ESPECIALIZACION EN CIBERSEGURIDAD

IMPLEMENTACION SGSI EN LA UNIDAD DE RENTAS BASADO EN LA ISO 27001

JOSE FERNANDO GOMEZ SANCHEZ

YERSON OCHOA PUERTA

LEONARDO PATIÑO CORREA

Universidad® Católica de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia de la Congregación

Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

IMPLEMENTACION SGSI UNIDAD DE RENTAS BASADO EN LA NORMA ISO 27001

Trabajo de grado presentado como requisito para optar al título de *especialización en ciberseguridad*

Modalidad de grado: Monografia

Jhon Cesar Arango

Jose Fernando Gomez Sanchez

Yerson Ochoa Puerta

Leonardo Patiño Correa

UNIVERSIDAD CATÓLICA DE MANIZALES

FACULTAD INGENIERIA Y ARQUITECTURA

ESPECIALIZACION EN CIBERSEGURIDAD

MANIZALES, CALDAS

2024

Resumen

La norma ISO 27001 es una herramienta importante para la gestión efectiva de la seguridad de la información en cualquier tipo de organización, proporcionando un enfoque sistemático y estructurado para la gestión de los riesgos de seguridad y la protección de la información. Esta norma nos dará las pautas necesarias para tomar los respectivos lineamientos para la planificación, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del sistema de gestión en la unidad de rentas de la Gobernación de Caldas.

Su objetivo principal es ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información que manejan. A continuación, se presenta un resumen de los aspectos más importantes a tener en cuenta para iniciar con el proceso de la implementación de un SGSI, basado en la norma ISO 27001

Palabras clave: SGSI, Riesgos, Políticas, Seguridad, Marcos de Referencia

Abstract

ISO 27001 is an important tool for effective information security management in any type of organization, providing a systematic and structured approach to security risk management and information protection. This standard will give us the necessary guidelines to take the respective guidelines for the planning, implementation, operation, monitoring, review, maintenance and continuous improvement of the management system in the revenue unit of the Government of Caldas.

Its main objective is to help organizations protect the confidentiality, integrity, and availability of the information they handle. Below is a summary of the most important aspects to take into account to start the process of implementing an ISMS, based on the ISO 27001 standard

Keywords: ISMS, Risks, Policies, Security, Reference Frameworks

Tabla de Contenido

Tabla de figuras

Tabla de Tablas

Capítulo 1. Introducción de la implementación

1.1 Introducción

En un mundo cada vez más tecnológico y globalizado, la seguridad de la información es un área de cuidado y de constante actualización para cualquier tipo de entidad; este trabajo se centrará en las Normas ISO 27001, desde el nro. 4.1, que hace referencia a la comprensión de la organización y su contexto y el nro. 5.2 que habla sobre la definición de políticas; y la ISO 31000, se tomará el nro. 5.4.1 que contempla la comprensión de la organización y su contexto, y por último, el nro. 6.4.2, que habla de la identificación de riesgos; estas anteriores, conocidas como normas internacionales de seguridad de la información que resguarda la confidencialidad, integridad y disponibilidad de un Sistema de Gestión de Seguridad de la Información (SGSI).

El presente trabajo de implementación del Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001(nro. 4.1 y nro. 5.2); de igual importancia, de la Norma ISO 31000 (nro. 5.4.1 y el nro. 6.4.2) revelando los resultados finales, de los aportes, sugerencias y recomendaciones, de esta manera, se realizará un documento de revisión en cita, los cuales se llevaron a cabo en la especialización de Ciberseguridad , Facultad de Ingeniería y Arquitectura, de la Universidad Católica de Manizales.

Este es efecto de un trabajo juicioso y continuo que se consolidó en identificar riesgos asociados durante la ejecución de los procedimientos asociados a la administración y recaudo de los diferentes impuestos administrados por la Unidad de Rentas de la Gobernación de Caldas, ubicada en la ciudad de Manizales, basado en la Norma ISO 27001, numeral 4.1, que hace referencia a la comprensión de la organización y su contexto, junto con el numeral 5.2 que habla sobre la definición de políticas; de igual importancia, de la Norma ISO 31000 se toma el

numeral 5.4.1 de la comprensión de la organización y su contexto, finalizando con el numeral 6.4.2 que habla sobre la identificación del riesgo.

En la actualidad, se presenta la necesidad de reconsiderar que toda organización que cuente con sistemas de información debe optar por una certificación que avale desde una norma internacional para asegurar y manejar dichos procesos. Al mismo tiempo, los conceptos definen de manera genérica el cómo se implementa y controla un sistema de gestión de seguridad de la información, a partir de la realización de un análisis de riesgos y de la planificación y la implementación de las respuestas a los mismos para su mitigación.

Después de llevar a cabo una detallada revisión bibliográfica, la cual implicó sí se habían realizado implementaciones del SGSI basados en la Norma ISO 27001 e ISO 31000 en ciertas entidades, se constató que el trabajo de especialización realizado en la Secretaría de hacienda del municipio de Cucunubá-Cundinamarca, un diseño del Sistema de Gestión de Seguridad de la Información, bajo la Norma ISO 27001; este trabajo de partido se obtuvo del repositorio de la Universidad Piloto de Colombia de la facultad de ingeniería.

El anterior, fue el trabajo que impulsó replantear la implementación de un SGSI, en la Unidad de Rentas de la Gobernación de Caldas. Por su parte, el estado del arte, permitió establecer a su vez, determinar que este trabajo de especialización posee un carácter innovador, ya que aspira a convertirse en un punto de referencia en términos de metodología e implementación práctica para impulsar nuevas direcciones de futuros trabajos, que se centran en la gestión de riesgos enfocado a averiguar y consultar qué tipo de seguridad utilizan en las entidades de orden estatal y cómo poder evitar que ocurran incidentes que comprometan la seguridad de la información cómo llegar a mitigarlos

Simultáneamente, ante los riesgos que se está expuesto todo, incluyendo pequeñas, medianas y grandes empresas de ataques de ciberdelincuentes o errores humanos que “intentan destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado a la misma; sabiendo de antemano que la información es demasiado importante en cualquier ámbito laboral, por lo tanto, es necesario evaluar los riesgos, en este caso, de la Unidad de Rentas de la Gobernación de Caldas, en la ciudad de Manizales y establecer medidas para solventarlas.

La implementación de un sistema de gestión de seguridad de información basado en la norma ISO 27001 y la norma ISO 31000, tiene ciertos puntos que deben considerarse importantes puesto que avalan la investigación en el campo de la seguridad informática por medio de una revisión exhaustiva en la bibliografía se logró identificarlas relevantes líneas de acción y las implicaciones prácticas que conlleva implementar esta norma de seguridad , que a su vez, no solo hace referencia a información almacenada en sistemas informáticos (correos electrónicos, videos, archivos), sino a documentos en papel (físicos). Así pues, se hace necesario garantizar que el acceso a los activos de información se realice de una manera segura y controlada.

Ahora bien, este trabajo busca dejar un punto de referencia para la implementación del Sistema de Gestión de Seguridad de la Información explorando desafíos, riesgos, asimismo, beneficios que contribuyan al análisis de componentes claves en los procesos de una evaluación desde una reunión administrativa, hasta cubrir auditorías para buscar la mejora continua esto; lo anterior, en pro de cumplir con los requisitos reglamentarios que se requiere para obtener la certificación ISO 27001, conocida como un reconocimiento externo de una organización al implementar un SGSI conforme a los estándares de la norma; generando

confianza en los contribuyentes y demás partes interesadas, demostrando así, el compromiso de la organización con la seguridad de la información.

1.2 Objetivos

1.2.1 Objetivo General

Crear un documento en el cual se establezca una partida para la implementación de un sistema de gestión de seguridad de la información en la unidad de rentas de la Gobernación de Caldas basado en la norma ISO 27001

1.2.2 Objetivos Específicos

Realizar un análisis del contexto de la unidad de rentas de la gobernación de Caldas y determinar el alcance del SGSI

Redactar un documento con políticas de seguridad las cuales deberán estar en constante monitoreo de cumplimiento para la implementación del SGSI.

1.3 Planteamiento del Problema

Las dificultades que se presentan a través de diferentes prácticas en la implementación de un Sistema de Gestión de Seguridad Información, hacen que se deba implementar estrategias y enfoques para ser efectiva conforme a la Norma ISO 27001.

En un país como Colombia, en el departamento de Caldas; particularmente en el municipio de Manizales, circunstancias que propician el paulatino detrimento de los SGSI y la forma en cómo los usuarios se desenvuelven en él. Es por esta razón que se suma la importancia de estar a la vanguardia de las certificaciones internacionales para establecer las buenas prácticas de un sistema de gestión de seguridad de la información ofreciendo no solo un prestigio a la organización qué los implementa, sino que, genera un ambiente de confiabilidad entre los actores de la institución.

Desde la posición de Mancuzo, (2023) señala que:

> Los riesgos en ciberseguridad son una amenaza es una probabilidad de ocurrencia de un suceso potencialmente peligroso, durante cierto periodo de tiempo, en un lugar indicado. Por otro lado, el riesgo aparece cuando esa amenaza tiene probabilidad de convertirse en un desastre, con pérdidas de algún tipo para la institución o persona que lo sufra. (párr.6)[1]

Por lo tanto, ¿cómo enfrentar y mitigar esta realidad de riesgos y dificultades ante ataques cibernéticos? pues no basta con identificarlos, tener un plan de manejo para

[1] Mancuzo, G. (2022, abril 12). ¿Qué es un riesgo en Ciberseguridad? Definición y tipos. Ciberseguridad; Ciberseguridad Tips. https://ciberseguridadtips.com/que-es-un-riesgo-en-ciberseguridad-definicion-causas

incidentes, sino que, es necesario considerar que, la unidad de rentas de la Gobernación de Caldas, es la encargada de la administración y el recaudo de los diferentes impuestos departamentales; y que en consecuencia, no cuenta actualmente con un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 y la norma ISO 31000.

Al mismo tiempo, la falta de tener unas políticas de la información definidas y el hecho de tener tercerizados la mayoría de sistemas de información, junto con la rotación del personal debido al modelo de contratación que se maneja en este tipo de Instituciones gubernamentales, hace que la información y los sistemas sean vulnerables ante los riesgos de ciberseguridad a los que se están expuestos en la actualidad.

Es así cómo se hizo indispensable, la identificación de los riesgos y la definición de un manual de políticas de la información, en el que permitirá tener un punto de partida para la implementación de un SGSI basado en la Norma ISO 27001, lo cual permitirá no solo al área de la Unidad de Rentas, sino a toda la Gobernación de Caldas como entidad gubernamental, gestionar de manera efectiva la seguridad de la información, minimizar los riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información. Sin embargo, es de tener en cuenta que, para la implementación del SGSI se debe contar con el recurso humano y económico, y desafortunadamente la entidad no dispone de este rubro, para dicha inversión.

En virtud de lo mencionado, se hizo necesario desarrollar una estrategia o primeros pasos en la implementación de un Sistema de Gestión de Seguridad de la Información identificando los riesgos y definiendo un manual de políticas de la información, lo cual ayudará a contener las amenazas de ciberseguridad e iniciar el proceso de implementación del SGSI basado en la Norma ISO 27001. Sumado a esto, a través del análisis de recolección de la información, se evidenció un panorama de importancia y regularización de la misma.

1.4 Formulación del Problema

Las particularidades de la implementación de un Sistema de Gestión de Seguridad de la Información es una necesidad que toda organización deja ver; el entramado complejo de cambios y la dificultad de la organización y sus sistemas hace que se implemente la norma para una interacción de forma productiva, sistemática y segura.

De tal manera que la pregunta axial es: ¿De qué manera la unidad de rentas de la gobernación de Caldas puede garantizar el uso adecuado de los activos de información inherentes a la administración y recaudo de los impuestos departamentales?

¿Cómo se puede garantizar que la información administrada por la unidad de rentas, cumpla con los principios de la seguridad de la información?

1.5 Justificación

Es importante tener documentado el proceso para la implementación de un sistema de gestión de seguridad de la información toda vez que la información es uno de los activos más valiosos con los que cuenta la unidad de rentas del departamento de caldas, al tener documentado este proceso se deben de realizar una serie de pasos los cuales nos llevan a identificar, proteger y clasificar la información, además de gestionar riesgos y dar una mayor confianza a los ciudadanos acerca de la información personal con la que cuenta la unidad de rentas en sus diferentes sistemas de información, por otra parte desde la administración departamental se debe garantizar que la información con la que se cuenta sea confiable, y pueda ser accedida por las personas autorizadas para ello ya que los procesos a los que se dedica la unidad de rentas son orientados a la administración y cobro de las rentas, tasas y contribuciones que por ley deben ser administradas por el departamento de Caldas.

Una pérdida de información o una alteración en la misma puede tener consecuencias de carácter jurídico, disciplinario, económico para las personas a cargo de cada una de las áreas encargadas del proceso de cobro además de la pérdida de credibilidad ante la ciudadanía en general.

Se puede ver la utilidad de tener un sistema de gestión de seguridad de la información porque como su nombre lo indica son procedimientos y prácticas aplicadas a salvaguardar la información ya que es un activo transversal a todos los procesos de la entidad, además que de esta manera se puede identificar, clasificar, corregir, mitigar cada una de las vulnerabilidades, riesgos a los que se expone la información.

Además de que es un punto de partida para que una entidad del estado se certifique en la norma ISO 27001, lo cual dará un parte de tranquilidad a todos los actores que intervienen en cada una de los procesos de la unidad de rentas como lo es la ciudadanía en general, proveedores externos de servicios informáticos y funcionarios de la entidad, garantizando de tal manera que el manejo que se le da a la información se hace de manera adecuada ya que de esta depende que los procesos de recaudo, liquidación, fiscalización y gestión de cobro coactivo de las diferentes áreas, puedan ser realizados de manera efectiva en caso de llegar a haber un incidente como pérdida, alteración o filtración de datos que pueden afectar directamente las finanzas del departamento.

1.6 Antecedentes

Al realizar, el levantamiento de información para determinar el alcance que podría tener un sistema de gestión de seguridad de la información en la unidad de rentas del departamento de Caldas, se pudo identificar que la unidad de rentas del departamento cuenta con un proceso principal el cual lo denominan Administración y recaudo y de este parte diferentes procedimientos algunos de ellos no cuentan con la documentación suficiente que defina bien el proceso y sus indicadores, otros de estos en el año 2024, ya no se realiza dado que estaban orientados al recaudo y administración de los peajes departamentales, por lo que no se deben tener en cuenta para el análisis.

Por otra parte existen procedimientos los cuales no cuentan con la documentación necesaria para poder determinar, el flujo de cada uno de estos e identificar los riesgos asociados, lo que se cuenta es con personal el cual cuenta con una amplia experiencia en cada uno de estos y se puede percibir que son procedimientos estables, pero sin la documentación, lo cual puede generar que en el momento de que las personas a cargo de uno de los procedimientos falte, el procedimiento queda huérfano y sin ninguna documentación para su continuidad.

Por otra parte la unidad de rentas de la gobernación de Caldas, cuenta con un gran número de contratistas prestadores de servicios los cuales en su objeto contractual realizan actividades de suma importancia, la cual sirve para dar continuidad y apoyo a los procesos de cobro coactivo, determinación y liquidación de fiscalización del impuesto vehicular y demás tasas y contribuciones del departamento de Caldas; Si bien el proceso macro de contratación está previamente establecido, por la Secretaría jurídica de la gobernación de Caldas, la unidad

de rentas del departamento de Caldas no cuenta con un procedimiento establecido orientado al recurso humano.

Aunque el proceso principal de la unidad de rentas es la administración y recaudo, se deben definir, determinar y documentar los procedimientos asociados a Tecnologías de la información y recursos humanos, ya que estos dos macroprocesos son fundamentales para la correcta planeación e implementación de un sistema de gestión de Seguridad de la Información en la unidad de rentas de la gobernación de Caldas.

1.6.1 Nacionales

En el año 2022 se presentó un incremento del 133% en el número de organizaciones e instituciones representativas de Colombia afectadas por ataques ransomware, respecto al año anterior [2].

En su totalidad fueron 34 instituciones hackeadas y vulneradas por el famoso ataque ransomware, el cual se especializa en el secuestro de la información a través de malware para luego pedir un rescate monetario a las organizaciones que los recuperen [2].

Caracol TV:

La importante empresa de medios de comunicación que todos conocen; Carcol TV, fue víctima de ataques por ciberdelincuentes en el mes de mayo. Este canal de televisión, alertó de la situación ya que la vulnerabilidad no alcanzó a tomar información sensible, sino que afectó varios programas de diseño, así como algunas aplicaciones operativas [2].

---

[2] Pachón, C.(s.f.). 10 reconocidas instituciones de Colombia hackeadas en el 2022. NSIT SAS. Recuperado el 13 de marzo de 2022 de https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/

Viva Air

Viva Air, la reconocida aerolínea colombiana también fue víctima de los ciberdelincuentes el pasado 14 de marzo del 2022. ¿Cómo sucedió? la entidad fue comprometida por un ransonware que robó y filtró información importante de la empresa y sus clientes. La banda RansomEXX se atribuyó este ataque [3].

Salud Total

La entidad Salud Total, el pasado 1 de mayo de 2022 se vio comprometida por un ataque cibernético. ¿Qué sucedió? el ataque produjo indisponibilidad en los servicios debido a que se deshabilitaron servidores físicos y virtuales, además de su infraestructura tecnológica, con el fin de que no se viera afectada la información de empleados y clientes [3].

Las entidades gubernamentales más suplantadas en Colombia son: DIAN, Fiscalia general de la Nación, Organismos de tránsito, Policía Nacional , Ministerio de Salud [3]

Esta información fue tomada desde el portal de ni, empresa dedicada a consultoría en ciberseguridad en una de las publicaciones realizadas dentro de la sección de noticias en en el año 2022 [3].

1.6.2 Internacionales

Uno de los incidentes más notables del año: Costa Rica fue atacada por el Grupo Conti, con sede en Rusia. En abril, los ciberdelincuentes exigieron 10 millones de dólares a cambio de cesar el ataque y devolver la información robada. El gobierno costarricense se negó a pagar.

[3] Pachón, C.(s.f.). 10 reconocidas instituciones de Colombia hackeadas en el 2022. NSIT SAS. Recuperado el 13 de marzo de 2022 de https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/

"Estamos en guerra y no es una exageración", fue lo que dijo entonces el presidente de este país centroamericano, Rodrigo Chaves [4].

El 18 de abril, Conti dirigió su ciberataque masivo en forma de ransomware a organizaciones e instituciones de toda Costa Rica. La banda de ciberdelincuentes atacó 30 instituciones costarricenses, entre ellas el Ministerio de Trabajo, el Ministerio de Ciencia, Tecnología y Telecomunicaciones, la Seguridad Social o el Instituto Meteorológico Nacional. Pero el más afectado fue el Ministerio de Hacienda, donde los ciberdelincuentes accedieron a los servidores y usurparon todo tipo de información [4].

Un informe de Tendencias de Protección de Datos 2023 elaborado por la empresa de pagos globales Veem indicó que el 85 % de las empresas en América Latina sufrió al menos un ataque cibernético en el último año, en el que solo pudo recuperarse el 55 % de los datos cifrados o destruidos [4].

Estos antecedentes de tipo internacional se tomo como fuente el blog de globalsign en una de sus publicaciones.

[4] https://www.globalsign.com/es/blog/tres-ciberataques-que-desafiaron-america-latina-en-2022

Capítulo 2. Marcos de la Investigación

2.1 Contexto Geográfico

La Gobernación de Caldas ubicada en la ciudad de Manizales en la carrera 21 entre calles 22 y 23, nos enfocaremos específicamente en la unidad de rentas del departamento la cual se encuentra en el primer piso del edificio de la antigua licorera Entidad de orden departamental la cual promueve el desarrollo económico, social y físico, dentro del territorio, mediante el ejercicio de funciones administrativas, de coordinación, de complementariedad y de subsidiariedad hacia la acción municipal y de intermediación entre la nación y los municipios, así como la prestación de los servicios que determinen la Constitución y las leyes.

Figura 1

Instalaciones Unidad de Rentas

Fuente: El autor, 2024

Figura 2

Imagen del edificio donde se encuentra ubicada la unidad de Rentas

Fuente: El autor, 2024

2.2 Marco Normativo

En Colombia existen varias normas que regulan la protección de datos personales y la ciberseguridad entre ellas está la ley 1581 del 2012[5] por la cual se dictan disposiciones generales para la protección de datos personales y cuyo objetivo es desarrollar el derecho

[5] Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 17 de abril de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma y su decreto reglamentario 1377 de 2013[6] el cual tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

LEY 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[7].

LEY 1266 DE 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.[8]

---

[6] Decreto 1377 de 2013

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[7] Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

[8] Ley 1266 de 2008 - Gestor Normativo.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

LEY 527 DE 1999

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [9].

Ordenanza 816 del 2017

Por la cual se expide el estatuto de rentas del departamento de caldas y se dictan otras disposiciones [10].

2.3 Marco Teórico

Norma ISO 27001 La seguridad de datos y la información de cualquier tipo en la actualidad se ha convertido en un reto dentro de una organización. Un SGSI (Sistema de gestión de la seguridad de la información) hace que los riesgos de seguridad de la información para las organizaciones sean calculables y manejables. Mientras que la norma ISO 27001 proporciona un conjunto de controles para la seguridad de la información que una organización debe implementar en función de los resultados de una evaluación de riesgos y los requisitos de las partes interesadas. Es decir, para cada riesgo a tratar se implementará una combinación de diferentes tipos de controles. Para la implementación de la norma ISO 27001 recurre al ciclo de

[9] Ley 527 de 1999

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

[10] El estatuto de rentas contiene todo el marco legal de los diferentes impuestos tasas y contribuciones administrados por la unidad de rentas del departamento de Caldas
https://site.caldas.gov.co/documentos-secretaria-de-hacienda/2942-ordenanza-816-estatuto-de-rentas

Deming que se encarga del continuo mejoramiento de la seguridad de la información[11]. Podemos concluir que: un SGSI actúa como un eje centralizado para salvaguardar y gestionar toda la información de una organización en un solo lugar.

La norma ISO 27001 es un estándar internacional que establece los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI).

Cláusula 1: Alcance.

Cláusula 2: Referencias normativas.

Cláusula 3: Términos y definiciones.

Cláusula 4: Contexto de la organización.

Cláusula 5: Liderazgo.

Cláusula 6: Planificación.

Cláusula 7: Soporte.

Cláusula 8: Operación.

Cláusula 9: Evaluación del desempeño.

Cláusula 10: Mejora [12].

Norma ISO 31000: La norma ISO 31000 es un estándar internacional que proporciona principios y directrices para la gestión del riesgo. A diferencia de la ISO 27001, la ISO 31000 no se estructura en "artículos" o "cláusulas" como en otras normas, sino en secciones y principios.

[11] Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. Recuperado 10 de marzo del 2022 https://dominiodelasciencias.com/ojs/index.php/es/article/view/2854

[12] Norma ISO 27001. (s/f). Norma ISO 27001. Recuperado el 17 de abril de 2024, de https://normaiso27001.es

La norma ISO 31000:2018 es aplicable a cualquier organización, independientemente de su tamaño, sector o naturaleza, y proporciona una guía sólida para ayudar a las organizaciones a gestionar el riesgo de manera efectiva. Es importante consultar la norma completa para obtener detalles específicos y orientación detallada sobre la implementación de la gestión del riesgo.

La ISO 31000:2018 consta de los siguientes elementos principales:

1- Introducción

2- Principios para la gestión del riesgo

3- Marco de trabajo para la gestión del riesgo

4- Proceso de gestión del riesgo

Cada sección aborda aspectos específicos relacionados con la gestión del riesgo. La norma es bastante concisa y se centra en proporcionar orientación general sobre los principios y procesos de gestión del riesgo. Te recomendaría revisar la versión más reciente de la norma para obtener detalles específicos y actualizados.

Internos: Los factores de riesgo internos se refieren a las amenazas y vulnerabilidades que provienen dentro de la propia organización. Estos riesgos pueden surgir debido a acciones, omisiones o situaciones dentro de la empresa. Aquí hay algunos ejemplos:

Descuido o Falta de Conciencia: Los empleados pueden cometer errores por descuido, como abrir correos electrónicos maliciosos, hacer clic en enlaces no seguros o compartir información confidencial de manera inadvertida.

Contraseñas Débiles o Compartidas: El uso de contraseñas débiles, compartir contraseñas entre empleados o no cambiar las contraseñas regularmente puede aumentar el riesgo de acceso no autorizado a sistemas y datos.

Acceso No Autorizado: La asignación incorrecta de privilegios y permisos puede dar lugar a accesos no autorizados. Además, la falta de una gestión efectiva de las cuentas de usuario puede llevar a que ex empleados mantengan acceso no autorizado.

Uso Inadecuado de Dispositivos de Almacenamiento: La conexión de dispositivos USB no seguros, la pérdida de dispositivos móviles con datos sensibles o el uso no autorizado de dispositivos externos pueden representar riesgos de seguridad.

Fuga de Información: La fuga de información confidencial debido a la negligencia, malas prácticas o intenciones maliciosas de empleados puede tener consecuencias significativas para la seguridad de la empresa.

Falta de Actualizaciones y Parches: No mantener actualizados los sistemas y software con los últimos parches de seguridad puede dejar a la empresa vulnerable a explotaciones de vulnerabilidades conocidas.

Insider Threats (Amenazas Internas): Empleados malintencionados que buscan dañar a la empresa, ya sea robando información, realizando actividades de sabotaje o colaborando con amenazas externas.

Falta de Políticas de Seguridad: La ausencia de políticas y procedimientos de seguridad claros puede resultar en prácticas inseguras por parte de los empleados y en la falta de un marco efectivo para la gestión de la seguridad.

Externos: Los ataques externos son aquellos orquestados por ciberdelincuentes, con el objetivo de robar información sensible. Estos datos pueden ser bancarios, como número de cuenta, token y contraseña, o de índole comercial o personal.

1- Ciberataques: Ataques perpetrados por hackers, crackers o grupos cibernéticos con el objetivo de comprometer la seguridad de la red, robar datos confidenciales o interrumpir lasoperaciones.

2- Malware: Software malicioso diseñado para dañar o acceder de manera no autorizada a sistemas informáticos. Esto incluye virus, troyanos, ransomware y spyware.

3- Ingeniería Social: Técnicas utilizadas por atacantes para manipular a empleados y obtener información confidencial. Esto puede incluir phishing, pretexting, o la manipulación psicológica para obtener contraseñas u otra información sensible.

4- Desastres Naturales y Eventos Ambientales: Eventos como terremotos, inundaciones, incendios u otras catástrofes naturales que pueden afectar la infraestructura física y la disponibilidad de los sistemas.

5-Phishing: El phising es un tipo de ingeniería social que se emplea, por lo general, para robar datos de usuario. Pueden ser números de tarjetas de crédito o contraseñas, por ejemplo. Ocurre cuando un delincuente se hace pasar por una persona de confianza. Entonces, engaña a la víctima para que abra un mensaje de texto, correo electrónico o SMS mediante un enlace malicioso. Este enlace puede causar la congelación de un sistema ransomware, revelar información confidencial o instalar malware [13].

6-Inyección SQL: La inyección SQL es una técnica de ataque informático que se ha convertido en uno de los problemas de seguridad más prevalentes en el mundo de la ciberseguridad. A través de este método, un atacante puede ejecutar comandos SQL

[13] Definición tomada de: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

malintencionados en una base de datos detrás de una aplicación web, lo que potencialmente le permite manipular o robar datos sensibles. Este tipo de ataque explota las vulnerabilidades presentes en las aplicaciones que no realizan una validación o saneamiento adecuado de las entradas de usuario antes de pasarlas a una consulta SQL [14].

2.4 Marco Conceptual

2.4.1 Terminología:

La seguridad informática: La seguridad informática está relacionada con las metodologías, procesos y procedimientos para mantener salvaguardada la información y los datos confidenciales de una organización, al interior de los sistemas informáticos. Los procesos se estructuran con el uso de estándares, normas, protocolos y metodologías para mitigar y minimizar los riesgos asociados a la infraestructura tecnológica [15].

Seguridad de la información: La seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos, como electrónicos. Por lo tanto, las organizaciones deben adoptar y adaptar metodologías para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuada que sirva para la custodia y salvaguarda de la información [15]

Vulnerabilidad informática: Una vulnerabilidad informática se refiere a una debilidad o fallo en un sistema, aplicación, red o proceso que podría ser explotado por un atacante para comprometer la seguridad de la información. Estas vulnerabilidades pueden existir en el

[14] https://masterenciberseguridadonline.es/inyeccion-sql-ejemplos/
[15] https://rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

software, hardware o incluso en las prácticas y procedimientos utilizados en entornos informáticos.

Amenaza informática: Una amenaza informática se refiere a cualquier evento o acción que tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad de los sistemas informáticos y la información que contienen. Estas amenazas pueden provenir de diversas fuentes y adoptar diferentes formas. Aquí hay algunas categorías comunes de amenazas informáticas:

Riesgo informático: El riesgo informático se refiere a la posibilidad de que eventos adversos impacten negativamente en los sistemas informáticos, la información que contienen y, en última instancia, en las operaciones de una organización. Estos riesgos pueden surgir de diversas fuentes y tener consecuencias que afectan la confidencialidad, integridad y disponibilidad de los recursos informáticos.

Evento: ocurrencia o cambio de un conjunto particular de circunstancias

Probabilidad (likelihood): posibilidad de que algo suceda

Control: medida que mantiene y/o modifica un riesgo

Sistema de gestión de la seguridad de la información: El SGSI, tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad. El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI,

además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados [16].

La norma ISO 27001 es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI). Esta norma proporciona un enfoque sistemático y proactivo para gestionar la seguridad de la información y aborda aspectos como la confidencialidad, la integridad y la disponibilidad de la información en una organización.

[16] https://rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Capítulo 3. Marco Metodológico

3.1 Metodología

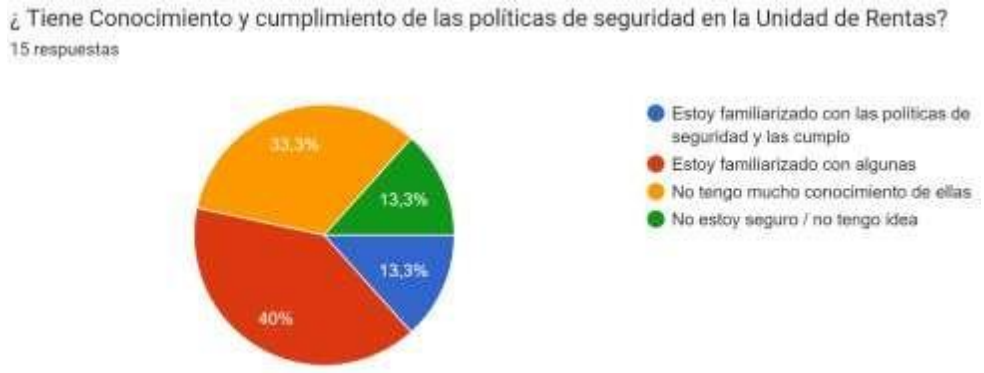
Para el desarrollo de este trabajo se usó como marco de referencia la norma ISO 27001.en sus numerales 4.1, y 5.1, los cuales están relacionados con el análisis del contexto de la organización y con la definición de políticas de seguridad de la información, para la definición de las políticas están se definieron basadas en el análisis de riesgos previamente realizado y también orientado las políticas al cumplimiento del ANEXO A, de la norma ISO 27001:2022 los numerales 5 al 8 los cuales definen controles organizacionales, controles de personas, Controles físicos y controles tecnológicos.

También se usó como marco de referencia la norma ISO 31000:2018, en su numeral 5.4.1 el cual nos indica que se debe realizar un análisis de los factores internos y externos de la unidad de rentas de la gobernación de caldas, para esto se realizó un proceso de recolección de información mediante charlas con los funcionarios o contratistas que administran los diferentes procedimientos, los encargados de dar soporte tanto de los aplicativos propios de la unidad de rentas como de los aplicativos que se encuentran tercerizados, por otra parte, la información contenida en medios digitales específicamente portales web.

De las 80 personas que trabajan en la unidad de rentas se tomó como muestra 15 personas las cuales están adscritas a la unidad de rentas como funcionarios o contratistas para poder conocer si las personas encargadas de manejar los activos de información de la unidad de rentas tienen conciencia y esta familiarizados con la importancia de la seguridad de la información, los resultados de dicha encuesta se muestran a continuación:

Figura 3

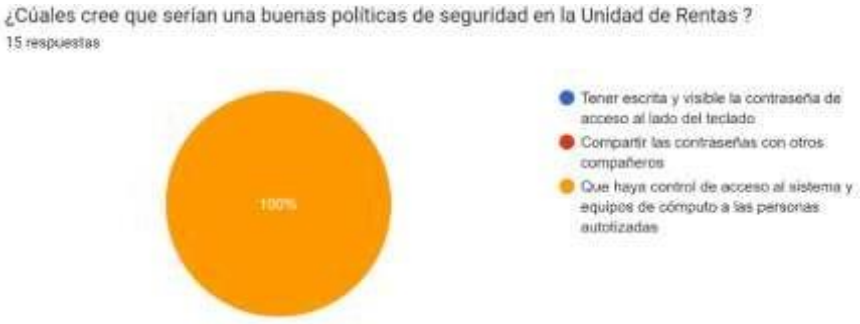
Resultado Porcentual Pregunta 1 Encuesta



Fuente: El autor, 2024

Figura 4

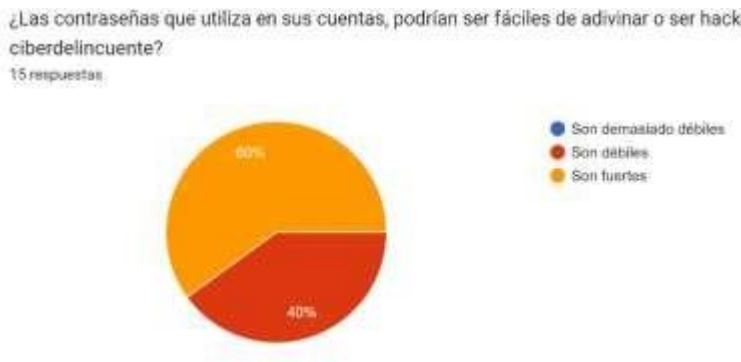
Resultado Porcentual Pregunta 2 Encuesta



Fuente: El autor, 2024

Figura 5

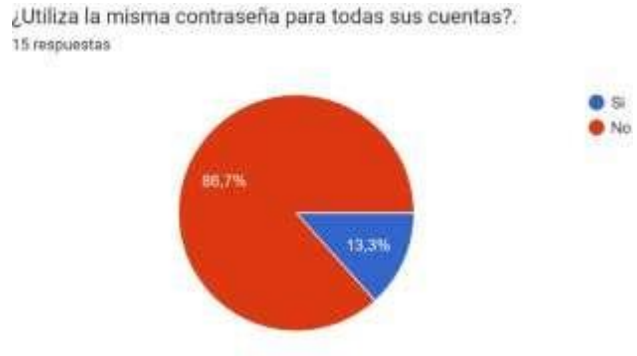
Resultado Porcentual Pregunta 3 Encuesta



Fuente: El autor, 2024

Figura 6

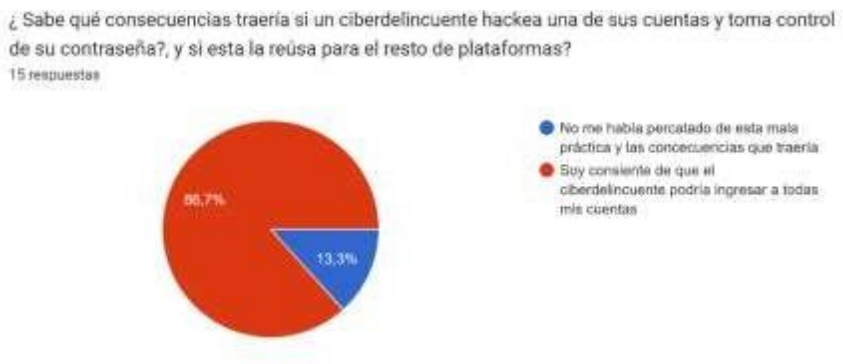
Resultado Porcentual Pregunta 4 Encuesta



Fuente: El autor, 2024

Figura 7

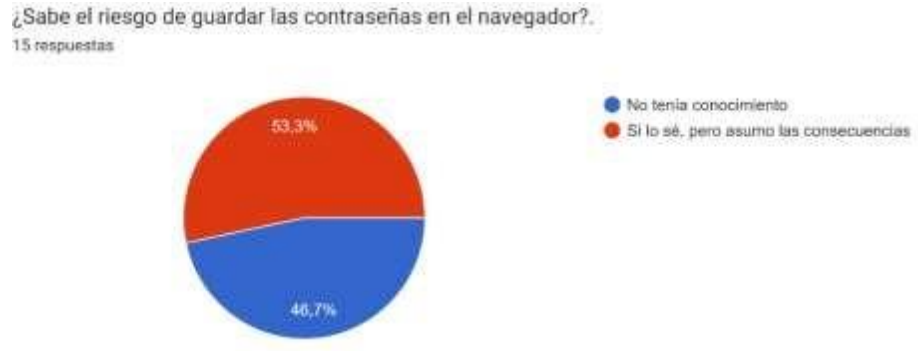
Resultado Porcentual Pregunta 5 Encuesta



Fuente: El autor, 2024

Figura 8

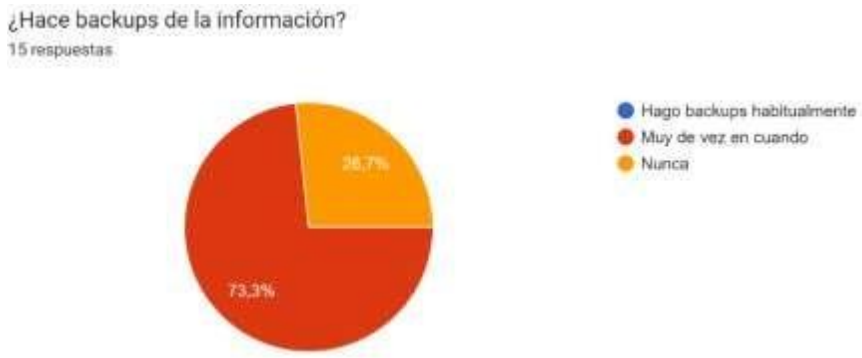
Resultado Porcentual Pregunta 6 Encuesta



Fuente: El autor, 2024

Figura 9

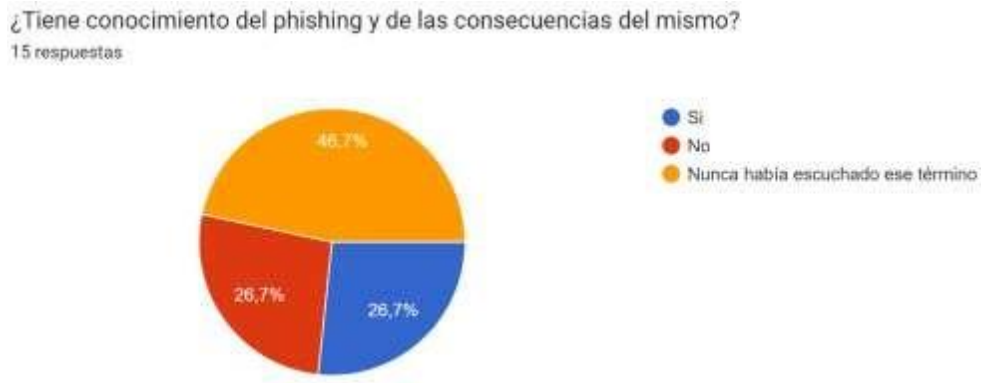
Resultado Porcentual Pregunta 7 Encuesta



Fuente: El autor, 2024

Figura 10

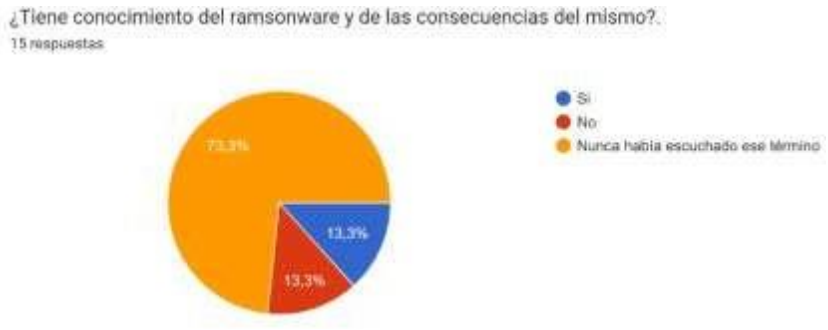
Resultado Porcentual Pregunta 8 Encuesta



Fuente: El autor, 2024

Figura 11

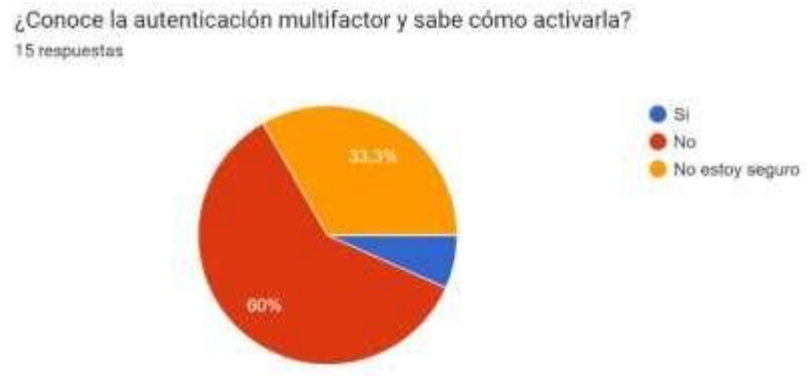
Resultado Porcentual Pregunta 9 Encuesta



Fuente: El autor, 2024

Figura 12

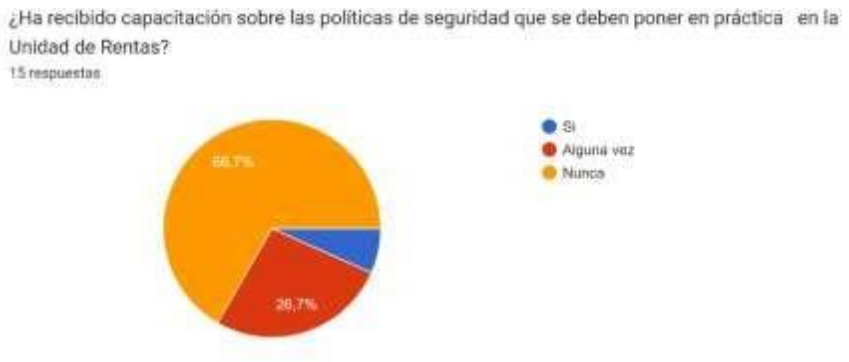
Resultado Porcentual Pregunta 10 Encuesta



Fuente: El autor, 2024

Figura 13

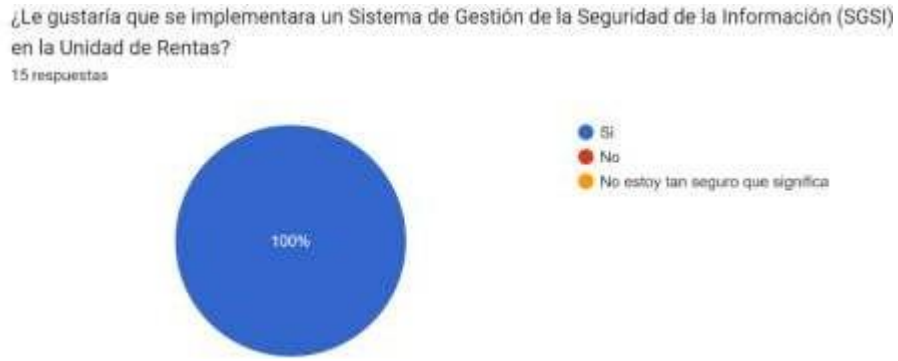
Resultado Porcentual Pregunta 11 Encuesta



Fuente: El autor, 2024

Figura 14

Resultado Porcentual Pregunta 12 Encuesta



Fuente: El autor, 2024

Después de validar los resultados de la encuesta se puede evidenciar que las personas encargadas del manejo de la información en la unidad de rentas conocen los riesgos asociados en la actualidad con el manejo de la misma, pero se tienen malas prácticas para salvaguardar la misma, se desconocen si existen las políticas de seguridad de la información y que estarían

interesados en que se implementaran un sistema de gestión de seguridad de la información en la unidad de rentas de la gobernación de Caldas

Se realizaron jornadas de observación con el fin de poder identificar cómo se realizaban las actividades propias de cada uno de los procedimientos, en los cuales se podían identificar, los riesgos asociados a cada uno de estos, apoyándonos en el literal 6.4.2 de la norma ISO 31000:2018.

En estas jornadas de observación se pudo recolectar información la cual permitió construir la matriz de riesgos asociados acerca del manejo de los activos de información a cada uno de los impuestos a cargo de la unidad de rentas del departamento de Caldas.

Una vez construidos los documentos de análisis de contexto de la organización y la definición de las políticas de seguridad de la información, se tuvo una reunión con el jefe de la unidad de rentas, con el fin de darle a conocer el trabajo realizado, el cual tuvo una buena aceptación del mismo y manifestando que esto será tenido en cuenta a futuro como parte inicial de la implementación de un SGSI en la unidad de rentas de la Gobernación de Caldas

Capítulo 4. Resultados y Discusión

4.1 Con relación al objetivo específico 1

Análisis de contexto de la organización y alcance del SGSI

Análisis del contexto de la organización

Para determinar el alcance del sistema de gestión de seguridad de la información creemos que es pertinente realizar un debido análisis del contexto de la organización, para esto nos hemos basado en el numeral 5.4.1 de la norma ISO 31000:2018 compresión de la organización y su contexto la cual nos indica que se debe tener en cuenta diferentes aspectos los cuales se tendrán en cuenta en dicho análisis

Términos y definiciones generales

Definición de los factores de riesgos:

Los factores de riesgo se refieren a las condiciones, eventos o situaciones que pueden poner en peligro la integridad, confidencialidad o disponibilidad de los sistemas de información y los datos. Estos factores pueden ser variados y suelen incluir aspectos tecnológicos, humanos y organizativos. Las amenazas pueden provenir de actores externos, como hackers, malware y ataques cibernéticos, así como de factores internos, como empleados malintencionados, descuido o falta de conciencia de seguridad.

Para abordar estos factores de riesgo internos, las empresas deben implementar medidas de seguridad adecuadas, incluyendo políticas y procedimientos claros, programas de

concienciación y formación en seguridad, controles de acceso adecuados, y la adopción de prácticas de gestión de riesgos de seguridad.

Contexto externo de la organización: La unidad de rentas de la gobernación de Caldas al pertenecer a una entidad pública de orden departamental, existen diferentes factores los cuales deben ser tenidos en cuenta como lo son el social, cultural, político, económico, legal, ambiental y tecnológico.

Al ser la dependencia encargada de realizar el recaudo y administración de las rentas del departamento, las cuales son pagadas por los contribuyentes, la responsabilidad social de esta unidad debe velar por los intereses de la ciudadanía en general y las necesidades de la gente del departamento.

Por otra parte se debe tener en cuenta que los tributos son deberes y obligaciones de los contribuyentes de las diferentes rentas que ya sea por su actividad económica o posesión de algún bien, impacta de manera directa el entorno político, económico y cultural del departamento de Caldas siendo la unidad de rentas quien de manera directa tiene relación y acercamiento a la ciudadanía durante las diferentes campañas de descentralización de los servicios ofrecidos por la unidad en todos los procedimientos que se derivan de su proceso principal el cual es la administración y el recaudo, se puede identificar necesidades y así planificar diferentes estrategias que permitan garantizar el debido cumplimiento de las obligaciones tributarias de los diferentes contribuyentes y generando una cultura de pago de los tributos en el departamento de Caldas.

Este acercamiento a los contribuyentes de las diferentes rentas, tasas y contribuciones del departamento de Caldas implica un despliegue tecnológico enfocado en garantizar a través de sistemas de información y el uso de las diferentes herramientas tecnológicas poder garantizar que el recaudo de los diferentes tributos se pueda realizar desde cualquier lugar del país, logrando de esta manera evitar la evasión de impuestos y lograr un recaudo que permita al departamento realizar inversiones en sus diferentes proyectos de salud, educación, vivienda, cultura y demás que permitan el crecimiento de la región, por otra parte la masificación de las transacciones electrónicas no son ajenas al recaudo de las rentas, además de poder realizar notificaciones de las diferentes etapas procesales a través de correo electrónicos ha permitido disminuir el uso del papel siendo esto un aporte importante al medio ambiente.

También es necesario mencionar que todas las rentas, tasas y contribuciones están regidas por un marco legal, las cuales comprenden leyes, decretos y ordenanzas, para el caso puntual de la unidad de rentas, el estatuto de rentas el cual se expide mediante la ordenanza 816 del 2017 y sus modificaciones ordenanza 842 del 2018, ordenanza 853 del 2019, ordenanza 885 del 2020, ordenanza 892 del 2021. y la ordenanza 965 del 2023.

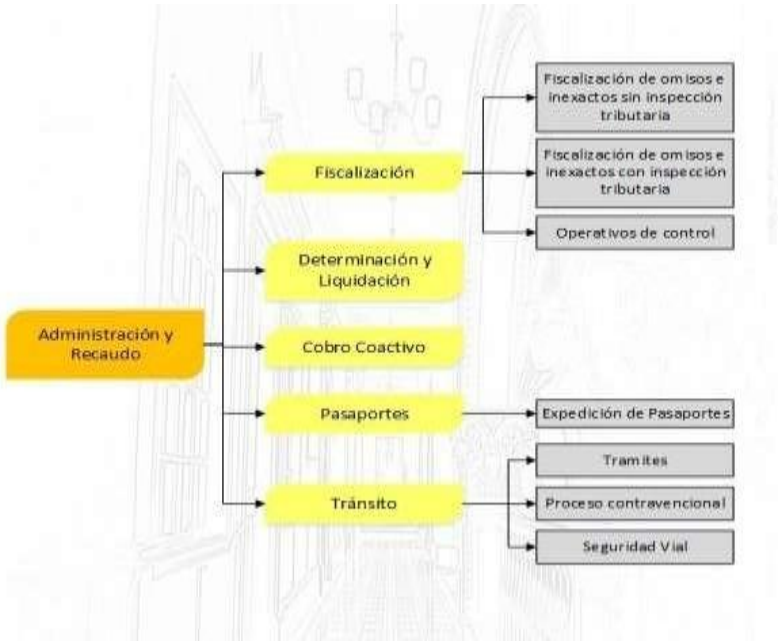
Además del manual de cartera el cual se adopta mediante decreto 575 del 26 de octubre del 2021, las ordenanzas y decretos antes mencionados es donde se encuentra escrito el cómo, cuando, a quien y que se debe cobrar en cuestión de las rentas departamentales.

Análisis del contexto interno: Para este análisis, fue necesario hablar con diferentes funcionarios acerca de las funciones que ejercen diariamente dentro de la unidad, y así poder

entender cómo funciona cada uno de los procedimientos asociados al proceso principal de la unidad, además de revisar la documentación existente en la plataforma Almera[17] en la cual se encuentra la documentación de los procedimientos los cuales mencionaremos a continuación:

Figura 15

Mapa de procesos unidad de rentas



Fuente: https://sgi.caldas.gov.co/sgi/seguimiento/?nosgim

45 Sistema de gestión integral de la gobernación de Caldas en el cual se encuentra la información de los procesos y procedimientos de la entidad https://sgi.caldas.gov.co/sgi/seguimiento/?nosgim

Procesos

Administración y Recaudo

Formular políticas y estrategias para la eficiente administración tributaria del Departamento de Caldas, a través de la implementación de mecanismos que fortalezcan el recaudo, la gestión de cobro, la liquidación y fiscalización de estos, con el propósito de incrementar el recaudo de los impuestos, disminuir la cartera y prevenir la evasión de los impuestos [18]

Impuestos Administrados por la unidad de rentas

Impuesto vehicular

Impuesto al consumo de cigarrillos, cervezas vinos y licores

Impuesto Sobretasa a la Gasolina

Impuesto Deguello ganado mayor

Impuesto estampillas departamentales

Impuesto de Registro

Procedimientos

Operativos de fiscalización y control

El objetivo de este procedimiento es ejecutar los procedimientos administrativos establecidos por las disposiciones legales ante las entidades o personal que no acredite el paz y salvo de los productos que causen el impuesto al consumo dentro del Departamento, y demás actividades relacionadas [18].

[18] Sistema de gestión integral de la gobernación de Caldas en el cual se encuentra la información de los procesos y procedimientos de la entidad https://sgi.caldas.gov.co/sgi/seguimiento/?nosgim

Grupo de determinación y liquidación

Adelantar gestiones de determinación y liquidación de las rentas a favor de la Gobernación de Caldas, utilizando para ello los medios establecidos en la normatividad vigente[19].

Cobro Coactivo

Adelantar gestiones de cobro de las acreencias y obligaciones a favor de la Gobernación de Caldas, utilizando para ello los medios coercitivos establecidos en la normatividad vigente [19].

Licencias de Conducción

Habilitar y expedir a los usuarios por medio de un documento público de carácter personal e intransferible la autorización para la conducción de vehículos con validez en todo el territorio nacional [19].

Tramites Vehículos

Vigilar, orientar, realizar e inspeccionar los procesos de desarrollo de tramites de vehículos que se prestan en la Unidad de Tránsito [19]

Expedición de Pasaportes

Realizar el proceso de expedición de pasaportes con la validación de los requisitos exigidos por la cancillería y revisión de la documentación legítima para el trámite [19]

[19] Sistema de gestión integral de la gobernación de Caldas en el cual se encuentra la información de los procesos y procedimientos de la entidad https://sgi.caldas.gov.co/sgi/seguimiento/?nosgim

Ahora pasaremos a la identificación del riesgo asociado a los procesos y procedimientos de la unidad de rentas, para ello nos basaremos en el literal 6.4.2 de la norma iso 31000:2018

Se realiza un análisis mediante una matriz de riesgos la cual nos permite identificar el riesgo, analizarlo y valorarlo, además de que mediante unas fórmulas nos permite calcular la zona de riesgo entre alta media y baja de la siguiente manera

Se identifica el proceso, y sobre este proceso se definen cierta información asociada a cada una de las entradas, actividades, la salida esperada, la causa o amenaza, la consecuencia o riesgo asociado, teniendo en cuenta esto se calcula la frecuencia con la siguiente tabla

Tabla 1

Tabla de frecuencia de riesgos

FRECUENCIA (20%)			365 días o menos
No.	**Rango**	**Formula**	
3	Alta	Entre > 0,5	# de Veces que ocurre la actividad/# días trabajados al año
2	Media	Entre <= 0,5 y >0,2	
1	Bajo	Entre <=0,2	

Para el impacto se utiliza los siguientes criterios:

Tabla 2

Tabla de impacto de riesgos

IMPACTO (50%)		
No.	**Rango**	**Criterio**
3	**Severo**	Supera o incumple el rango permitido por los requisitos establecidos (Normatividad Legal - Acuerdos - Disposiciones establecidas por la entidad o partes interesadas)
2	**Moderado**	Se encuentra dentro de los rangos o parametros establecidos (Normatividad Legal - Acuerdos - Disposiciones establecidas por la entidad o partes interesadas)
1	**Leve**	Supera las expectativas de los rangos o parametros establecidos (Normatividad Legal - Acuerdos - Disposiciones establecidas por la entidad)

Para el alcance utilizamos la siguiente tabla:

Tabla 3

Tabla de criterio de los riesgos

No.	**Rango**	**Criterio**
3	**Global**	Eventos que Superan los limites del área donde se ejecutan las actividades propias de la entidad
2	**Local**	Eventos que están dentro de los límites donde se ejecutan las actividades propias de la entidad
1	**Puntual**	Eventos que suceden puntualmente y que se pueden tratar dentro de los límites donde se ejecutan las actividades propias de la entidad

Con esta información se construye la matriz de riesgos asociada a la unidad de rentas del departamento de Caldas.

4.2 Con relación al objetivo específico 2

Políticas de seguridad de la información

4.2.1 Introducción

La seguridad de la información es uno de los principales factores para el cumplimiento de las metas pactadas por la unidad de rentas en cada uno de los diferentes procesos que se tienen a cargo dentro del departamento de Caldas es por esto que esta política de seguridad establece los lineamientos para poder a futuro cumplir con los requisitos de la norma ISO 27001:2022.

4.2.2 Alcance

Esta política se aplica a todos los activos de información, procesos, personal y sistemas relacionados con la unidad de rentas de la gobernación de Caldas y sus colaboradores

4.2.3 Compromiso

El jefe de la unidad de rentas de la gobernación de Caldas se compromete a:

Apoyar la implementación y cumplimiento de las políticas establecidas en este documento.

Gestionar los recursos adecuados para dar cumplimiento a las políticas de seguridad de la información.

Realizar seguimiento periódico a la implementación y cumplimiento de las políticas de seguridad de la información además de realizar las respectivas correcciones y sanciones necesarias.

4.2.4 Políticas

Políticas de control de la organización

El documento de políticas de la información será compartido a todos los interesados (funcionarios, contratistas y terceros) de la unidad de rentas del departamento, con previa aprobación del jefe de rentas, en los grupos de WhatsApp de cada área, o por el canal de comunicación que tengan establecido; además se les enviará al drive que cada uno tiene asociado a su correo institucional.

El jefe de la unidad de rentas a través del personal designado, deberá realizar seguimiento y control permanente al sistema de gestión de seguridad de la información y que se lleven a cabo todas las políticas establecidas.

El jefe de TI debe controlar el acceso físico a las salas donde estén almacenados dispositivos de tecnologías (Data Center, racks, switches, routers, etc); únicamente lo pueden hacer personas autorizadas por la unidad de sistemas.

El jefe de TI debe controlar el acceso lógico a los computadores de la unidad de rentas, los funcionarios que no les pertenece o no utilizan esos equipos, no pueden ingresar a ellos, de igual manera todos deben tener un usuario y contraseña para ingresar al sistema.

La unidad de sistemas debe estructurar un documento con los procesos a seguir cuando se presenten incidentes de seguridad, los integrantes que pertenecen a este grupo de respuesta a incidentes, deben tener un rol asignado.

La unidad de sistemas debe dar respuesta a los incidentes, de conformidad con los procedimientos a seguir en el documentado previamente diligenciado.

Es necesario por parte de la unidad de sistemas, recopilar, identificar y preservar la evidencia relacionada con eventos de seguridad, para poder dar solución y rapidez en el menor tiempo posible en un evento recurrente.

La unidad de rentas de debe tener protegida la información contra pérdida, destrucción, falsificación, acceso no autorizado y cualquier tipo de ataque informático (ransomware, malware, virus, etc).

Cuando se finalice el contrato o la vinculación directa con la unidad de rentas, es deber de cada funcionario informar al administrador de los sistemas de información, con el fin de inactivar todas las cuentas asociadas al mismo.

Es obligación de la unidad de sistemas revisar periódicamente las políticas de seguridad y mirar si se les está dando cumplimiento por parte de los empleados (de planta y contratistas)

Políticas de funcionarios, contratistas y colaboradores

El personal de TI debe capacitar a los funcionarios de la unidad de rentas, para concientizarlos y de las buenas prácticas de seguridad que deben llevar a cabo en el trabajo.

Se debe abrir un proceso disciplinario a las personas que incumplan o cometan violaciones a las políticas de seguridad establecidas por la unidad de sistemas.

Debe haber un acuerdo de confidencialidad y no divulgación entre la unidad de sistemas y los empleados que manejen datos sensibles, para proteger de una manera segura y que no sea filtrada o divulgada a terceros la información.

Si existe trabajo remoto, se debe tomar las medidas de seguridad necesarias para que personas ajenas a la gobernación no intercepten o accedan a la información privada y relevante que maneja la unidad.

Si alguno de los empleados de la organización debe realizar las funciones inherentes al cargo que desempeña de manera remota y estas implican conectarse a la infraestructura de la red de la gobernación de Caldas, debe hacerlo a través de una VPN y su equipo debe contar con antivirus y Sistema operativo licenciado

El personal de la unidad de rentas, debe informar inmediatamente a la unidad de sistemas sobre eventos sospechosos (correos, enlaces, archivos, etc), a través de los canales de comunicación establecidos previamente.

Después de finalizar el contrato, la persona a cargo del proceso ejecutado durante el mismo, debe de entregar toda la información la cual fue procesada en ejercicio de sus funciones en medio magnético al supervisor del contrato.

Políticas de control de acceso físico

Se debe establecer perímetros y zonas de restricción a empleados y terceros para que no ingresen sin permiso a áreas no permitidas (rack, data center, etc)

Las zonas restringidas deben estar protegidas por los controles de entrada

Las instalaciones deben tener cámaras de seguridad para estar monitoreando continuamente y detectar el acceso de personal no autorizado.

Debe estar establecido por parte de TI, el escritorio y pantalla limpia; son normas que deben acatar los empleados de mantener adecuadamente su puesto de trabajo, papeles, medios de almacenamiento extraíbles, no deben permanecer.

El equipo de cómputo debe estar en punto seguro, bien situado y de forma que no ocurra un accidente.

Las instalaciones deben estar protegidas contra cortes de energía, para prevenir pérdida de información o daño físico de los equipos (estabilizadores de voltaje, ups, etc)

Los dispositivos de almacenamiento desde el momento de su adquisición deben de estar debidamente registrados en el inventario además de que persona o área será la encargada de darle el debido uso al dispositivo.

En caso de que se presente alguna falla de energía eléctrica se debe contar con un sistema para restablecer el servicio.

Antes de asignar un equipo de cómputo el cual se ha utilizado anteriormente por otro funcionario se debe de realizar copia de seguridad de la información del mismo, posteriormente realizar una instalación limpia del sistema operativo y aplicaciones.

Políticas de control tecnológico

Establecer pruebas de auditoría a los diferentes sistemas de información, por entidades externas con la autorización de la unidad de sistemas.

Informar el resultado de las pruebas realizadas a las personas interesadas(desarrolladores, jefes de área).

Los cambios realizados a los sistema de información deben ser gestionados mediante la plataforma dispuesta para ellos, de cada uno de los proveedores de los sistemas de información, además de que deben ser previamente analizados y aprobados por el jefe de la unidad de rentas o jefe de área.

Los entornos de desarrollo, pruebas y producción de los sistemas de información realizados por funcionarios o contratistas de la unidad de rentas deben estar separados y debidamente protegidos.

El líder TI de la unidad de rentas debe realizar el seguimiento a las etapas de analisis, diseño, implementacion y puesta en marcha de los sistemas de información subcontratados por la unidad de rentas

Se debe definir e implementar las pruebas de seguridad en todas las fases del ciclo de vida del desarrollo

Los sistemas de información propios y subcontratados de la unidad de rentas deben cumplir con los principios de codificación segura.

Los desarrollos de sistemas de información deben de estar debidamente documentados, en todas sus etapas de desarrollo cumpliendo con los principios de la ingeniería segura.

Los requerimientos de seguridad para la adquisición o desarrollo de aplicaciones debe de estar definido, aprobado y documentado.

El proceso para el desarrollo de software debe de estar definido y regulado.

La unidad de sistemas de la gobernación de Caldas debe restringir el acceso a sitios web según las necesidades de la unidad de rentas.

La unidad de sistemas debe garantizar que las redes y los dispositivos de la red deben de estar asegurados, gestionados y controlados para proteger la información de los sistemas y aplicaciones

Los equipos usados por los contratistas de la unidad de rentas deben de contar con antivirus y sistema operativo debidamente licenciado, para poder tener acceso a la red de la gobernación de Caldas.

Los funcionarios o contratistas de la unidad de sistemas son los únicos autorizados para instalar aplicaciones en los equipos de cómputo de la unidad de rentas

El uso de programas con capacidades de cambiar o anular procesos del sistema, deben contar con privilegios de usuario administrador.

Se debe dar seguimiento a los sucesos anómalos en la red, en los diferentes sistemas y aplicaciones utilizadas en la unidad de rentas de posibles amenazas o incidentes de seguridad.

Debe haber un registro de todas las actividades, anomalías, sospechas e incidentes, entre otros, y estos se deben guardar para su posterior análisis.

La información debe estar disponible siempre, por eso se deben establecer sistemas de backups autosuficientes para el momento que se requiera.

La unidad de sistemas debe verificar que las copias de seguridad se hagan periódicamente y revisar que se estén ejecutando correctamente sin ningún percance.

Se requieren mantener actualizados todos los equipos, redes, software y sistemas, que almacenen o compartan información sensible

Tener mucho cuidado y estar seguros de la información que se elimina de cualquier medio de almacenamiento, ya que este proceso se realiza únicamente cuando ya no se hace uso de ella

Se deben establecer medidas de seguridad y configuraciones fuertes para los sistemas informáticos, hardware, software y se deben documentar y monitorear constantemente

La unidad de sistemas debe estar actualizada en cuanto a las vulnerabilidades que salen cada día y estar con las herramientas de software y hardware disponibles para atacarlas y contrarrestarlas

La unidad de sistemas debe implementar un software contra malware y virus que protejan los equipos de cómputo y por ende la red de la gobernación, también los funcionarios deben tomar conciencia de la implicación que tiene el malware en un sistema informático.

La unidad de sistemas debe tener el control total de las personas que hacen uso de los sistemas informáticos en la unidad de rentas, implementando nuevas técnicas de autenticación, basadas en accesos y restricciones

El acceso al código fuente de los diferentes softwares de la gobernación, para leer, escribir, modificar, se debe gestionar apropiadamente

El acceso a la información debe ser con previa autorización y autenticación, lo mismo la restricción de la misma; debe estar establecida en las políticas de control de acceso

El control de acceso total a los diferentes sistemas debe estar a cargo de personal restringido, seleccionado y privilegiado.

Se deben proteger todos los equipos de punto final conectados a la red de la unidad de rentas, para proteger la información almacenada, procesada o accesible

Capítulo 5 Conclusiones

-Implementar un sistema de seguridad de la información es una decisión estratégica que puede tener numerosos beneficios, desde la protección de datos sensibles hasta la mejora de la confianza del cliente y la continuidad del negocio. Es fundamental que la unidad de rentas reconozca la importancia de la seguridad de la información y asignen los recursos adecuados para su implementación y mantenimiento continuo.

-El documento desarrollado, establece claramente las medidas que debe tener en cuenta la unidad de rentas, implementarlas y ponerlas en práctica a través de un sistema de gestión de seguridad de la información, lo que ayuda a alinear los esfuerzos para la implementación, con las necesidades y expectativas de los líderes de las diferentes dependencias de la unidad de rentas de la Gobernación de Caldas.

-Ayudará a identificar y mitigar los riesgos de seguridad, como brechas de seguridad, ataques cibernéticos, pérdida de datos y violaciones de la privacidad. Esto puede ayudar a minimizar el impacto financiero y reputacional en toda la unidad de rentas de la Gobernación de Caldas

Capítulo 6 Recomendaciones

Realizar la documentación de todos los procedimientos realizados en la unidad de rentas departamentales para cada una de las rentas administradas por el departamento en sus diferentes etapas.

Publicar las políticas de seguridad de la información en lugar de acceso a todos los interesados de la unidad de rentas los procedimientos asociados a cada una de las oficinas internas de la unidad de rentas

Realizar jornadas de concientización acerca del buen uso de la información y de la importancia del manejo adecuado de los sistemas que la contienen.

Tener en cuenta el análisis de riesgo realizado y tomar las medidas pertinentes para el tratamiento de los riesgos

Referencias

Congreso de la República de Colombia. (s/f). Gov.co. Recuperado el 17 de abril de 2024. Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

(S/f). Redalyc.org. Recuperado el 17 de abril de 2024, de https://www.redalyc.org/pdf/922/92218768002.pdf

Ciberseguridad en Colombia y el mundo: 10 cifras y datos. (2021, febrero 9).Restablecer Marketing Digital. https://resetmarketingdigital.com/ciberseguridad-en-colombia-y-mundo-cifras

Congreso de la República de Colombia. (s/f). Gov.co. Recuperado el 17 de abril de 2024 Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial 45.587 de 7 de octubre de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (s/f). Gov.co. Recuperado el 17 de abril de 2024 Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

Asamblea Departamental de Caldas (2022). Gov.co. Por la cual se expide el estatuto de rentas del departamento de caldas y se dictan otras disposiciones.

https://site.caldas.gov.co/documentos-secretaria-de-hacienda/2942-ordenanza-816-estatuto-de-rentas

Decreto 1377 de 2013 - Gestor Normativo. (s/f). Gov.co. Recuperado el 17 de abril de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

El peor enemigo de la seguridad informática en la empresa son los propios empleados. (2017, abril 4). SOFECOM, Servicios Informáticos Para Empresas; SOFECOM. https://sofecom.com/peor-enemigo-de-la-seguridad-informatica/

GlobalSign (10 de enero de 2013). Tres Ciberataques que desafiaron a América Latina en 2022. https://www.globalsign.com/es/blog/tres-ciberataques-que-desafiaron-america-latina-en-2022

Jiménez, M. M. (s/f). Vulnerabilidades que afectan la seguridad de la información. Piranirisk.com. Recuperado el 17 de abril de 2024, de https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

Juliá, S. (2017, enero 18). 5 riesgos de seguridad informática que deberías evitar. Informática para empresas. https://www.gadae.com/blog/riesgos-de-seguridad-informatica/

Legro, A. (2024, abril 2). Ataques informáticos: Causas y 15 Tipos de Ciberataques. WIN Empresas. https://winempresas.pe/blog/ataques-informaticos-causas-y-12-tipos-de-ciberataques

Ley 1266 de 2008 - Gestor Normativo. (s/f). Gov.co. Recuperado el 17 de abril de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 17 de abril de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Mancuzo, G. (2022, abril 12). ¿Qué es un riesgo en Ciberseguridad? Definición y tipos. Ciberseguridad; Ciberseguridad Tips. https://ciberseguridadtips.com/que-es-un-riesgo-en-ciberseguridad-definicion-causas

Martínez Vargas, D. P. (2021) .Ataques cibernéticos más frecuentes en las mipymes de Colombia durante el periodo 2020 - 2021 de la pandemia covid-19. [Monografía]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/51471

Norma ISO 27001. (s/f). Norma ISO 27001. Recuperado el 17 de abril de 2024, de https://normaiso27001.es

Normatividad sobre delitos informáticos. (2017, julio 25). Policía Nacional de Colombia. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Pachón, C.(s.f.). 10 reconocidas instituciones de Colombia hackeadas en el 2022. NSIT SAS. Recuperado el 13 de marzo de 2022 de https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/

Pirateque, P. y Ramírez, S. (2022) . El Riesgo de los Ciberataques para Colombia. Boletín Estratégico Multidisciplinar. https://esici.edu.co/wp-content/uploads/2023/04/Boleti%CC%81n-05-V5.pdf

International Organization for Standardization. (2018). *ISO 31000:2018 - Risk management - Guidelines*. Recuperado de https://www.iso.org/standard/65694.html

(S/f). https://www.iebschool.com/blog/. Recuperado el 20 de abril de 2024, de https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

(S/f). https://masterenciberseguridadonline.es/ Recuperado el 29 de junio de 2024, de https://masterenciberseguridadonline.es/inyeccion-sql-ejemplos/

Revista Tecnológica ESPOL –RTE, Vol. 28, N. 5, 492-507, (Diciembre2015)

https://rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co

;

ANEXOS

FORMATO IDENTIFICACION Y VALORACION DE RIESGOS										
IDENTIFICACION DEL RIESGO						ANALISIS DE CALIFICACION Y VALORACION				
PROCESO	ENTRADA	ACTIVIDAD	SALIDA (Tangible)	AMENAZA / CAUSA	CONSECUENCIA / RIESGO	FRECUENCIA	IMPACTO	ALCANCE	CALIFICACION (9+10+11)	ZONA DE RIESGO
Administracion y recaudo	Solicitud de liquidacion de impuesto vehicular	Generacion de Decalracion de Impuesto vehicular	Declaracion de impuesto vehicular lista para pago sea virtual o presencial	**Declaracion generada con informacion incorrecta**	Pago de lo no debido por el impuesto vehicular	0,1	1	3	1,4	BAJO
Administracion y recaudo	Solicitud de generacion de proceso de actos administrativos de impuesto vehicular.	Generacion de proceso masivo de cobro de impuesto vehicular	Documento o documentos de alguno de los actos administrativos generados dentro del proceso de cobro coactivo o persuasivo con informacion acecra del proceso generado	**Generar un proceso a un tercero que no es debido**	Desgaste administrativo, dado que se generarn derechos de peticion, falta de credibilidad de la entidad.	0	1	3	1,4	BAJO
Administracion y recaudo	Alistamiento para envio de procesos masivos de cobro	Envio de actos administrativos a los contribueyntes de impuesto vehicular	Base de datos de envio y los documentos impresos y debidamiente organizados para el envio mediante la empresa de correo	**Perdida de documentos, Envios entregados a direccion errada, porcentaje de devolucion de envio altos**	Prescripcion de la deuda, perdida de la competencia para el cobro del impuesto.	0,3	3	3	2,5	MEDIO
Administracion y recaudo	Ingreso de informacion a sistemas de informacion	Creacion de terceros, en los sistemas de recaudo de la gobernacion	Tercero creado dentro del sistema de recaudo de alguno de los impuestos administardos por la unidad de rentas	**Ingreso de informacion erronea**	Daño de la reputacion de alguna persona, cobro indebido de los impuestos	0,1	2	2	1,6	BAJO
Administracion y recaudo	Pago de impuestos en oficina	Recaudo en efectivo a traves de bancos autorizados	El pago ha sido exitoso y puede verse reflejado en la plataform	**Perdida de conexion con los servidores**	Menos ingresos por las rentas en el departamento	0	3	3	2,4	MEDIO
Administracion y recaudo	Pago de impuestos a traves del boton de pagos pse	Recaudo a traves del boton de pagos pse de las plataformas dispuestas para ello	El pago ha sido exitoso y puede verse reflejado en la plataform	**Fallas en la red, problemas con el servidor de la pasarela de pagos**	Menos ingresos por las rentas en el departamento	0,1	3	3	2,4	MEDIO
Tecnologias de informacion	Entrega de informacion de la unidad de rentas por parte de los contratistas al finalizar un contrato	Entrega del puesto al finalizar el contrato al supervisor	Informe de las actividades ejecutadas durante el contrato con los respectivos soportes	No se haga la entrega de las evidencias al finalizar el contrato	Perdida de informacion , no continuidad de los procesos	0,2	3	2	2,1	MEDIO

FORMATO IDENTIFICACION Y VALORACION DE RIESGOS										
IDENTIFICACION DEL RIESGO						ANALISIS DE CALIFICACION Y VALORACION				
PROCESO	ENTRADA	ACTIVIDAD	SALIDA (Tangible)	AMENAZA / CAUSA	CONSECUENCIA / RIESGO	FRECUENCIA	IMPACTO	ALCANCE	CALIFICACION (9+10+11)	ZONA DE RIESGO
Tecnologias de informacion	Respaldo de la informacion equipos de computo de la unidad de Rentas	Realizacion copias de seguridad periodicas	Copia de seguridad en disco duro extraible o en la nube	Daño del disco duro, no realizar copia de seguridad de los dispositivos	Perdida de informacion, no cumplimiento de los indicadores, perdida de tiempo y la confianza	0,2	3	2	2,1	MEDIO
Tecnologias de informacion	Informacion correo electronico institucional	Realizacion copias de seguridad correo electronico	Archivo con la informacion contenida en el correo electronico y el drive del mismo	Al finalizar la relacion contractual el correo queda inactivo y sin acceso a	Perdida de informacion historica importante para los procesos de la unidad de Rentas	0	2	3	1,9	BAJO
Recursos Humanos	No cumplimiento de Horario	Atencion al publico	Contribuyente atendido satisfactoriamente	Contratistas, los cuales por su tipo de contrato no deben cumplir horarios	Afectacion directa del recaudo del impuesto a cargo, mala imagen institucional	0,2	2	2	1,6	BAJO

Políticas de seguridad de la información unidad de rentas versión 1.0

Introducción

La seguridad de la información es uno de los principales factores para el cumplimiento de las metas pactadas por la unidad de rentas en cada uno de los diferentes procesos que se tienen a cargo dentro del departamento de Caldas es por esto que esta política de seguridad establece los lineamientos para poder a futuro cumplir con los requisitos de la norma ISO 27001:2022.

Alcance
Esta política se aplica a todos los activos de información, procesos, personal y sistemas relacionados con la unidad de rentas de la gobernación de Caldas y sus colaboradores

Compromiso
El jefe de la unidad de rentas de la gobernación de Caldas se compromete a:

- Apoyar la implementación y cumplimiento de las políticas establecidas en este documento.
- Gestionar los recursos adecuados para dar cumplimiento a las políticas de seguridad de la información.
- Realizar seguimiento periódico a la implementación y cumplimiento de las políticas de seguridad de la información además de realizar las respectivas correcciones y sanciones necesarias.

Políticas
Políticas de control de la organización

- El documento de políticas de la información será compartido a todos los interesados (funcionarios, contratistas y terceros) de la unidad de rentas del departamento, con previa aprobación del jefe de rentas, en los grupos de WhatsApp de cada área, o por el canal de comunicación que tengan establecido; además se les enviará al drive que cada uno tiene asociado a su correo institucional.
- El jefe de la unidad de rentas a través del personal designado, deberá realizar seguimiento y control permanente al sistema de gestión de seguridad de la información y que se lleven a cabo todas las políticas establecidas.
- El jefe de TI debe controlar el acceso físico a las salas donde estén almacenados dispositivos de tecnologías (Data Center, racks, switches, routers, etc); únicamente lo pueden hacer personas autorizadas por la unidad de sistemas.
- El jefe de TI debe controlar el acceso lógico a los computadores de la unidad de rentas, los funcionarios que no les pertenece o no utilizan esos equipos, no pueden ingresar a ellos, de igual manera todos deben tener un usuario y contraseña para ingresar al sistema.
- La unidad de sistemas debe estructurar un documento con los procesos a seguir cuando se presenten incidentes de seguridad, los integrantes que pertenecen a este grupo de respuesta a incidentes, deben tener un rol asignado.
- La unidad de sistemas debe dar respuesta a los incidentes, de conformidad con los procedimientos a seguir en el documentado previamente diligenciado.
- Es necesario por parte de la unidad de sistemas, recopilar, identificar y preservar la evidencia relacionada con eventos de seguridad, para poder dar solución y rapidez en el menor tiempo posible en un evento recurrente.
- La unidad de rentas de debe tener protegida la información contra pérdida, destrucción, falsificación, acceso no autorizado y cualquier tipo de ataque informático (ransomware, malware, virus, etc).

- Cuando se finalice el contrato o la vinculación directa con la unidad de rentas, es deber de cada funcionario informar al administrador de los sistemas de información, con el fin de inactivar todas las cuentas asociadas al mismo.
- Es obligación de la unidad de sistemas revisar periódicamente las políticas de seguridad y mirar si se les está dando cumplimiento por parte de los empleados (de planta y contratistas)

Políticas de funcionarios, contratistas y colaboradores

- El personal de TI debe capacitar a los funcionarios de la unidad de rentas, para concientizarlos y de las buenas prácticas de seguridad que deben llevar a cabo en el trabajo.
- Se debe abrir un proceso disciplinario a las personas que incumplan o cometan violaciones a las políticas de seguridad establecidas por la unidad de sistemas.
- Debe haber un acuerdo de confidencialidad y no divulgación entre la unidad de sistemas y los empleados que manejen datos sensibles, para proteger de una manera segura y que no sea filtrada o divulgada a terceros la información.
- Si existe trabajo remoto, se debe tomar las medidas de seguridad necesarias para que personas ajenas a la gobernación no intercepten o accedan a la información privada y relevante que maneja la unidad.
- Si alguno de los empleados de la organización debe realizar las funciones inherentes al cargo que desempeña de manera remota y estas implican conectarse a la infraestructura de la red de la gobernación de Caldas, debe hacerlo a través de una VPN y su equipo debe contar con antivirus y Sistema operativo licenciado
- El personal de la unidad de rentas, debe informar inmediatamente a la unidad de sistemas sobre eventos sospechosos (correos, enlaces, archivos, etc), a través de los canales de comunicación establecidos previamente.
- Después de finalizar el contrato, la persona a cargo del proceso ejecutado durante el mismo, debe de entregar toda la información la cual fue procesada en ejercicio de sus funciones en medio magnético al supervisor del contrato.

Políticas de control de acceso físico

- Se debe establecer perímetros y zonas de restricción a empleados y terceros para que no ingresen sin permiso a áreas no permitidas (rack, data center, etc)
- Las zonas restringidas deben estar protegidas por los controles de entrada
- Las instalaciones deben tener cámaras de seguridad para estar monitoreando continuamente y detectar el acceso de personal no autorizado.
- Debe estar establecido por parte de TI, el escritorio y pantalla limpia; son normas que deben acatar los empleados de mantener adecuadamente su puesto de trabajo, papeles, medios de almacenamiento extraíbles, no deben permanecer.
- El equipo de cómputo debe estar en punto seguro, bien situado y de forma que no ocurra un accidente.
- Las instalaciones deben estar protegidas contra cortes de energía, para prevenir pérdida de información o daño físico de los equipos (estabilizadores de voltaje, ups, etc)
- Los dispositivos de almacenamiento desde el momento de su adquisición deben de estar debidamente registrados en el inventario además de que persona o área será la encargada de darle el debido uso al dispositivo.
- En caso de que se presente alguna falla de energía eléctrica se debe contar con un sistema para restablecer el servicio.
- Antes de asignar un equipo de cómputo el cual se ha utilizado anteriormente por otro funcionario se debe de realizar copia de seguridad de la información del mismo, posteriormente realizar una instalación limpia del sistema operativo y aplicaciones.

Políticas de control tecnológico

- Establecer pruebas de auditoría a los diferentes sistemas de información, por entidades externas con la autorización de la unidad de sistemas.
- Informar el resultado de las pruebas realizadas a las personas interesadas(desarrolladores, jefes de área).
- Los cambios realizados a los sistema de información deben ser gestionados mediante la plataforma dispuesta para ellos, de cada uno de los proveedores de los sistemas de información, además de que deben ser previamente analizados y aprobados por el jefe de la unidad de rentas o jefe de área.
- Los entornos de desarrollo, pruebas y producción de los sistemas de información realizados por funcionarios o contratistas de la unidad de rentas deben estar separados y debidamente protegidos.
- El líder TI de la unidad de rentas debe realizar el seguimiento a las etapas de analisis, diseño, implementacion y puesta en marcha de los sistemas de información subcontratados por la unidad de rentas
- Se debe definir e implementar las pruebas de seguridad en todas las fases del ciclo de vida del desarrollo
- Los sistemas de información propios y subcontratados de la unidad de rentas deben cumplir con los principios de codificación segura.
- Los desarrollos de sistemas de información deben de estar debidamente documentados, en todas sus etapas de desarrollo cumpliendo con los principios de la ingeniería segura.
- Los requerimientos de seguridad para la adquisición o desarrollo de aplicaciones debe de estar definido, aprobado y documentado.
- El proceso para el desarrollo de software debe de estar definido y regulado.
- La unidad de sistemas de la gobernación de Caldas debe restringir el acceso a sitios web según las necesidades de la unidad de rentas.
- La unidad de sistemas debe garantizar que las redes y los dispositivos de la red deben de estar asegurados, gestionados y controlados para proteger la información de los sistemas y aplicaciones
- Los equipos usados por los contratistas de la unidad de rentas deben de contar con antivirus y sistema operativo debidamente licenciado, para poder tener acceso a la red de la gobernación de Caldas.
- Los funcionarios o contratistas de la unidad de sistemas son los únicos autorizados para instalar aplicaciones en los equipos de cómputo de la unidad de rentas
- El uso de programas con capacidades de cambiar o anular procesos del sistema, deben contar con privilegios de usuario administrador.
- Se debe dar seguimiento a los sucesos anómalos en la red, en los diferentes sistemas y aplicaciones utilizadas en la unidad de rentas de posibles amenazas o incidentes de seguridad.
- Debe haber un registro de todas las actividades, anomalías, sospechas e incidentes, entre otros, y estos se deben guardar para su posterior análisis.
- La información debe estar disponible siempre, por eso se deben establecer sistemas de backups autosuficientes para el momento que se requiera.
- La unidad de sistemas debe verificar que las copias de seguridad se hagan periódicamente y revisar que se estén ejecutando correctamente sin ningún percance.
- Se requieren mantener actualizados todos los equipos, redes, software y sistemas, que almacenen o compartan información sensible
- Tener mucho cuidado y estar seguros de la información que se elimina de cualquier medio de almacenamiento, ya que este proceso se realiza únicamente cuando ya no se hace uso de ella
- Se deben establecer medidas de seguridad y configuraciones fuertes para los sistemas informáticos, hardware, software y se deben documentar y monitorear constantemente

- La unidad de sistemas debe estar actualizada en cuanto a las vulnerabilidades que salen cada día y estar con las herramientas de software y hardware disponibles para atacarlas y contrarrestarlas
- La unidad de sistemas debe implementar un software contra malware y virus que protejan los equipos de cómputo y por ende la red de la gobernación, también los funcionarios deben tomar conciencia de la implicación que tiene el malware en un sistema informático.
- La unidad de sistemas debe tener el control total de las personas que hacen uso de los sistemas informáticos en la unidad de rentas, implementando nuevas técnicas de autenticación, basadas en accesos y restricciones
- El acceso al código fuente de los diferentes softwares de la gobernación, para leer, escribir, modificar, se debe gestionar apropiadamente
- El acceso a la información debe ser con previa autorización y autenticación, lo mismo la restricción de la misma; debe estar establecida en las políticas de control de acceso
- El control de acceso total a los diferentes sistemas debe estar a cargo de personal restringido, seleccionado y privilegiado.
- Se deben proteger todos los equipos de punto final conectados a la red de la unidad de rentas, para proteger la información almacenada, procesada o accesible

EL SUSCRITO JEFE DE LA UNIDAD DE RENTAS DEL DEPARTAMENTO DE CALDAS
HACE CONSTAR QUE:

Que durante el trabajo de grado elaborado por los contratistas de la unidad de Rentas Leonardo Patiño Correa, José Fernando Gómez Sánchez y Yerson Ochoa Puerta, desarrollaron unos documentos de análisis de la unidad de rentas orientados a los riesgos asociados a la seguridad de la información. Además, se sugirieron establecer unas políticas de seguridad de la información las cuales serán tomadas en cuenta, para posteriormente dar inicio a la implementación de un sistema de gestión de seguridad de la información en la unidad de Rentas del departamento de Caldas

Dada en Manizales a los 02 días del mes de mayo de 2024.

JOHN JAIRO GARCIA GIRALDO
Jefe Unidad de Rentas