO	Hardware	MEDIA
85	Impresora Ricoh Copias 1	1 PISO	Hardware	BAJA
86	Impresora Ricoh Copias 2	2 PISO	Hardware	BAJA
87	Pc Registro	2 PISO	Hardware	MEDIA
88	Pc Registro 2	2 PISO	Hardware	MEDIA
89	Impresora Kyocera m3660	1 PISO	Hardware	BAJA
90	Escrituras fisicas	FISICA	Información	ALTA
91	Software seguimiento escrituras	DIGITAL	Software	MEDIA
92	Datos proceso	DIGITAL	Información	ALTA

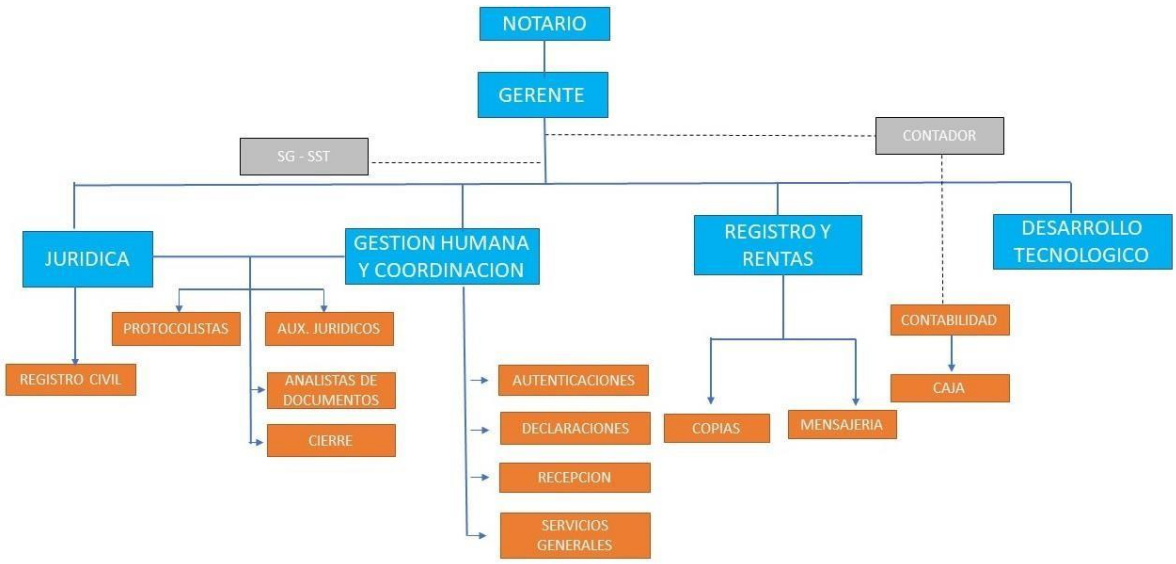
Fuente: Elaboración propia

El proceso de identificación de activos permitió identificar 92 activos en total en las instalaciones de la notaría Única de la ciudad de Dosquebradas, donde 24 son considerados con una alta criticidad, 43 con media y 25 con baja criticidad, esto permitirá tener un panorama global de los activos con que cuenta la organización.

7 DEFINIR EL ALCANCE DEL DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SEGÚN LOS PARÁMETROS DEL ESTÁNDAR ISO/IEC 27001:2013

La Notaria Única de la ciudad de Dosquebradas se dedica a la prestación de servicios notariales; entre estos se destacan, elaboración y autenticación de documentos privados, digitación de escrituras públicas, Declaraciones extrajuicio, asesorías jurídicas, registros civiles de nacimiento, matrimonio y defunción, entre otros servicios. En la figura 1 se muestra la distribución de los procesos internos en la organización, donde los ítems de color azul son los procesos principales coordinados por un líder de proceso, los de color naranja son los servicios operativos de atención al cliente y los de color gris son los procesos contratados externamente, todo este conjunto permite a la organización prestar un óptimo servicio con agilidad, buen servicio y confianza valores corporativos que se ven reflejados en la disponibilidad, integridad y confidencialidad de la información.

Figura 1. Organigrama Notaría Única Dosquebradas



Fuente: Elaboración propia

Cada proceso dentro de la notaría consulta, genera, procesa y recolecta información; a continuación, se detalla la información en formato físico y digital por proceso que hace parte del alcance del SGSI.

- **Gerencia**: Desde gerencia se consultan los diferentes informes de gestión de los procesos y se generan los respectivos informes de cumplimiento.
- **Sistemas**: Desde esta área se gestiona el buen funcionamiento y disponibilidad de los equipos de cómputo utilizados para la prestación de los servicios notariales.
- **Contabilidad**: El área contable recibe todas las facturas físicas y digitales generadas por las compras y los servicios prestados, igualmente cuenta con un software de gestión contable instalado en el servidor de datos donde se gestionan los datos de nómina y liquidaciones para la presentación de informes y hojas de vida de los empleados y proveedores.
- **Jurídica**: Esta área se encarga de consultar las escrituras públicas en formato digital y físico para dar el visto bueno de su cumplimento legal, los informes generados son almacenados en una ubicación lógica en el servidor de datos.
- **Autenticaciones y Declaraciones**: Desde estás área se realiza la toma de fotografías y huellas biométricas de los ciudadanos que comparecen ante el notario y se elaboran los diferentes documentos extra-proceso almacenados en formato digital en el servidor de datos.
- **Protocolo y Recursos Humanos**: En este proceso se elaboran las Escrituras públicas en formato digital y físico, cada protocolista tiene un equipo de cómputo con una carpeta digital en el servidor de datos ; en recursos humanos, se gestiona la información de los empleados y el cumplimento de los deberes legales en torno al Sistema de gestión de seguridad y salud en el trabajo, su información digital se almacena en el servidor de datos.

- **Registro y Rentas**: En este proceso se consultan las Escrituras en formato digital y físico que posteriormente se enviarán a la oficina de Registro e Instrumentos públicos, tiene a su cargo el área de copias donde se realiza el escaneo de los documentos físicos quedando un archivo en ubicación digital en el servidor de datos.

Toda la información digital generada en los procesos se almacena en el servidor local tipo rack Hp Proliant que cuenta dentro de sus características físicas con 24 Gb de memoria RAM y 8 TB de almacenamiento; mientras que la información física (Escrituras, registros civiles, facturas) se encuentran distribuidas en estanterías dentro de las instalaciones. El local donde se ubica la notaría cuenta con 3 pisos donde se ubican los servicios al público y administrativos de la siguiente manera:

- **Primer piso**: Servicios de autenticaciones, protocolo y jurídica.
- **Segundo Piso**: Área administrativa, recursos humanos, gerencia, declaraciones, registro civil, registro y cuarto donde se ubica el servidor de datos.
- **Tercer Piso**: Sistemas, protocolo.

Como entidad publico privada se debe garantizar el buen uso de los datos personales de los usuarios amparados bajo la ley estatutaria 1581 de 2012 y el decreto 1377 de 2013 donde la organización se compromete a proteger los datos de los usuarios, empleados y proveedores[22] haciendo parte del SGSI toda la información física y digital que se gestione en la organización a partir de los anteriores lineamientos.

[22] NOTARÍA DOSQUEBRADAS, Política de tratamiento de datos. [Sitio Web]. Dosquebradas. [Consulta: 10 de abril de 2023]. Disponible en: https://notariaprimeradosquebradas.co/?botonTransparencia&politicaDatosPersonales

El diseño del SGSI tendrá en cuenta todos los activos identificados donde su nivel de criticidad se encuentre entre Alta y Media (incluidos empleados directos e indirectos que tengan acceso a los sistemas que gestionan la información); A estos activos, se les identificará sus vulnerabilidades, sus riesgos y el impacto entre leve, medio o severo; aplicando los respectivos controles que indique el anexo A del estándar ISO/IEC 27001:2013; se excluyen del Alcance del diseño del SGSI, las tomas biométricas realizadas en el proceso de autenticaciones y la información digital almacenada en los equipos de cómputo de los empleados.

8 IDENTIFICAR LAS VULNERABILIDADES PARA LOS ACTIVOS DE LA NOTARÍA ÚNICA DE LA CIUDAD DE DOSQUEBRADAS (RISARALDA)

Teniendo como base la identificación de los activos de la Notaría única de la ciudad de Dosquebradas, uno de los pasos que para el estándar ISO/IEC 27001:2013 es de vital importancia, es la identificación del riesgo que pueden afectar la integridad, disponibilidad y confidencialidad de la información.

Partiendo de la valoración de criticidad previamente realizada sobre los activos identificados, donde fueron valorados entre alta, media y baja según su afectación a dos o más características que debe mantener la información; siendo alta y media la valoración que se considera para la organización como activos importantes para la gestión de información y sobre los que se realiza la identificación de vulnerabilidades. Para determinar las debilidades de seguridad, se definió cada activo dentro de una categoría que ayudó a identificarlos de una forma más general. En la tabla 1 se define las categorías: Software de terceros, información digital, computadores de escritorio, libros físicos, instalaciones físicas, vigilancia, control de voltaje, servidor de datos, servicio de red, página web. asociando estas al proceso y al Identificador del activo (ID) al que pertenecen.

Tabla 1. Activos valorados entre criticidad alta y media

Proceso	Id activo	categoría
GERENCIA	4	Información digital.
	5	Instalaciones.
	6	Activo físico.
	1-2	Computadores de escritorio.

Proceso	Id activo	categoría
SISTEMAS	8-9-10-15	Vigilancia.
	11	Control de voltaje.
	12	Servidores.
	21	Servicios.
	13-14-19-22	Red de datos.
	23	Información digital.
	16	Telefonía IP.
	18	Computadores de escritorio.
	20	Página Web.
CONTABILIDAD	29	Libros.
	30-32	Información digital.
	24-25-26	Computadores de escritorio.
	31	Software de terceros.
JURIDICA	42	Información digital.
	33-34-36-37-38	Computadores de escritorio.
	40	Software de terceros.
	41	Software de terceros.
AUTENTICACIONES	58	Software de terceros.
	59	Información digital.
	44-45-46-47-48	Computadores de escritorio.
PROTOCOLO-RECURSOS HUMANOS	75	Información digital.
	76	Información digital.
	79	Software de terceros.
	81	Información digital.
	82	Información digital.
	60-61-62-63-64-65-66-67-68-70-71	Computadores de escritorio.
	79-80	Software de terceros.

Proceso	Id activo	categoría
REGISTRO Y RENTAS	90	Libros físicos.
	92	Información digital.
	83-84-85-86	Computadores de escritorio.
	91	Software de terceros.

Fuente: Elaboración Propia

Teniendo definido los activos por categorías y agrupando los Identificadores (Id activo) se consultan en diferentes repositorios alojados en la web las debilidades que sobre estas categorías se han identificado. Dentro de los repositorios consultados se encuentran los CVE (Common Vulnerabilites and Exposure) y CWE (Common Weakness Enumeration), donde se encuentra un listado estandarizado de las vulnerabilidades que pueden afectar la seguridad de los activos de información. En la tabla 2 se realiza la descripción de las debilidades que pueden afectar las categorías identificadas incluyendo los colaboradores de la organización.

Tabla 2. Identificación de Vulnerabilidades por categoría

Categoría	Vulnerabilidad
Software de terceros	CWE-89 Neutralización incorrecta de elementos especiales utilizados en un comando SQL ('inyección SQL').
	CEW-79 Neutralización incorrecta de la entrada durante la generación de la página web ("Cross-site Scripting").
	CWE-352 Falsificación de solicitud entre sitios (CSRF).
	CWE-78 Neutralización incorrecta de elementos especiales utilizados en un comando de sistema operativo ('inyección de comando de sistema operativo').
	CWE-798 Uso de Credenciales Codificadas.
	CWE-502 Deserialización de datos no confiables.
	CWE-269 Gestión de privilegios inadecuada.
	CWE-400 Consumo de recursos no controlado.
	CWE-306 Autenticación faltante para función crítica.
	CWE-862 Autorización faltante.

Categoría	Vulnerabilidad
Red de datos - Telefonía IP	Ataque de denegación de servicio.
	Ataque denegación de servicio distribuido.
	Escaneo de puertos.
	Secuencia TCP.
	Redireccionamiento ICMP.
	Transferencia de zona DNS.
	Envenenamiento de caché DNS.
	IP Spoofing.
	Ataque Man-In-The-Middle.
Servidor	Lugar de ubicación de fácil acceso por terceros.
	CVE-2019-0536 Vulnerabilidad de divulgación de información del kernel de Windows.
	CVE-2018-8611 vulnerabilidad de elevación de privilegios del kernel de Windows.
	CVE-2018-8622-CVE-2018-8639 vulnerabilidad de divulgación de información del kernel de Windows.
	CVE-2018-8450 ejecución remota de código cuando Windows Search.
	CVE-2018-8423- CVE-2019-0584 ejecución remota de código en el motor de base de datos de Microsoft.
	CVE-2018-8626 ejecución remota de código en los servidores del Sistema de nombres de dominio.
	Inexistencia de frecuencia de ejecución de actualizaciones.
Computadores de escritorio	CVE-2021-43211-CVE-2021-42297-CVE-2021-36945 elevación de privilegios del asistente de actualización de Windows 10.
	CVE-2022-21882 Vulnerabilidad de elevación de privilegios de Win32k.
	CVE-2021-40469 Vulnerabilidad de ejecución remota de código del servidor DNS de Windows.
	CVE-2021-41338 Vulnerabilidad de omisión de la función de seguridad de las reglas de firewall de Windows AppContainer.
	Amenazas naturales.
	Ingreso de Pendrive externas sin control.

Categoría	Vulnerabilidad
Información digital	Copia no controlada de datos.
	Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.
	Respaldo inapropiado o irregular.
	Clasificación inadecuada de la información.
	Eliminación de medios de almacenamiento sin eliminar datos.
Usuarios	Falta de formación y conciencia sobre seguridad.
Libros físicos	Agua.
	Fuego.
	Amenazas naturales.
	Humedad.
	Mala o inexistente rotulación y almacenado.
	Robo o vandalismo.
	Plagas.
	Temperatura.
Instalaciones	Amenazas naturales.
	Robo.
	Vandalismo.
	Clima laboral.
Control de voltaje	Falla por baterías.
	Falla por Temperatura.
	ventilación o temperatura ambiente no controlada.
	sobrecarga de Ups.
	Falla de ventiladores por fin de ciclo de vida o nulo mantenimiento (limpieza).
	Mala instalación eléctrica.
	Deficiencias en el mantenimiento.
Vigilancia	Fallo por conexión con central de vigilancia.
	Frecuencia de verificación de estado de equipos.

Categoría	Vulnerabilidad
Página Web	Redirección a sitios maliciosos.
	Recopilación de datos.
	Ataques a la base de datos.
	Autenticación fraudulenta.
	Ataque de denegación de servicio.
	Cross-site scripting o Secuencias de comando entre sitios (XSS).

Fuente: Elaboración Propia

Cada una de las vulnerabilidades identificadas permitió valorar el riesgo al que se encuentran expuestos los activos de la organización; para ello, se evaluó el impacto y la probabilidad de ocurrencia (valoración cualitativa). Con esta valoración a través de una matriz de riesgo se identificaron los riesgos a los que se encuentran expuestos los activos de la organización (valoración cuantitativa). En el cuadro 9 se observa la categoría, descripción y puntuación, definidas para evaluar la probabilidad e impacto del riesgo.

Cuadro 9. Ejes de evaluación del riesgo

PROBABILIDAD		
CATEGORÍA	DESCRIPCIÓN	PUNTUACIÓN
BAJA	Muy poco probable que ocurra	1
MEDIA	probablemente puede ocurrir	2
ALTA	probabiliadad alta de que ocurra	3

IMPACTO		
CATEGORÍA	DESCRIPCIÓN	PUNTUACIÓN
LEVE	Impacto con baja severidad	1
MEDIO	Perdida momentanea de la operación	2
SEVERO	Perdida de la prestación del servicio	3

Fuente: Elaboración propia

Definidos los parámetros para hallar la probabilidad e impacto se llevo a cabo la valoración cuantitativa de las vulnerabilidades. En la tabla 3 se muestra la valoración de la probabilidad e impacto para cada una de las vulnerabilidades antes identificadas.

Tabla 3. Valoración cualitativa de la probabilidad e impacto de las vulnerabilidades identificadas

Categoría	Vulnerabilidad	Probabilidad	Impacto
Software de terceros	CWE-89 Neutralización incorrecta de elementos especiales utilizados en un comando SQL ('inyección SQL').	Media	Medio
	CEW-79 Neutralización incorrecta de la entrada durante la generación de la página web ("Cross-site Scripting").	Media	Medio
	CWE-352 Falsificación de solicitud entre sitios (CSRF).	Alta	Severo
	CWE-78 Neutralización incorrecta de elementos especiales utilizados en un comando de sistema operativo ('inyección de comando de sistema operativo').	Baja	Medio
	CWE-798 Uso de Credenciales Codificadas.	Alta	Severo
	CWE-502 Deserialización de datos no confiables.	Alta	Severo
	CWE-269 Gestión de privilegios inadecuada.	Alta	Severo
	CWE-400 Consumo de recursos no controlado.	Alta	Severo
	CWE-306 Autenticación faltante para función crítica.	Media	Severo
	CWE-862 Autorización faltante.	Media	Medio

Categoría	Vulnerabilidad	Probabilidad	Impacto
Red de datos - Telefonía IP	Ataque de denegación de servicio.	alta	Severo
	Ataque denegación de servicio distribuido.	Media	Severo
	Escaneo de puertos.	Alta	Leve
	Secuencia TCP.	Media	Medio
	Redireccionamiento ICMP.	Media	Severo
	Transferencia de zona DNS.	Media	Severo
	Envenenamiento de caché DNS.	Alta	Leve
	IP Spoofing.	Alta	Severo
	Ataque Man-In-The-Middle.	Media	Severo
Servidor	Lugar de ubicación de fácil acceso por terceros.	Alta	Severo
	CVE-2019-0536 Vulnerabilidad de divulgación de información del kernel de Windows.	baja	Medio
	CVE-2018-8611 vulnerabilidad de elevación de privilegios del kernel de Windows.	baja	Severo
	CVE-2018-8622-CVE-2018-8639 vulnerabilidad de divulgación de información del kernel de Windows.	baja	Severo
	CVE-2018-8450 ejecución remota de código cuando Windows Search.	baja	Severo
	CVE-2018-8423- CVE-2019-0584 ejecución remota de código en el motor de base de datos de Microsoft.	baja	Medio
	CVE-2018-8626 ejecución remota de código en los servidores del Sistema de nombres de dominio.	baja	Medio
	Inexistencia de frecuencia de ejecución de actualizaciones.	Alta	Leve

Categoría	Vulnerabilidad	Probabilidad	Impacto
Computadores de escritorio	CVE-2021-43211-CVE-2021-42297-CVE-2021-36945 elevación de privilegios del asistente de actualización de Windows 10.	Media	Severo
	CVE-2022-21882 Vulnerabilidad de elevación de privilegios de Win32k.	Media	Severo
	CVE-2021-40469 Vulnerabilidad de ejecución remota de código del servidor DNS de Windows.	Baja	Severo
	CVE-2021-41338 Vulnerabilidad de omisión de la función de seguridad de las reglas de firewall de Windows AppContainer.	Baja	Medio
	Amenazas naturales.	Alta	Severo
	Ingreso de Pendrive externas sin control.	Alta	Severo
Información digital	Copia no controlada de datos.	Alta	Severo
	Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.	Alta	Medio
	Respaldo inapropiado o irregular.	Alta	Severo
	Clasificación inadecuada de la información.	Alta	Leve
	Eliminación de medios de almacenamiento sin eliminar datos.	Media	Leve
Usuarios	Falta de formación y conciencia sobre seguridad.	Alta	Severo

Categoría	Vulnerabilidad	Probabilidad	Impacto
Libros físicos	Agua.	Media	Severo
	Fuego.	Alta	Severo
	Amenazas naturales.	Alta	Severo
	Humedad.	Alta	Medio
	Mala o inexistente rotulación y almacenado.	Alta	Medio
	Robo o vandalismo.	Alta	Severo
	Plagas.	Alta	Severo
	Temperatura.	Baja	Leve
Instalaciones	Amenazas naturales.	Alta	Severo
	Robo.	Alta	Severo
	Vandalismo.	Alta	Severo
	Clima laboral.	Baja	Medio
Control de voltaje	Falla por baterías.	Alta	Severo
	Falla por Temperatura.	Baja	Severo
	ventilación o temperatura ambiente no controlada.	Alta	Severo
	sobrecarga de Ups.	Media	Severo
	Falla de ventiladores por fin de ciclo de vida o nulo mantenimiento (limpieza).	Alta	Severo
	Mala instalación eléctrica.	Baja	Medio
	Deficiencias en el mantenimiento.	Baja	Severo
Vigilancia	Fallo por conexión con central de vigilancia.	Alta	Medio
	Frecuencia de verificación de estado de equipos.	Media	Leve

Fuente: Elaboración Propia

Con la valoración cualitativa donde se le dio a cada vulnerabilidad un valor de probabilidad e impacto del riesgo se llevó a cabo a través de una matriz de riesgo de 3 x 3 la valoración cuantitativa. En el cuadro 10 se muestran los resultados de esta valoración, donde se destacan 23 vulnerabilidades que cuentan con una probabilidad alta de ocurrencia y un impacto severo, 9 vulnerabilidades con una probabilidad media y un impacto severo y 4 vulnerabilidades con una probabilidad alta y un impacto medio.

Cuadro 10. Matriz de riesgos

			IMPACTO		
			LEVE	MEDIO	SEVERO
			1	2	3
PROBABILIDAD	BAJA	1	1	7	6
	MEDIA	2	2	4	9
	ALTA	3	4	4	23

Fuente: Elaboración Propia

El anterior análisis de riesgos permitió generar una serie de controles que brindarán a la información gestionada en la notaría Única de la ciudad de Dosquebradas y sus activos un manejo adecuado, seguro y confiable.

9 PROPONER EL DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS LINEAMIENTOS EL ESTÁNDAR ISO/IEC 27001:2013

9.1 INTRODUCCIÓN

Las políticas de seguridad de la información permiten a las organizaciones la mejora continua en la protección de la información, estas son el punto de partida en el conocimiento del parte tecnológico, sus debilidades y posibles tratamientos, ayudando a las empresas a llevar un manejo adecuado de los incidentes que se pueden presentar.

Para la notaría Única de la ciudad de Dosquebradas se proponen las políticas de seguridad a partir de los dominios del estándar ISO/IEC 27001:2013 en su anexo A donde los dominios sugeridos según el análisis de vulnerabilidades se identifican el en cuadro 9 donde se identifica su código y el nombre de dominio.

Cuadro 11. Dominios sugeridos estándar ISO 27001 anexo A

ID	DOMINIO
A7	Seguridad de los recursos humanos
A8	Gestión de activos
A9	Control de acceso
A11	Seguridad física y del entorno
A12	Seguridad de las operaciones
A13	Seguridad de las comunicaciones

Fuente: Elaboración propia

9.2 OBJETIVO

Proponer a la alta dirección de la Notaria única de la ciudad de Dosquebradas el diseño de las políticas de seguridad de la información para que sean contempladas dentro de sus procesos internos.

9.3 ALCANCE

El alcance de las políticas de seguridad de la información para la Notaría única de Dosquebradas abarca los procesos de Autenticaciones, Registro y rentas, Protocolo, Recursos Humanos, contabilidad, gerencia, sistema y el área jurídica incluyendo el personal contratado y los que hagan uso autorizado de los equipos tecnológicos que gestionan la información de la entidad.

9.4 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

Para la seguridad de los recursos humanos se proponen los controles del anexo A en su numeral A.7 del estándar ISO/IEC 27001:2013; en el cuadro 10, se detalla el numeral correspondiente, la categoría a la que pertenece el activo, los identificadores del activo y el control que se debe tener en cuenta para mantener la seguridad de la información.

Cuadro 12. Numeral A.7 anexo A estándar ISO/IEC 27001:2013

DOMINIO		Seguridad relativa a los recursos humanos		
OBJETIVO		Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en		
Numeral	**Descripción**	**Categoría**	**Activos**	**Control**
A.7.2.1	Responsabilidades de gestión	Usuarios	Todos los empleados directos e indirectos de la organización	La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Usuarios	Todos los empleados directos e indirectos de la organización	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A.7.2.3	Proceso disciplinario	Usuarios	Todos los empleados directos e indirectos de la organización	Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.
A.7.3.1	Responsabilidades ante la finalización o cambio	Usuarios	Todos los empleados directos e indirectos de la organización	Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.

Fuente: Elaboración propia

9.5 POLÍTICA DE GESTIÓN DE ACTIVOS

La política de gestión de activos en una organización permite mantener el control sobre estos, conocer su estado, quien es su responsable, su ubicación dentro de las instalaciones, de la misma manera esta política clasifica de manera adecuada la información (numeral A.8.2) y el adecuado manejo de medios de almacenamiento de la información evitando su pérdida o destrucción (numeral A.8.3). Se proponen las pautas del numeral A.8 del estándar ISO/IEC 27001:2013; en el cuadro 11, se detalla el numeral correspondiente, la categoría a la que pertenece el activo, los identificadores del activo y el control que se debe tener en cuenta para mantener la seguridad de la información.

Cuadro 13. Numeral A.8 anexo A estándar ISO/IEC 27001:2013

DOMINIO		Gestión de activos		
OBJETIVO		Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
Numeral	**Descripción**	**Categoría**	**Activos**	**Control**
A.8.1.1	Inventario de activos	Computadores de escritorio Información Digital Servidor	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
A.8.1.2	Propiedad de los activos	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	Todos los activos que figuran en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
A.8.1.4	Devolución de activos	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
A.8.2.1	Clasificación de la información	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
A.8.2.2	Etiquetado de la información	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

A.8.2.3	Manipulado de la información	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.1	Gestión de soportes extraíbles	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de soportes	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
A.8.3.3	Soportes físicos en tránsito	Computadores de escritorio Información Digital Servidor Libros Fisicos	4-1-2-12-18-23-24-25-26-29-30-32-33-34-35-36-37-38-42-44-25-46-47-48-59-60-61-62-63-64-65-66-67-68-69-70-71-75-76-81-82-86-84-85-86-92	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

Fuente: Elaboración propia

9.6 POLÍTICA DE CONTROL DE ACCESO

El control de acceso permite definir que o quienes tienen acceso a los recursos digitales y físicos de la organización incluye las redes de datos, el control de usuarios, los privilegios que se otorgan, las restricciones, las responsabilidades de los usuarios frente al manejo de la información y controlar el acceso a los sistemas propios y de terceros con que cuenta la notaría. Se proponen las pautas del numeral A.9 del estándar ISO/IEC 27001:2013; en el cuadro 12, se detalla el numeral correspondiente, la categoría a la que pertenece el activo, los

identificadores del activo y el control que se debe tener en cuenta para mantener la seguridad de la información.

Cuadro 14. Numeral A.9 anexo A estándar ISO/IEC 27001:2013

DOMINIO		Control de acceso		
OBJETIVO		Limitar el acceso a los recursos de tratamiento de la información y a la información.		
Numeral	**Descripción**	**Categoría**	**ID Activos**	**Control**
A.9.1.2	Acceso a las redes y a los servicios de red	Redes de datos Telefonía IP	13-14-16-19-22	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
A.9.2.1	Registro y baja de usuario	Usuarios	Todos los empleados directos e indirectos de la organización	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
A.9.2.2	Provisión de acceso de usuario	Usuarios	Todos los empleados directos e indirectos de la organización	Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A.9.2.3	Gestión de privilegios de acceso	Usuarios	Todos los empleados directos e indirectos de la organización	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Usuarios Información Digital	Todos los empleados directos e indirectos de la organización-4-23-30-32-42-59-75-76-81-82-92	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
A.9.2.5	Revisión de los derechos de acceso de usuario	Usuarios	Todos los empleados directos e indirectos de la organización	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Retirada o reasignación de los derechos de acceso	Usuarios Información Digital	Todos los empleados directos e indirectos de la organización-4-23-30-32-42-59-75-76-81-82-92	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
A.9.3.1	Uso de la información secreta de autenticación	Usuarios Información Digital	Todos los empleados directos e indirectos de la organización-4-23-30-32-42-59-75-76-81-82-92	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A.9.4.1	Restricción del acceso a la información	Usuarios Información Digital	Todos los empleados directos e indirectos de la organización-4-23-30-32-42-59-75-76-81-82-92	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A.9.4.2	Procedimientos seguros de inicio de sesión	Software de Terceros	31-40-41-58-79-80-91	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
A.9.4.3	Sistema de gestión de contraseñas	Usuarios Información Digital	Todos los empleados directos e indirectos de la organización	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A.9.4.5	Control de acceso al código fuente de los programas	Software de Terceros	31-40-41-58-79-80-91	Se debe restringir el acceso al código fuente de los programas.

Fuente: Elaboración propia

9.6.1 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física es de vital importancia para las organizaciones en especial para las que realizan atención al público ya que en sus instalaciones se desplazan constantemente personas que pueden de manera indirecta participar en la seguridad de la información; la adopción de una política que mejoren la seguridad de entornos donde se procesa la información ayuda a salvaguardarla; se proponen las pautas del numeral A.11 del estándar ISO/IEC 27001:2013; en el cuadro 13, se detalla el numeral correspondiente, la categoría a la que pertenece el activo, los identificadores del activo y el control que se debe tener en cuenta para mantener la seguridad de la información.

Cuadro 15. Numeral A.11 anexo A estándar ISO/IEC 27001:2013

DOMINIO		Seguridad física y del entorno		
OBJETIVO		Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la		
Numeral	**Descripción**	**Categoría**	**ID Activos**	**Control**
A.11.1.1	Perímetro de seguridad física	Instalaciones Vigilancia	5-8-9-10-15	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.
A.11.1.3	Seguridad de oficinas, despachos y recursos	Instalaciones Vigilancia	5-8-9-10-15	Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
A.11.1.4	Protección contra las amenazas externas y ambientales	Instalaciones Vigilancia	5-8-9-10-15	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
A.11.2.1	Emplazamiento y protección de equipos	Computadores de escritorio Servidor	1-2-12-18-24-25-26-29-33-34-35-36-37-38-44-25-46-47-48-60-61-62-63-64-65-66-67-68-69-70-71-86-84-85-86	Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.
A.11.2.2	Instalaciones de suministro	Control Voltaje	11	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
A.11.2.3	Seguridad del cableado	Redes de datos Telefonía IP	13-14-16-19-22	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A.11.2.4	Mantenimiento de los equipos	Computadores de escritorio Servidor	1-2-12-18-24-25-26-29-33-34-35-36-37-38-44-25-46-47-48-60-61-62-63-64-65-66-67-68-69-70-71-86-84-85-86	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

A.11.2.5	Retirada de materiales propiedad de la empresa	Computadores de escritorio Servidor	1-2-12-18-24-25-26-29-33-34-35-36-37-38-44-25-46-47-48-60-61-62-63-64-65-66-67-68-69-70-71-86-84-85-86	Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Computadores Escritorio	1-2-18-24-25-26-29-33-34-35-36-37-38-44-25-46-47-48-60-61-62-63-64-65-66-67-68-69-70-71-86-84-85-86	Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.
A.11.2.7	Reutilización o eliminación segura de equipos	Computadores de escritorio Servidor Redes de datos Telefonía IP	13-14-16-19-22	Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.
A.11.2.8	Equipo de usuario desatendido	Usuarios	Todos los empleados directos e indirectos de la organización	Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Usuarios	Todos los empleados directos e indirectos de la organización	Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

Fuente: Elaboración propia

9.7 POLÍTICA DE LA SEGURIDAD DE LAS OPERACIONES

La seguridad de las operaciones permite al área técnica de la notaría y a sus responsables conocer los controles que debe tener para la configuración y procedimientos de uso de los equipos que gestionan la información, se proponen las pautas del numeral A.12 del estándar ISO/IEC 27001:2013; en el cuadro 14, se detalla el numeral correspondiente, la categoría a la que pertenece el activo, los identificadores del activo y el control que se debe tener en cuenta para mantener la seguridad de la información.

Cuadro 16. Numeral A.12 anexo A estándar ISO/IEC 27001:2013

DOMINIO		Seguridad de las operaciones		
OBJETIVO		Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.		
Numeral	**Descripción**	**Categoría**	**ID Activos**	**Control**
A.12.1.1	Documentación de procedimientos operacionales	Todos los activos	Todos los activos o procesos incluidos en el alcance del Diseño del SGSI	Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.
A.12.2.1	Controles contra el código malicioso	Computadores de escritorio Servidor Página web	1-2-18-20-24-25-26-29-33-34-35-36-37-38-44-25-46-47-48-60-61-62-63-64-65-66-67-68-69-70-71-86-84-85-86	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
A.12.3.1	Copias de seguridad de la información	Información Digital	4-23-30-32-42-59-75-76-81-82-92	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
A.12.5.1	Instalación del software en explotación	Computadores de escritorio Servidor	1-2-12-18-24-25-26-29-33-34-35-36-37-38-44-25-46-47-48-60-61-62-63-64-65-66-67-68-69-70-71-86-84-85-86	Se deben implementar procedimientos para controlar la instalación del software en explotación.
A.12.6.1	Gestión de las vulnerabilidades técnicas	Computadores de escritorio Servidor	1-2-12-18-24-25-26-29-33-34-35-36-37-38-44-25-46-47-48-60-61-62-63-64-65-66-67-68-69-70-71-86-84-85-86	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
A.12.6.2	Restricción en la instalación de software	Computadores de escritorio Servidor	1-2-12-18-24-25-26-29-33-34-35-36-37-38-44-25-46-47-48-60-61-62-63-64-65-66-67-68-69-70-71-86-84-85-86	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.

Fuente: Elaboración propia

9.8 POLÍTICA DE LA SEGURIDAD DE LAS COMUNICACIONES

La seguridad de las comunicaciones permite tener los controles necesarios para la gestión, la seguridad y la segmentación de las redes, estos permitirán el manejo adecuado y seguro de la información, se proponen las pautas del numeral A.13 del estándar ISO/IEC 27001:2013, en el cuadro 15 se detalla el numeral correspondiente, la categoría a la que pertenece el activo, los identificadores del activo y el control que se debe tener en cuenta para mantener la seguridad de la información.

Cuadro 17. Numeral A.13 anexo A estándar ISO/IEC 27001:2013

DOMINIO		Seguridad de las comunicaciones		
OBJETIVO		Asegurar la protección de la información en las redes y los recursos de tratamiento de la		
Numeral	**Descripción**	**Categoría**	**ID Activos**	**Control**
A.13.1.1	Controles de red	Redes de datos Telefonía IP	13-14-16-19-22	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Redes de datos Telefonía IP	13-14-16-19-22	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
A.13.1.3	Segregación en redes	Redes de datos Telefonía IP	13-14-16-19-22	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.

Fuente: Elaboración propia

Los controles sugeridos por el anexo A del estándar ISO/IEC 27001:2013 permitirán a la notaría Única de la ciudad de Dosquebradas contar con un SGSI en su fase inicial adecuado para el manejo seguro de la información siendo la puerta de entrada de una cultura organizacional en torno a los procesos seguros donde se minimicen las debilidades que puede tener la infraestructura tecnológica de la organización.

10 CONCLUSIONES

- La identificación de los activos permitió a la notaría única de la ciudad de Dosquebradas tener un panorama de los recursos que gestionan la información en sus diferentes procesos; conocer su ubicación, su clasificación y criticidad ayudaron a la organización a conocer sus debilidades y riesgos, el diseño del SGSI facilitó la creación de políticas y controles para el manejo seguro de la información dentro de sus procesos ayudando a mejorar la seguridad de la información que se gestiona; igualmente, darle un identificador a cada recurso ayudó a unirlo a un control del anexo A del estándar ISO/IEC 27001:2013 ayudando a llevar una mejor trazabilidad en el proceso.

- El alcance permitió definir 67 activos ubicados dentro de las instalaciones físicas de la notaría Única de la ciudad de Dosquebradas que comprometen como mínimo dos de los tres atributos que debe tener la información para que su tratamiento sea seguro; esto quiere decir que, el 72.83 % de los activos fueron objeto de búsqueda de vulnerabilidades, permitiendo de esta manera en el diseño del SGSI cubrir un alto número de activos que dará a los usuarios internos y externos la tranquilidad del manejo de buenas prácticas en el uso de la información.

- Agrupar los activos identificados por categorías permitió de una manera más sencilla hallar las vulnerabilidades que pueden afectar la seguridad de la información, apoyando esta búsqueda en repositorios como el CVE y CWE que son fuentes internacionales donde se agrupan las debilidades encontradas en el uso de software; Las debilidades identificadas, permitieron darle más estructura al diseño del SGSI identificando de una manera más idónea las políticas y controles a utilizar.

- El diseño de las políticas permitió identificar de manera adecuada los controles que sobre los activos se deben implementar, adoptarlos beneficiará la seguridad de la información que se gestione en la organización; estos controles ligados a los identificadores y la categoría permitirán ser más específicos, ayudando al área TI a dar un mejor seguimiento y alinear los procesos internos en procura de brindar mejor seguridad a la información.

11 RECOMENDACIONES

Con la finalización de esta etapa del diseño del SGSI para la notaría Única de Dosquebradas se hace pertinente realizar las siguientes recomendaciones:

- Si bien el diseño realizado del SGSI permitió detectar las vulnerabilidades que tienen los activos y generar controles para salvaguardar su seguridad es muy importante generar una frecuencia de revisión del presente diseño, de este modo se pueden actualizar los activos, su categoría, sus debilidades y las políticas de tratamiento, este proceso se sugiere debe estar acompañado de una persona responsable designado por la alta gerencia y el compromiso de todo el recurso humano de la organización.

- En el proceso realizado se detectaron vulnerabilidades que afectan 2 de las 3 características de la seguridad de la información; es importante para futuros análisis, generar estrategias de tratamiento de los riesgos sobre los activos; para ello, el estándar ISO 31000 que trata en profundidad el manejo adecuado del riesgo ayudarían a reforzar los controles aplicados en la organización.

- La gerencia determinará la persona o personas encargadas de la actualización y si corresponde continuar con las fases siguientes del SGSI, es importante crear un comité que se encargue del uso y adecuación de las políticas de seguridad de la información, su actualización y mejores prácticas en el uso de la información física y digital.

- Incluir en el presupuesto anual una partida económica que permita el fortalecimiento de la seguridad de la información; si bien este proceso permitió definir las políticas de seguridad de información, es de vital

importancia contar con el recurso económico que lo mantenga en el tiempo y cumplan su objetivo.

BIBLIOGRAFÍA

¿CÓMO DISEÑAR UNA MATRIZ DE RIESGOS? [Sitio Web]. [Consulta: 4 de abril de 2023]. Disponible en: https://blogs.portafolio.co/buenas-practicas-de-auditoria-y-control-interno-en-las-organizaciones/disenar-una-matriz-riesgos/

4 CONSEJOS PARA CREAR UNA MATRIZ DE RIESGOS. [Sitio Web]. [Consulta: 4 de abril de 2023]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2018/10/4-consejos-para-crear-una-matriz-de-riesgos/

BANCO SANTANDER, ¿Qué es una vulnerabilidad informática? [Sitio Web]. [Consulta: 18 de marzo de 2022]. Disponible en:
BIBLIOTECA NACIONAL DE COLOMBIA, Gestión de riesgos. [Sitio Web]. [Consulta: 17 de octubre de 2022]. Disponible en:

https://bibliotecanacional.gov.co/es-co/servicios/profesionales-del-libro/conservacion-de-colecciones/gestion-de-riesgos

CIBERSEGURIDAD, Explicación de las vulnerabilidades y exposiciones comunes. [Sitio Web]. [Consulta: 21 de octubre de 2022]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

CMX ELECTRIC, UPS tripplite smart2200vs. [Sitio Web]. [Consulta: 19 de octubre de 2022]. Disponible en: https://tripplitesmart2200vs.blogspot.com/2018/07/principales-fallas-en-equipos-ups.html

CÓMO EVALUAR LAS CONSECUENCIAS Y LA PROBABILIDAD EN EL ANÁLISIS DE RIESGOS ISO 27001. [Sitio Web]. [Consulta: 4 de abril de 2023]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2019/03/como- evaluar-las-consecuencias-y-la-probabilidad-en-el-analisis-de-riesgos-iso-27001/

CONEXIÓN ESAN, Las cuatro etapas para la mejora continua en la organización. [Sitio Web]. Monterico. [Consulta: 17 de marzo de 2022]. Disponible en: https://www.esan.edu.pe/conexion-esan/las-cuatro-etapas-para-la-mejora-continua-en-la-organizacion#:~:text=El%20nombre%20del%20ciclo%20PDCA,etapas%20en%20el%20siguiente%20art%C3%ADculo.

CVE, Common Weakness Enumeration. [Sitio Web]. [Consulta: 18 de octubre de 2022]. Disponible en: https://cwe.mitre.org/

CVE, Vulnerabilidades Windows server 2012. [Sitio Web]. [Consulta: 14 de

septiembre de 2022]. Disponible en: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=windows+server+2012+r2

CWE, Vulnerabilidades Windows server 2012. [Sitio Web]. [Consulta: 14 de septiembre de 2022]. Disponible en:

ESCUELA EUROPEA DE EXCELENCIA, Listado de amenazas y vulnerabilidades en ISO 27001. [Sitio Web]. [Consulta: 15 de septiembre de 2022]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/

FIRMA-E. ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? [Sitio Web]. Mursia. [Consulta: 17 de marzo de 2022]. Disponible en: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

GLOBAL SUITE, ¿Cuál es el objetivo fundamental de las normas ISO? [Sitio Web]. [Consulta: 18 de marzo de 2022]. Disponible en: https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:~:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.

HEFLO. Mejora continua. [Sitio Web]. Brasil. [Consulta: 19 de marzo de 2022]. Disponible en: https://www.heflo.com/es/definiciones/mejora-continua/ https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.

HUERTAS CUERVO, Lorena Astrid. Diseño de Políticas de acuerdo al estándar ISO 27001 de seguridad de la información en la fundación internacional MARYOS. [En línea]. Proyecto de grado. Universidad Nacional Abierta y a Distancia, UNAD. 2020. [Consulta: 17 de septiembre de 2022]. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/35738/1/lacuervoh.pdf

INCIBE, Vulnerabilidad en la función VisitPointers de heap.cc (CVE-2019-2052). [Sitio Web]. [Consulta: 19 de octubre de 2022]. Disponible en: https://www.incibe-cert.es/content/boletin-vulnerabilidades-1556

ISO 27001, Fase 2 análisis del contexto de la organización y determinación del alcance. [Sitio Web]. Barcelona. [Consulta: 9 de mayo de 2022]. Disponible en: https://normaiso27001.es/fase-2-analisis-del-contexto-de-la-organizacion-y-determinacion-del-alcance/

ISOTOOLS, ¿Qué es la seguridad de la información y cuantos tipos hay? [Sitio Web]. Santiago. [Consulta: 18 de marzo de 2022]. Disponible en: https://www.pmg-

ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

LAC, 8 Tipos principales de vulnerabilidad de seguridad en las empresas. [Sitio Web]. [Consulta: 15 de octubre de 2022]. Disponible en: https://digital.la.synnex.com/8-tipos-principales-de-vulnerabilidad-de-seguridad-en-las-empresas

LD GRUPO, Ciberseguridad. [Sitio Web]. Lima, Breña [Consulta: 19 de marzo de 2022]. Disponible en: https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/

MEDIACLOUD, ¿Cómo protegerse? El análisis de vulnerabilidad informática. [Sitio Web]. Lima, Breña [Consulta: 29 de septiembre de 2022]. Disponible en: https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/

MESA MENDIVELSO, Luis Manuel. Diseño de un sistema de gestión de la seguridad de la información en la empresa ALGORÍTMICOS M&C. [En línea]. Proyecto de grado. Universidad Nacional Abierta y a Distancia, UNAD. 2020. [Consulta: 18 de septiembre de 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36123/lmmesame.pdf?sequence=1

MINTIC, Seguridad y privacidad de la información. [Sitio Web]. Bogotá. [Consulta: 19 de marzo de 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

NOTARIA 7 BOGOTÁ, funciones y deberes de los notarios. [Sitio Web]. Bogotá. [Consulta: 17 de marzo de 2022]. Disponible en: https://notaria7bogota.com/wp-content/uploads/2020/10/3.2-FUNCIONES-Y-DEBERES-DE-LAS-NOTARIAS.pdf

OÑATE ARBOLEDA, Adriana. Propuesta de políticas de seguridad de la información para proteger los activos de información en las organizaciones. [En línea]. Proyecto de grado. Universidad Nacional Abierta y a Distancia, UNAD. 2021. [Consulta: 12 de agosto de 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/41984/aonatear_3ago2021.pdf?sequence=1&isAllowed=y

P27001 ACADEMY, ¿Qué es norma ISO 27001? [Sitio Web]. Zagreb. [Consulta: 18 de marzo de 2022]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

RAMÍREZ TÁMARA, Germán Darío y MONTOYA URREA, Robinson Arley. Diseño de un Sistema De Gestión de Seguridad de la Información Basado En La Norma Iso 27001:2013 Para La Corporación Universitaria Antonio José De Sucre. En

línea]. Proyecto de grado. Universidad Nacional Abierta y a Distancia, UNAD. 2022. [Consulta: 5 de abril de 2023]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/54506/gdramirezt.pdf?sequence=1&isAllowed=y

REDES ZONE, Estos son todos los ataques a las redes que existen y cómo evitarlos. [Sitio Web]. [Consulta: 12 de septiembre de 2022]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/listado-completo-ataques-redes-como-evitarlos/

REDES ZONE, Principales amenazas de seguridad en una web. [Sitio Web]. [Consulta: 20 de octubre de 2022]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/principales-amenazas-seguridad-web/

RINCÓN BRITO, Cesar Daniel. Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en la norma internacional ISO/IEC 27001:2013 para la compañía ESSENSALE S.A.S. [En línea]. Proyecto Aplicado. Universidad Nacional Abierta y a Distancia, UNAD. 2020. [Consulta: 14 de agosto de 2022]. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/39179/3/cdrinconb.pdf

SEGURIDAD INDUSTRIAL, Seguridad Fisica, Riegos en la Industria. [Sitio Web]. [Consulta: 19 de octubre de 2022]. Disponible en: https://iutsi.wordpress.com/seguridad-fisica-riegos-en-la-industria/

SEGURIDAD INFORMATICA, Vulnerabilidades de un sistema informático. [Sitio Web]. [Consulta: 25 de septiembre de 2022]. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

TECNOLOGÍAS INFORMACION, Integridad de datos. [Sitio Web]. [Consulta: 18 de marzo de 2022]. Disponible en: https://www.tecnologias-informacion.com/integridaddatos.html

UNIR, Claves de las políticas de seguridad informática. [Sitio Web]. La Rioja [Consulta: 19 de marzo de 2022]. Disponible en: unir.net/ingenieria/revista/POLÍTICAs-seguridad-informatica/

UPS COMUNICACIONES, Fallas más comunes de su equipo ups. [Sitio Web]. [Consulta: 20 de octubre de 2022]. Disponible en: https://upscomunicaciones.com/fallas-mas-comunes-de-sus-equipo-ups/