PLAN DE GESTIÓN DE CONTINUIDAD DE NEGOCIO BASADO EN EL ESTÁNDAR ISO 22301 E ISO 27001 PARA MITIGAR LOS RIESGOS DE LOS ACTIVOS DE INFORMACIÓN EN LA SECRETARÍA DE HACIENDA DEPARTAMENTAL DEL AMAZONAS

RICARDO ANDRES CUBILLOS MORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LETICIA
2023

PLAN DE GESTIÓN DE CONTINUIDAD DE NEGOCIO BASADO EN EL ESTÁNDAR ISO 22301 E ISO 27001 PARA MITIGAR LOS RIESGOS DE LOS ACTIVOS DE INFORMACIÓN EN LA SECRETARÍA DE HACIENDA DEPARTAMENTAL DEL AMAZONAS.

RICARDO ANDRES CUBILLOS MORA

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

YENNY STELLA NUÑEZ ALVAREZ
Directora de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LETICIA
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Leticia., Fecha sustentación

DEDICATORIA

Esta dedicatoria es una manifestación de mi profundo agradecimiento y reconocimiento hacia mis padres, quienes han sido la piedra angular de mi crecimiento personal y académico. Su amor inquebrantable y su constante respaldo han sido la fuerza impulsora detrás de cada logro en mi vida.

Desde el inicio de mi trayecto educativo, mis padres han estado a mi lado, brindándome no solo su apoyo emocional, sino también su sabiduría y orientación. Cuando mis propias dudas y obstáculos amenazaban con detenerme, ellos creyeron en mí, incluso más de lo que yo podía hacerlo por mí mismo. Su confianza inquebrantable me ha dado la fuerza para perseverar y superar los desafíos que se cruzaron en mi camino. A lo largo de los años, he sido testigo de la paciencia incansable de mis padres y de su dedicación inquebrantable hacia mi educación. Han sido modelos ejemplares de trabajo duro, sacrificio y compromiso. Cada sacrificio que han hecho en su propio camino ha sido para asegurarse de que yo tenga las oportunidades que merezco.

Este proyecto que hoy presento es solo una pequeña expresión de mi gratitud hacia mis padres. Es un tributo modesto a la increíble influencia que han tenido en mi vida. Espero sinceramente que este logro los haga sentir orgullosos, aunque sé que su amor es incondicional y que su satisfacción proviene simplemente de verme crecer y prosperar.

Llevaré siempre en mi corazón las lecciones y los valores que mis padres me han inculcado. Continuaré trabajando con ahínco y determinación, con la esperanza de retribuir, en la medida de lo posible, todo lo que me han brindado. Mi camino no habría sido el mismo sin ellos, y estoy eternamente agradecido por la bendición de tener padres tan excepcionales.

Con amor y gratitud infinita.

RICARDO ANDRES CUBILLOS MORA

AGRADECIMIENTOS

Quiero destacar el valor que tiene la educación virtual en la actualidad, y en particular, la Universidad Nacional Abierta ya Distancia (UNAD), que nos ofrece una educación de calidad en un entorno flexible y accesible. Agradezco a las directivas de la UNAD por su constante dedicación en la mejora de la educación virtual y por brindarnos la oportunidad de desarrollarnos académicamente y profesionalmente.

Además, es importante reconocer la labor y el compromiso de los tutores y asesores de la UNAD, quienes han sido pieza clave en mi proceso de aprendizaje. Su dedicación y guía han sido fundamentales para alcanzar mis metas y culminar exitosamente este proyecto.

Finalmente, quiero expresar mi gratitud a mi familia, amigos y seres queridos que me han brindado su apoyo y motivación constante durante todo este proceso. Su amor y confianza en mí han sido un gran impulso para alcanzar mis objetivos y continuar en la búsqueda constante del conocimiento.

CONTENIDO

Pág.

Introducción 17
1 definición del problema 18
1.1 antecedentes del problema 18
1.2 formulación del problema 19
2 justificación 20
3 objetivos 21
3.1 objetivo general 21
3.2 objetivos específicos 21
4 marco referencial 22
4.1 marco teórico 22
4.1.1 ¿qué es la iso 22301? 22
4.1.2 ¿qué es la iso 27001? 23
4.1.3 plan de continuidad de negocio 24
4.2 gestión del plan de continuidad de negocio 25
4.2.1 etapa 1 25
4.2.2 etapa 2 25
4.2.3 etapa 3 25
4.2.4 etapa 4 25
4.2.5 etapa 5 26
4.2.6 etapa 6 26
4.3 marco conceptual 26
4.3.1 ¿qué es un plan o sistema de gestión de continuidad de negocio (sgcn)? 26
4.3.2 ¿cómo ayuda a nuestra organización implantar un sistema de gestión de continuidad de negocio? 27
4.3.3 ¿cómo elaborar un sistema de gestión de continuidad de negocio? 28
4.3.4 pasos o fases principales para la implantación: 30
determinar el alcance: 30
4.4 marco histórico 32
4.5 antecedentes o estado actual 32
4.6 marco científico o tecnológico 32
4.7 marco legal 33
4.7.1 la norma iso 22301 puede ser aplicada a todo tipo y tamaño de organizaciones que quieran: 33
4.7.2 la norma iso 22301 está organizada según la siguiente estructura: 33
5 diseño metodológico 35
5.1 determinación del alcance 35
5.2 análisis de la empresa 35
5.3 análisis de riesgos 35
5.4 plan de tratamiento de riesgos 35

5.5 determinación de la estrategia 35
5.6 identificación de escenarios de crisis 36
5.7 planes detallados de respuesta y recuperación 36
5.8 respuesta a la contingencia.....36
6 alcance y requerimientos del inventario de activos de información 37
6.1 identificacion de los factores internos y externos 37
6.1.1 actividad de la secretaria de hacienda 37
6.1.2 funciones de la secretaria de hacienda.....38
6.1.3 servicios que ofrece la secretaria de hacienda 38
6.1.4 requerimientos y activos de la secretaria de hacienda.....39
6.1.5 inventario de activos: 40
6.1.5.1 propiedad de los activos: 40
6.1.5.2 uso aceptable de los activos: 40
6.1.5.3 devolución de activos:.....40
6.1.5.4 clasificación de la información: 40
6.1.5.5 etiquetado de la información: 40
6.1.5.6 manejo de activos: 41
6.2 vincular y alinear estratégicamente 41
6.2.1 politicas de la secretaria de hacienda 41
6.2.1.1 politica del sistema de gestion 41
6.2.1.2 política de comunicaciones 42
6.2.1.3 política de seguridad de la información y seguridad digital 42
6.2.1.4 política de administración de riesgo y cumplimiento 43
6.2.1.5 política subsistema de gestión de seguridad en el trabajo sg-sst .44
6.2.1.6 políticas de uso del data center 44
7 evaluación de los riesgos e impactos a la continuidad del negocio con base a los lineamientos de la iso 22301 y la iso 27001 46
7.1 desafíos a tener en cuenta para realizar un análisis de impacto de negocio 47
7.2 puntos clave en el análisis de impacto de negocio 48
7.3 proceso para evaluacion de riesgos y sus resultados. 49
8 diseño de un plan de tratamiento de riesgos para la implementación de controles preventivos que minimicen la probabilidad de ocurrencia de las amenazas en la secretaría de hacienda departamental del amazonas. 50
8.1 plan tratamiento de riesgos de seguridad y privacidad de la informacion ...51
8.2 objetivo 52
8.3 alcance 52
8.4 proceso para el tratamiento de riesgos de seguridad y privacidad de la información 52
8.5 sensibilización institucional sobre política de seguridad de la información .53
8.6 actualizar el inventario de activos de información 54
8.7 elaborar procedimientos de seguridad de la información 55
8.8 definir metodología para la gestión de los riesgos de seguridad y privacidad de la información.....55

8.9 definir herramienta del análisis de riesgo de seguridad de la información para la implementación del riesgo 56
8.10 establecer contexto estratégico.....57
8.11 establecer equipo de trabajo con asignación responsabilidades 57
8.12 identificación de riesgos.....58
8.13 análisis de riesgos.....59
8.14 valoración de riesgos 59
8.15 evaluación de controles.....60
8.16 socialización y comunicación políticas de riesgos.....61
8.17 monitoreo y revisión al tratamiento de los riegos 61
8.18 terminología 62
8.19 administración del riesgo:.....62
8.20 activo de información: 63
8.21 análisis de riesgos:.....63
8.21.1 amenaza: 64
8.21.2 causa: 64
8.21.3 confidencialidad: 64
8.21.4 criterios del riesgo: 65
8.21.5 control: 65
8.21.6 declaración de aplicabilidad: 65
8.21.7 disponibilidad: 65
8.21.8 evento: 65
8.21.9 evitación del riesgo: 65
8.21.10 factores de riesgo: 65
8.21.11 gestión del riesgo: 66
9 políticas y medidas de seguridad.....67
9.1 objetivos comerciales: 67
9.1.1 mejorar la continuidad del negocio:.....67
9.1.2 fortalecer la confianza del cliente: 67
9.1.3 cumplir con requisitos legales y regulatorios:.....67
9.2 objetivos de seguridad de la información: 67
9.2.1 mejorar la detección de incidentes:.....67
9.2.2 optimizar la respuesta a incidentes: 67
9.2.3 garantizar la recuperación de datos críticos:.....68
9.3 requisitos de las partes interesadas: 68
9.3.1 partes interesadas internas: 68
9.3.2 partes interesadas externas: 68
9.3.3 entidades reguladoras:.....68
9.4 política general de seguridad y privacidad de la información 68
9.5 principios de seguridad que respaldan el sgsi de la secretaría de hacienda departamental del amazonas.....70
9.6 fases de implementación de políticas de seguridad de la información.....71
9.7 importancia de las políticas de seguridad de la información 71

9.8 fases de implementación de las políticas de seguridad de información 71
9.8.1 desarrollo de las políticas: 71
en esta fase la entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos: 71
9.8.2 justificación de la creación de política: 71
9.8.3 alcance: 71
9.8.4 roles y responsabilidades: 71
9.8.5 revisión de la política: 72
9.8.6 aprobación de la política: 72
9.9 cumplimiento: 72
9.10 comunicación: 72
9.11 monitoreo: 72
9.12 mantenimiento: 73
9.13 retiro: 73
9.14 políticas específicas recomendadas para la implementación de controles de seguridad de la información 73
9.14.1 organización de la seguridad de la información 73
9.15 gestión de activos 74
9.15.1 identificación de activos: 74
9.15.2 clasificación de activos: 74
9.15.3 etiquetado de la información: 74
9.15.4 devolución de los activos: 74
9.15.5 gestión de medios removibles: 74
9.15.6 disposición de los activos: 75
9.15.7 dispositivos móviles: 75
9.16 control de acceso 75
9.16.1 control de acceso con usuario y contraseña: 75
9.16.2 suministro del control de acceso: 76
9.16.3 gestión de contraseñas: 76
9.16.4 perímetros de seguridad: 76
9.16.5 áreas de carga: 76
9.17 no repudio 77
9.18 trazabilidad: 77
9.18.1 retención: 77
9.18.2 auditoría: 77
9.18.3 intercambio electrónico de información: 77
9.18.4 privacidad y confidencialidad 78
9.19 ámbito de aplicación 78
9.19.1 excepción al ámbito de aplicación de las políticas de tratamiento de datos personales 78
9.19.2 principios del tratamiento de datos personales 78
9.19.2.1 principio de la legalidad: 79
9.19.2.2 principio de finalidad: 79

9.19.2.3 principio de libertad: 79
9.19.2.4 principio de veracidad o calidad: 79
9.19.2.5 principio de transparencia: 79
9.20 principio de acceso y circulación restringida: 79
9.20.1 principio de seguridad: 79
9.20.2 principio de confidencialidad: 79
9.21 autorización del titular 80
9.21.1 deberes de los responsables del tratamiento 80
9.21.2 política de controles criptográficos 80
9.22 integridad 81
9.23 disponibilidad del servicio e información 81
9.23.1 niveles de disponibilidad: 81
9.23.2 planes de recuperación: 81
9.23.3 interrupciones: 82
9.23.4 acuerdos de nivel de servicio: 82
9.24 segregación de ambientes: 82
9.25 gestión de cambios: 83
9.26 registro y auditoría 83
9.26.1 responsabilidad: 83
9.26.2 almacenamiento de registros: 83
9.26.3 normatividad: 83
9.26.4 garantía cumplimiento: 83
9.26.5 periodicidad: 84
9.26.6 gestión de incidentes de seguridad de la información: 84
9.27 visión general: 84
9.28 definir responsables: 85
9.29 actividades: 85
9.30 documentación: 86
9.31 descripción del equipo que manejará los incidentes: 86
9.32 aspectos legales: 87
9.33 capacitación y sensibilización en seguridad de la información 88
10 conclusiones 90
11 recomendaciones 93
12 divulgación 95
bibliografía 96
anexos 100
anexo 1. Personal y dependencias 100
anexo 2. Inventario de activos 103
anexo 3. Matriz de inventario, clasificacion y riesgos de activos de informacion 107
anexo 4. Valoración de activos 107
anexo 5. Activos y valoracion cualitativa 111
anexo 6. Nomenclatura de la valoracion del riesgo 119
anexo 7. Matriz valoracion del riesgo de los activos de informacion 119
anexo 8. Gestion del riesgo y plan de tratamiento 124

LISTA DE FIGURAS E ILUSTRACIONES

Pág.

Figura 1 Fases SGCN.....30
Ilustración 1 Criterios de Clasificación 53
Ilustración 2 Criterios De Evaluación……..53

LISTA DE ANEXOS

Pág.

Anexo 1. Personal Y Dependencias 101
Anexo 2. Inventario De Activos……104
Anexo 3. Matriz De Inventario, Clasificacion Y Riesgos De Activos De Informacion……...108
Anexo 4. Valoración De Activo……..108
Anexo 5. Activos Y Valoracion Cualitativa 112
Anexo 6. Nomenclatura De La Valoracion Del Riesgo.....120
Anexo 7. Matriz Valoracion Del Riesgo De Los Activos De Informacion.....120
Anexo 8. Gestion Del Riesgo Y Plan De Tratamiento.....125

GLOSARIO

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o sami-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 20144.

Información pública reservada: Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información: Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la **ley 1712 del 2014**, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

RESUMEN

Este documento se enfoca en el diseño de un plan de gestión de continuidad de negocio, aprovechando las directrices proporcionadas por los estándares ISO 22301 e ISO 27001. El propósito central es abordar los riesgos que acechan a los activos de información pertenecientes a la Secretaría de Hacienda Departamental del Amazonas.

La estrategia se fundamenta en llevar a cabo una identificación exhaustiva de los activos de información existentes en la entidad. Esto implica una evaluación minuciosa del estado actual de estos activos. Además, se realiza un análisis meticuloso de las amenazas y riesgos potenciales que, de no ser controlados, podrían desencadenar situaciones de gran magnitud y alcance.

Sobre esta base de información, se procederá a la construcción de matrices de evaluación de riesgos individuales para cada activo de información. Estas matrices servirán como cimiento para la formulación de un sólido y eficaz plan de gestión de continuidad de negocio. El objetivo es establecer estrategias preventivas y de mitigación que anticipen y contrarresten futuras crisis y contingencias vinculadas a los activos de información.

En resumen, este proyecto aplicado se enfoca en el diseño e implementación de un plan de gestión de continuidad de negocio que se apoya en estándares internacionales reconocidos. Su alcance abarca la evaluación y control de riesgos de los activos de información de la Secretaría de Hacienda Departamental del Amazonas, con el propósito de salvaguardar su integridad y funcionamiento en el largo plazo.

Palabras clave: Activos de información, Estándares ISO 22301 e ISO 27001, Gestión de continuidad de negocio, Matrices de evaluación de riesgos, Plan de mitigación, Riesgos y amenazas.

ABSTRACT

This document focuses on the implementation of a business continuity management plan, utilizing the guidelines provided by the ISO 22301 and ISO 27001 standards. The central purpose is to address the risks facing the information assets belonging to the Departmental Treasury of the Amazon.

The strategy is grounded in conducting a thorough identification of the existing information assets within the entity. This involves a meticulous assessment of the current state of these assets. Furthermore, a meticulous analysis of potential threats and risks is performed, which, if left unchecked, could lead to situations of considerable magnitude and scope.

Upon this foundation of information, individual risk assessment matrices will be constructed for each information asset. These matrices will serve as the basis for the formulation of a robust and effective business continuity management plan. The objective is to establish preventive and mitigation strategies that anticipate and counteract future crises and contingencies linked to the information assets.

In summary, this applied project focuses on the design and implementation of a business continuity management plan supported by recognized international standards. Its scope encompasses the assessment and control of risks to the information assets of the Departmental Treasury of the Amazon, with the aim of safeguarding their integrity and operation in the long term.

Keywords: Business continuity management, Information assets, ISO 22301 and ISO 27001 standards, Mitigation plan, Risk assessment matrices, Risks and threats.

INTRODUCCIÓN

En el entorno empresarial actual globalizado y altamente interconectado, ninguna organización, independientemente de su tamaño o sector, está exenta de incidentes que puedan interrumpir su actividad y poner en peligro la continuidad del negocio. Estos incidentes pueden incluir desastres naturales, ciberataques, fallas en la infraestructura tecnológica, entre otros. Por esta razón, es fundamental contar con un Plan de Gestión de Continuidad de Negocio (PGCN) que incluya acciones de respuesta adecuadas para controlar, reducir y recuperarse de los efectos de estos eventos adversos.

La Secretaría de Hacienda Departamental del Amazonas, responsable de administrar un servidor y aproximadamente 40 ordenadores, enfrenta desafíos significativos en términos de seguridad y protección de estos activos informáticos. Estos sistemas albergan información financiera crítica de la entidad que abarca los últimos 30 años, lo que destaca la importancia de implementar un plan de continuidad de negocio sólido y efectivo basado en el estándar internacional ISO 22301. Este enfoque ayudará a minimizar los riesgos asociados y establecer mecanismos de seguridad eficientes para garantizar la resiliencia de la organización. Asimismo, la adopción del estándar ISO 27001 contribuirá a asegurar la confidencialidad, integridad y disponibilidad de la información.

En este documento, se abordará de manera exhaustiva la creación e implementación de un Plan de Gestión de Continuidad de Negocio basado en los estándares ISO 22301 e ISO 27001. Se describirán las etapas clave del proceso, tales como análisis de impacto en el negocio, evaluación de riesgos, definición de objetivos y estrategias de continuidad, y establecimiento de procedimientos de respuesta y recuperación. El objetivo principal es asegurar la continuidad de las operaciones de la Secretaría de Hacienda Departamental del Amazonas y proteger su valiosa información financiera frente a cualquier amenaza o interrupción, garantizando al mismo tiempo el cumplimiento de las normas y normas aplicables.

1 DEFINICIÓN DEL PROBLEMA

La Secretaría de Hacienda de la Gobernación del Amazonas se enfrenta actualmente a desafíos significativos en términos de seguridad y la adopción de una metodología adecuada para identificar y gestionar los riesgos asociados a los activos de información que maneja. Es crucial desarrollar e implementar un plan de gestión de continuidad de negocio, fundamentado en los estándares ISO 22301 e ISO 27001, para mitigar estos riesgos y determinar de manera precisa las posibilidades de que los daños puedan volverse irreversibles.

En el contexto actual, la ausencia de medidas de seguridad apropiadas expone la información crítica manejada por esta dependencia a riesgos considerables, lo cual puede tener serias repercusiones en la continuidad de las operaciones. La adopción de un plan de gestión de continuidad de negocio basado en normas reconocidas internacionalmente, como ISO 22301 e ISO 27001, facilitará la identificación y gestión eficiente de los riesgos asociados a los activos de información, con el propósito de prevenir y minimizar situaciones que puedan derivar en daños irreparables.

Este documento aborda la urgente necesidad de establecer un plan de gestión de continuidad de negocio fundamentado en dichos estándares, con el objetivo de salvar la información crítica gestionada por la Secretaría de Hacienda de la Gobernación del Amazonas y asegurar la continuidad de sus en un entorno seguro y protegido.

1.1 ANTECEDENTES DEL PROBLEMA

La Secretaría de Hacienda Departamental del Amazonas está estructurada en cuatro oficinas principales: Presupuesto, Contabilidad, Tesorería y Rentas, que constituyen los pilares fundamentales de esta área. Cabe resaltar que el servidor central de la Secretaría de Hacienda Departamental del Amazonas, ubicado en la división de Contabilidad, alberga información financiera crítica de la entidad, así como el software contable PCT Enterprise.

En total, alrededor de 40 equipos informáticos y el servidor central se encuentran bajo la responsabilidad del Secretario de Hacienda Departamental. Estos

dispositivos almacenan los activos de información esenciales para el adecuado funcionamiento de la entidad. La seguridad y protección de dichos activos de información revisan una importancia primordial para garantizar la continuidad de las operaciones y preservar la confidencialidad, integridad y disponibilidad de la información financiera y contable de la Secretaría de Hacienda Departamental del Amazonas.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el análisis y gestión de riesgos informáticos a partir de las normas ISO 27001 e ISO 22301 contribuye a mantener la continuidad del negocio y garantizar la disponibilidad, integridad y confidencialidad de la información en la Secretaria de Hacienda Departamental del Amazonas?

2 JUSTIFICACIÓN

La adopción de un Sistema de Gestión de Continuidad de Negocio fundamentado en las normas ISO 22301 e ISO 27001 proporciona un marco estructurado y exhaustivo para garantizar la capacidad de operaciones de la Secretaría de Hacienda Departamental del Amazonas de afrontar eventos adversos y sostener la continuidad de sus operaciones. Estas normas brindan orientaciones y mejores prácticas para identificar y gestionar los riesgos que podrían impactar la continuidad del negocio, así como para salvar la confidencialidad, integridad y disponibilidad de la información.

La puesta en marcha de un Sistema de Gestión de Continuidad de Negocio basado en dichas normas permite a la organización establecer políticas, procedimientos, roles y responsabilidades precisas para enfrentar situaciones de crisis. Además, posibilita la realización de análisis de impacto y evaluaciones de riesgos para identificar las áreas más críticas y vulnerables del negocio, así como la elaboración de planes de contingencia y la ejecución de pruebas y simulacros para asegurar la efectividad de las medidas implementadas.

Al seguir estas normas, la Secretaría de Hacienda Departamental del Amazonas puede estar mejor preparada para afrontar eventos adversos como pandemias, ciberataques, incendios, terremotos, inundaciones, entre otros, y mitigar su impacto en las del negocio. Además, el enfoque en la protección de la confidencialidad e integridad de la información garantiza la seguridad de los activos de información y la confianza de las partes interesadas.

En conclusión, el diseño de un Sistema de Gestión de Continuidad de Negocio basado en las normas ISO 22301 e ISO 27001 resulta esencial para asegurar la capacidad de la Secretaría de Hacienda Departamental del Amazonas de superar eventos adversos y mantener la continuidad de sus operaciones, preservar la confidencialidad e integridad de la información, y mantener su reputación ante situaciones de crisis.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un plan de gestión de continuidad del negocio basado en los estándares ISO 22301 e ISO 27001 para minimizar los riesgos que amenazan la disponibilidad, integridad y confidencialidad de los activos de información en la Secretaria de Hacienda Departamental del Amazonas

3.2 OBJETIVOS ESPECÍFICOS

Definir el alcance y los requerimientos de las partes interesadas para realización del inventario de los activos de información en la Secretaría de Hacienda Departamental del Amazonas.

Evaluar los riesgos e impacto a la continuidad del negocio a partir de los lineamientos de la ISO 22301 y la ISO 27001.

Realizar un plan de tratamiento de riesgos para la implementación de controles preventivos que minimicen la probabilidad de ocurrencia de las amenazas en la Secretaría de Hacienda Departamental del Amazonas.

Establecer políticas y medidas de seguridad que mejoren la detección, respuesta y recuperación de incidentes, ante los escenarios críticos que puedan alterar la continuidad del negocio en la Secretaría de Hacienda Departamental del Amazonas.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 ¿QUÉ ES LA ISO 22301?

El Sistema de Gestión de Continuidad de Negocio ISO 22301 es una norma internacional de gestión que provee un marco detallado y completo para establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad de negocio en una organización. Esta norma ha sido creada en respuesta a la creciente demanda a nivel mundial que obtuvo la norma británica original BS 25999-2 y otras normas similares.

ISO 22301 identifica los fundamentos esenciales para la gestión de la continuidad de negocio, estableciendo los procesos, principios y terminología necesarios para asegurar una gestión efectiva y robusta. Proporciona una base sólida de entendimiento, desarrollo e implantación de la continuidad de negocio dentro de la organización.

El objetivo principal de ISO 22301 es ayudar a las organizaciones a prepararse y enfrentar eventos adversos que puedan afectar su capacidad para mantener la continuidad de sus operaciones y servicios. Esta norma proporciona un enfoque estructurado y sistemático para identificar, evaluar y gestionar los riesgos y amenazas que pueden interrumpir la operación normal del negocio.

Además, ISO 22301 establece requisitos claros para la planificación y la implementación de medidas de mitigación y respuesta ante situaciones de emergencia y crisis. Esto incluye la identificación y protección de los recursos y activos críticos, la elaboración de planes de continuidad de negocio, la realización de pruebas y ejercicios de simulación, y la revisión y mejora continua del sistema de gestión de la continuidad de negocio.

La implementación de un Sistema de Gestión de Continuidad de Negocio basado en ISO 22301 ayuda a asegurar a las partes interesadas clave, incluyendo a los clientes, proveedores, empleados y reguladores, que la organización está plenamente preparada para afrontar situaciones adversas y que puede cumplir con los requisitos internos, regulatorios y del cliente en términos de continuidad de

negocio. Además, permite mantener la reputación y la confianza de la organización en el mercado, al demostrar un enfoque proactivo y robusto para asegurar la continuidad de sus operaciones en situaciones de crisis.

En resumen, ISO 22301 es una norma internacional de gestión de continuidad de negocio que provee un marco completo y detallado para establecer y mantener un sistema de gestión efectivo en organizaciones, ayudando a asegurar la preparación y capacidad de la organización para enfrentar eventos adversos, cumplir con requisitos internos y regulatorios, proteger activos y recursos críticos, y mantener su reputación y confianza en el mercado.

4.1.2 ¿QUÉ ES LA ISO 27001?

La norma internacional ISO 27001:2013 proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el objetivo de garantizar la confidencialidad, integridad y disponibilidad continua de la información, así como cumplir con los requisitos legales. Obtener la certificación ISO 27001 es esencial para proteger los activos más valiosos de una organización, como la información de clientes y empleados, la reputación corporativa y otros datos confidenciales. La norma ISO 27001 utiliza un enfoque basado en procesos para el lanzamiento, implementación, operación y mantenimiento de un SGSI.

La implementación de la ISO 27001 es la respuesta ideal a los requisitos legislativos y de los clientes, incluyendo el Reglamento General de Protección de Datos (RGPD), así como otras amenazas potenciales como el cibercrimen, la violación de datos personales, vandalismo/terrorismo, incendios/dañinos, uso malintencionado, robo y ataques de virus. De hecho, en 2019, cerca del 32% de las empresas sufrieron una violación de datos personales o ataques en los últimos 12 meses, lo que resalta la importancia de implementar medidas de seguridad adecuadas.

La norma ISO 27001 está diseñada para ser compatible con otras normas de sistemas de gestión, como la ISO 9001, y es neutral en términos de tecnología y proveedores, lo que significa que es independiente de la plataforma de IT utilizada. Por lo tanto, es crucial que todos los miembros de la organización sean educados sobre el significado de la norma y cómo se aplica en la organización.

Obtener la certificación ISO 27001 acreditada demuestra el compromiso de una empresa con las mejores prácticas de seguridad de la información. Además, la

certificación ISO 27001 proporciona una evaluación experta de si la información de la empresa está adecuadamente protegida. A continuación, se presentan algunos de los beneficios adicionales de obtener la certificación ISO 27001.

4.1.3 PLAN DE CONTINUIDAD DE NEGOCIO

De acuerdo con Rodrigo Ferrer, La continuidad de negocio se refiere a la capacidad de una organización para mantener sus operaciones y minimizar la interrupción de los servicios y productos críticos durante y después de eventos adversos, como desastres naturales, incidentes de seguridad, fallos tecnológicos, entre otros. Es importante contar con procedimientos, tecnología e información estructurada y actualizada que permita hacer frente a estos eventos y garantizar la continuidad de las actividades de la empresa.".[1]

La gestión de riesgos es un componente clave en la planificación de la continuidad de negocio, ya que permite identificar, evaluar y controlar los riesgos que pueden afectar a la organización. Una solución tecnológica como Pirani Riskment Suite puede facilitar este proceso al proporcionar una plataforma centralizada para gestionar y monitorear los riesgos de manera eficiente.[2]

Es importante tener en cuenta que la continuidad de negocio no se limita a la prevención de pérdidas, sino que busca mantener la operación normal de la empresa y minimizar el impacto de eventos adversos. Por lo tanto, es fundamental contar con un plan de continuidad de negocio bien estructurado y actualizado que incluya procedimientos claros, tecnología adecuada y una gestión efectiva de riesgos para garantizar la resiliencia y supervivencia de la organización en situaciones difíciles.[3]

---

[1] Welivesecurity, 4 pasos para armar un plan de continuidad del negocio que asegure el futuro digital de la empresa, citado el 15 de octubre del 2021, (14 de mayo del 2014), tomado de: https://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/

[2] Piranirisk, Guía para gestionar un plan de continuidad de negocio, según la ISO 22301, citado el 15 de octubre del 2021, (19 de abril del 2021), tomado de: https://www.piranirisk.com/es/academia/especiales/guia-para-gestionar-un-plan-de-continuidad-de-negocio-segun-la-iso-22301

[3] GOBIERNO DE COLOMBIA – Escuela superior de Administración Pública, Plan de continuidad del negocio BCP, citado el 15 de octubre del 2021, (2018), tomado de: https://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-continuidad-del-negocio-v1.pdf

Por otro lado, hay que tener en cuenta que la continuidad de negocio no se debe relacionar con el plan de prevención de pérdidas**,** pues para este se deben registrar las actividades que se van a llevar a cabo a través de sistemas, autenticación, seguridad y control para poder identificar la magnitud de lo que se extravió[4].

4.2 GESTIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO

Se desarrolla en seis etapas que explicaremos a continuación:

4.2.1 ETAPA 1

CREACIÓN DEL PROGRAMA: Aquí se debe elaborar el programa de gestión de continuidad, en el que se debe tener cuenta el tamaño y complejidad de la organización, a su vez se elegirán los responsables, quiénes estarán a cargo y se les designará su función.

4.2.2 ETAPA 2

COMPRENSIÓN DE LA COMPAÑÍA: Se recolecta la información necesaria con el fin de darle importancia a cada una de las actividades, que deben ser clasificadas en clave, de apoyo y a su vez designar los recursos que se necesitan. Se realiza la evaluación del impacto del negocio y de los riesgos.

4.2.3 ETAPA 3

DEFINICIÓN DE ESTRATEGIAS: Se seleccionan aquellas actividades que permiten que la organización pueda recuperar su servicio en un tiempo determinado en caso de sufrir algún tipo de incidente.

4.2.4 ETAPA 4

ELABORACIÓN Y EJECUCIÓN DE UNA RESPUESTA: Se redactan las respuestas que se darán frente alguna amenaza que se pueda presentar. Este

[4] NAE, Claves para un plan de continuidad de negocio (BCP), citado el 15 de octubre del 2021, (10 de junio de 2020), tomado de: https://nae.global/es/claves-para-un-plan-de-continuidad-de-negocio-bcp/

contará con un paso a paso que se deberá poner en práctica para actuar de manera correcta y siguiendo los protocolos establecidos.

4.2.5 ETAPA 5

CUMPLIR LOS ACUERDOS PACTADOS: En esta etapa se le da relevancia a las estrategias y planes definidos con el fin de cumplir el propósito por el que se implementó el sistema. Se lleva a cabo a través de ejercicios en diferentes momentos que permitan evaluar la continuidad de negocio y a su vez tener la oportunidad de mejora.

4.2.6 ETAPA 6

CULTURA ORGANIZACIONAL: Todos los empleados y miembros de la organización deben estar alineados con el sistema de gestión de continuidad de negocio, entender que esto hace parte de la compañía y que de ellos también depende su buen funcionamiento. Se debe incluir dentro de los valores para que ellos sientan y entiendan esta relación.

Por marco teórico se entiende la elaboración teórica del problema planteado y que da razón de la estructura conceptual básica en la que va a plantear la investigación para explicar o solucionar el problema. Es importante indicar los referentes teóricos del problema; por tanto, teorice el problema y construya el plan teórico y los recursos de conocimiento disciplinar e interdisciplinar que serán sustantivos en la investigación proyectada.

4.3 MARCO CONCEPTUAL

4.3.1 ¿QUÉ ES UN PLAN O SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO (SGCN)?

Todas las organizaciones, independientemente de su tamaño o sector, enfrentan la posibilidad de enfrentar incidentes inesperados que pueden causar interrupciones en su operación normal. Estos incidentes pueden variar desde desastres naturales, fallos técnicos, ciberataques, hasta errores humanos, entre otros. Estas interrupciones pueden tener un impacto significativo en la continuidad del negocio, provocando una parada de su actividad y causando pérdidas financieras, daños a la reputación y pérdida de clientes.

Por esta razón, es fundamental que las organizaciones cuenten con planes de respuesta bien establecidos que les permitan gestionar eficazmente estos eventos y minimizar sus efectos. Un enfoque comúnmente utilizado para abordar esta necesidad es la implementación de un Plan o Sistema de Gestión de Continuidad de Negocio (SGCN), el cual es un marco de trabajo integral que establece políticas, procedimientos y procesos para asegurar que una organización pueda continuar con sus operaciones críticas en caso de interrupciones.

Un SGCN bien diseñado incluye la identificación y evaluación de los riesgos y amenazas potenciales, la implementación de medidas de prevención y mitigación, la elaboración de planes de respuesta ante incidentes, la asignación de roles y responsabilidades, la capacitación del personal, la realización de pruebas y simulacros, y la revisión y mejora continua del plan. Además, el SGCN debe estar alineado con la estrategia de negocio y adaptarse a los cambios internos y externos de la organización.

La implementación de un SGCN no solo ayuda a proteger a la organización ante posibles interrupciones, sino que también fortalece la resiliencia de la misma, permitiéndole recuperarse de manera más rápida y eficiente en caso de incidentes. Además, puede ser un factor clave en la toma de decisiones, al proporcionar una mayor confianza a los clientes, proveedores, empleados y otras partes interesadas sobre la capacidad de la organización para garantizar la continuidad de su operación en situaciones adversas.

En resumen, la implementación de un Plan o Sistema de Gestión de Continuidad de Negocio es esencial para cualquier organización, ya que ayuda a anticiparse y gestionar de manera efectiva las interrupciones en la operación normal, protegiendo así la continuidad del negocio y asegurando su capacidad para enfrentar y recuperarse de incidentes imprevistos.

4.3.2 ¿CÓMO AYUDA A NUESTRA ORGANIZACIÓN IMPLANTAR UN SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO?

La implementación de un Sistema de Gestión de Continuidad de Negocio (SGCN) brinda a las organizaciones la capacidad de enfrentar y superar eventos adversos que podrían tener un impacto negativo y poner en peligro la continuidad de su actividad. Estos eventos pueden variar desde pandemias, ciberataques, incendios, terremotos, inundaciones, entre otros.

Un SGCN bien establecido permite a una organización estar preparada para hacer frente a estos eventos imprevistos de manera proactiva y eficiente. Proporciona un marco de trabajo estructurado que permite identificar y evaluar los riesgos y amenazas potenciales que podrían afectar a la organización, así como implementar medidas de prevención y mitigación adecuadas. Además, el SGCN incluye la elaboración de planes de respuesta ante incidentes, la asignación clara de roles y responsabilidades, la capacitación del personal y la realización de pruebas y simulacros para asegurar la preparación del equipo en caso de un evento real.

El SGCN se adapta a la realidad y necesidades de cada organización, lo que permite establecer procedimientos y acciones específicas para enfrentar situaciones particulares. Por ejemplo, en caso de una pandemia, el SGCN podría incluir planes para el trabajo remoto, medidas de protección sanitaria y continuidad operativa bajo escenarios de contingencia. En caso de un ciberataque, el SGCN podría contar con procedimientos para la recuperación de datos y sistemas, así como medidas de seguridad adicionales para proteger la información sensible de la organización.

Contar con un SGCN bien implementado tiene numerosos beneficios. Además de garantizar la continuidad de las operaciones en situaciones adversas, también puede ayudar a reducir el impacto financiero de los eventos disruptivos, minimizar la pérdida de clientes y proteger la reputación de la organización. Además, un SGCN puede ser un requisito para cumplir con regulaciones y normativas específicas, así como un factor diferenciador en la competitividad del mercado, ya que muestra a clientes, proveedores y otras partes interesadas el compromiso de la organización con la gestión eficaz de la continuidad del negocio.

En resumen, la implementación de un Sistema de Gestión de Continuidad de Negocio proporciona a las organizaciones la capacidad de sobrevivir y recuperarse de eventos que podrían poner en peligro la continuidad de su actividad. Es una herramienta estratégica que asegura la preparación, respuesta y recuperación adecuada ante situaciones adversas, protegiendo así los intereses de la organización y sus partes interesadas en un entorno empresarial cambiante y desafiante.

4.3.3 ¿CÓMO ELABORAR UN SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO?

La norma ISO 22301 y la norma ISO 27001 son marcos de referencia ampliamente reconocidos y utilizados para la implementación y mantenimiento de un Sistema de Gestión de Continuidad de Negocio.

La norma ISO 22301, titulada "Sistemas de Gestión de Continuidad de Negocio - Requisitos", proporciona un enfoque estructurado y basado en procesos para

establecer, implementar, mantener y mejorar un Sistema de Gestión de Continuidad de Negocio. Define los requisitos necesarios para identificar y gestionar los riesgos y amenazas que pueden afectar la continuidad del negocio, así como para desarrollar e implementar planes de continuidad de negocio, realizar pruebas y simulacros, y asegurar la capacidad de recuperación en caso de interrupciones.

Por otro lado, la norma ISO 27001, titulada "Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de Seguridad de la Información - Requisitos", se enfoca en la seguridad de la información y proporciona un marco de trabajo para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La seguridad de la información es un componente importante de la continuidad de negocio, ya que la pérdida o compromiso de información sensible puede tener un impacto significativo en la operación de una organización.

Ambas normas se basan en el enfoque Planificar-Hacer-Verificar-Actuar (PDCA) de mejora continua, y comparten principios y enfoques comunes, como el enfoque basado en riesgos, la implicación de la alta dirección, la participación de los empleados, la comunicación interna y externa, y la revisión y mejora periódica del sistema.

La implementación de estas normas puede ayudar a las organizaciones a establecer un enfoque sistemático y estructurado para la gestión de la continuidad de negocio, así como para garantizar la protección de la información sensible. Además, la certificación según estas normas puede ser utilizada como una herramienta de demostración de conformidad y confianza para clientes, proveedores y otras partes interesadas. Sin embargo, es importante tener en cuenta que la implementación de un SGCN o un SGSI debe ser adaptada a las necesidades y características específicas de cada organización, y se recomienda buscar el apoyo de profesionales y expertos en la materia para asegurar una implementación efectiva y exitosa.

4.3.4 PASOS O FASES PRINCIPALES PARA LA IMPLANTACIÓN:

Figura 1 Fases SGCN

Fuente: GlobalSUITEsolutions, ¿Cómo elaborar un plan de continuidad?,[En Línea] citado el 15 de octubre del 2021, (10 de septiembre de 2020), tomado de: https://www.globalsuitesolutions.com/es/como-elaborar-un-plan-de-continuidad/

DETERMINAR EL ALCANCE:

La identificación de los procesos de negocio de la organización es el primer paso en la implementación de un Sistema de Gestión de Continuidad de Negocio (SGCN). Esto implica identificar y comprender los procesos clave de la organización que son necesarios para mantener sus operaciones y servicios en funcionamiento.

El siguiente paso es llevar a cabo un Análisis de Impacto en el Negocio (BIA), que implica evaluar la criticidad de cada proceso identificado en términos de los impactos que su interrupción podría tener en la organización. Esto incluye la determinación de los diferentes tipos de impacto que podrían surgir, como operacionales, financieros, legales, reputacionales, etc., y cómo estos impactos evolucionarían a lo largo del tiempo.

El BIA también implica identificar los requerimientos temporales y de recursos necesarios para la continuidad del negocio y la vuelta a la normalidad de cada proceso. Esto incluye la identificación de los recursos humanos, infraestructuras, proveedores, servicios, maquinaria, tecnologías utilizadas, tiempos de recuperación, tiempo máximo tolerable de caída del servicio, niveles mínimos de recuperación del servicio, etc.

Una vez que se haya realizado el BIA, el siguiente paso es llevar a cabo un Análisis de Riesgos, que implica identificar las posibles amenazas a las que la organización está expuesta y evaluar su probabilidad de ocurrencia e impacto en caso de que se materialicen. Con esta evaluación de riesgos, se determina el nivel de riesgo de cada amenaza y se establece un Plan de Tratamiento de Riesgos, que incluye la implementación de controles preventivos para reducir la probabilidad de ocurrencia de las amenazas.

A partir de los resultados del Análisis de Riesgos, se identifican posibles escenarios de crisis y se establece una estrategia de recuperación para cada uno de ellos. Esto implica desarrollar planes detallados de respuesta y recuperación ante los escenarios críticos identificados, que incluyen los pasos a seguir desde la comunicación del incidente hasta la vuelta a la normalidad.

Es importante documentar todos los planes de respuesta y recuperación, y realizar pruebas y ejercicios para comprobar su eficacia y adecuación. Los resultados de estas pruebas se registran en informes que documentan los resultados obtenidos y las incidencias surgidas, lo que permite realizar mejoras y ajustes en los planes de forma continua.

En resumen, la implementación y mantenimiento de un SGCN implica la identificación de los procesos de negocio críticos, la realización de un análisis de impacto en el negocio, un análisis de riesgos, el establecimiento de planes de tratamiento de riesgos, la creación de planes de respuesta y recuperación, y la realización de pruebas y ejercicios para asegurar la eficacia de los planes. Todo ello en un enfoque de mejora continua para garantizar la continuidad de las operaciones de la organización en caso de interrupciones.

Realizar revisiones y auditorías de nuestro Sistema de Gestión para garantizar su mantenimiento, actualización y establecimiento de medidas correctoras. Con ello conseguiremos su mejora continua.[5]

[5] GlobalSUITEsolutions, ¿Cómo elaborar un plan de continuidad?, citado el 15 de octubre del 2021, (10 de septiembre de 2020), tomado de: https://www.globalsuitesolutions.com/es/como-elaborar-un-plan-de-continuidad/

4.4 MARCO HISTÓRICO

El marco histórico en una investigación científica tiene como propósito describir el contexto histórico relevante para el estudio y cómo éste ha evolucionado con el tiempo. Según Carrasco (2009), el marco histórico proporciona una narración descriptiva de cómo surgió, evolucionó y se agudizó el problema de investigación en cuestión.

Es importante destacar que el marco histórico no sólo describe los antecedentes históricos del problema, sino que también explica cómo éstos han influido en la formulación del problema y en su importancia actual. Al contextualizar el problema de investigación en su marco histórico, se puede entender mejor su origen y las razones por las cuales es importante abordarlo en la actualidad.

4.5 ANTECEDENTES O ESTADO ACTUAL

Análisis de activos de información para un sistema misional basados en la metodología Magerit v3 y la norma ISO 27001:2013.[6]

4.6 MARCO CIENTÍFICO O TECNOLÓGICO

Las normas ISO 22301 e ISO 27001 pueden ser una herramienta tecnológica útil para aplicar en los modelos de negocios con el fin de mitigar riesgos. Ambas normas proporcionan una metodología clara y concisa que permite aprovechar al máximo las distintas variables de los activos de información, lo que permite calcular su estado actual utilizando matrices estandarizadas.

Al utilizar estas normas, las empresas pueden tener una mejor comprensión de los riesgos potenciales y cómo abordarlos. Además, esto puede ayudar a las empresas a cumplir con los requisitos reglamentarios y de seguridad, lo que puede aumentar la confianza de los clientes y mejorar la reputación de la empresa

[6] Suárez, R. (2018). Análisis de activos de información para un sistema misional basados en la metodología Magerit v3 y la norma ISO 27001:2013.. [Monografia, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/19571.

4.7 MARCO LEGAL

La Ley 1712 de 2014 establece que el término "información" se refiere a cualquier conjunto organizado de datos que se encuentra contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Esta ley proporciona a las organizaciones un marco legal que asegura su continuidad operativa durante situaciones adversas e inesperadas, protegiendo a sus empleados, manteniendo su reputación y permitiéndoles seguir trabajando y comercializando. Al cumplir con los requisitos de la Ley 1712, las organizaciones pueden proteger su información, lo que aumenta la confianza de sus clientes y mejora su reputación.

4.7.1 LA NORMA ISO 22301 PUEDE SER APLICADA A TODO TIPO Y TAMAÑO DE ORGANIZACIONES QUE QUIERAN:

Establecer, implantar, mantener y mejorar un SGCN. Demostrar conformidad con la política establecida de la continuidad de negocio de la organización. Dar a las partes interesadas confianza en su conformidad y compromiso con las buenas prácticas reconocidas internacionalmente. Norma ISO 22301Estructura de la norma ISO 22301

4.7.2 LA NORMA ISO 22301 ESTÁ ORGANIZADA SEGÚN LA SIGUIENTE ESTRUCTURA:

La norma ISO 22301 establece los requisitos para la implementación de un Sistema de Gestión de la Continuidad del Negocio (SGCN). El ámbito de aplicación, referencias normativas y términos y definiciones son los primeros aspectos a considerar en su implementación. Para ello, se debe identificar el alcance del SGCN tomando en cuenta los objetivos estratégicos, productos y servicios claves, tolerancia al riesgo y obligaciones reglamentarias de la organización.

El liderazgo de la alta dirección es fundamental en la implementación del SGCN, ya que debe demostrar un compromiso continuo y crear un ambiente de involucramiento del personal. La planificación estratégica del SGCN es otro de los aspectos clave en su implementación, estableciendo objetivos y principios para su orientación.

Para la gestión diaria del SGCN, es necesario contar con recursos apropiados, personal competente, comunicación efectiva y documentación necesaria. La operación del SGCN es el resultado de la planificación previa y debe ser evaluada periódicamente para su mejora continua.

La Plataforma Tecnológica ISOTools es una herramienta que facilita la implementación, automatización y mantenimiento del SGCN conforme al ciclo PHVA. Esta plataforma permite a las organizaciones estar preparadas ante posibles incidentes que puedan poner en riesgo su continuidad de negocio, disminuyendo los tiempos de inactividad, la probabilidad de ocurrencia y costos asociados.

Además, ISOTools permite la integración del estándar ISO 22301 con otras normas como ISO 9001, ISO 14001 y OHSAS 18001, gracias a su estructura modular. En resumen, la implementación de ISO 22301 con el uso de ISOTools puede garantizar la continuidad de negocio y reducir los riesgos y costos asociados a la interrupción de las actividades empresariales.

Este software permite la integración del estándar ISO 22301 con otras normas, tales como ISO 9001, ISO 14001 y OHSAS 18001, de forma sencilla gracias a su estructura modular.[7]

[7] ISOTOLLS, ISO 22301, 22 de julio del 2020, citado el 26 de noviembre del 2021, tomado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301/

5 DISEÑO METODOLÓGICO

La metodología escogida está basada en los procedimientos para hacer un Plan de Continuidad de Negocio (SGCN) basados en aplicar la ISO 22301.

5.1 DETERMINACIÓN DEL ALCANCE

Se debe clasificar cada una de las áreas dándole una clasificación de prioridad a cada una de ellas, con el fin de entender cuáles son las más vulnerables y de esta manera poder ir trabajando en la continuidad de la organización, en este punto es clave la participación de la dirección.

5.2 ANÁLISIS DE LA EMPRESA

Se debe recoger toda la información de la organización con el fin de identificar cuáles son los procesos de negocios críticos (activos), cómo se les dará soporte y cuáles son las necesidades que se presentan.

5.3 ANÁLISIS DE RIESGOS

Determinar las posibles amenazas sobre los activos a las que está expuesta la organización;
determinar el nivel de riesgo de cada amenaza, evaluando su probabilidad de ocurrencia y el impacto que causaría en caso de producirse. Un riesgo alto debe indicar que nos preocupa la continuidad de negocio para ese activo.

5.4 PLAN DE TRATAMIENTO DE RIESGOS

Consistente en la implantación de controles, normalmente preventivos, que ayuden a reducir la probabilidad de ocurrencia de las amenazas.[8]

5.5 DETERMINACIÓN DE LA ESTRATEGIA

Una vez estén definidos los activos se debe establecer que si en caso de que se llegue a presentar una amenaza están en la capacidad de recuperar estos activos

[8] GlobalSUITEsolutions, ¿Cómo elaborar un plan de continuidad?, citado el 15 de octubre del 2021, (10 de septiembre de 2020), tomado de: https://www.globalsuitesolutions.com/es/como-elaborar-un-plan-de-continuidad/

en corto plazo, si por el contrario requiere de un tiempo mayor se deben establecer estrategias.

5.6 IDENTIFICACIÓN DE ESCENARIOS DE CRISIS

A partir de los resultados del Análisis de Riesgos, identificar los posibles escenarios de crisis y establecer la estrategia de recuperación para cada uno de ellos.

5.7 PLANES DETALLADOS DE RESPUESTA Y RECUPERACIÓN

Crear y documentar planes detallados de respuesta y recuperación ante los escenarios críticos identificados, que incluyan los pasos a dar desde la comunicación del incidente hasta la vuelta a la normalidad. Su objetivo es evitar la ausencia o la toma de decisiones improvisada que pueda empeorar la situación o hacer esta irreversible.

5.8 RESPUESTA A LA CONTINGENCIA

Se elegirán las estrategias necesarias que se podrán en marcha en caso de presentarse un desastre y se creará un plan de crisis en donde se documentará toda la información.[9]

[9] DISASTER RECOVERY DRJOURNAL En español, El Plan de Continuidad del Negocio, citado el 15 de octubre del 2021, (10 de septiembre de 2020), tomado de: https://drjenespanol.com/recursos/el-plan-de-continuidad-del-negocio/

6 ALCANCE Y REQUERIMIENTOS DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN

El presente trabajo de grado se enmarca en los proyectos aplicados que se llevan a cabo en el ámbito de las entidades públicas. El objetivo principal es elaborar un plan de continuidad basado en el estándar ISO 22301 y utilizar la metodología MARGERIT, que se basa en la norma ISO 27001. A través de un análisis de riesgos, se busca mitigar los riesgos asociados a los activos de información en la Secretaría de Hacienda del Departamento del Amazonas.

Este trabajo tiene una gran relevancia en la actualidad, debido a la importancia de garantizar la continuidad de las operaciones críticas en una entidad pública, en este caso, en la Secretaría de Hacienda del Departamento del Amazonas. Un plan de continuidad adecuado puede prevenir la interrupción de las actividades y la pérdida de información valiosa, lo que puede tener un impacto significativo en el servicio prestado a la ciudadanía.

La implementación de la norma ISO 22301 proporciona una estructura sólida para desarrollar un plan de continuidad efectivo, asegurando que la organización esté preparada para enfrentar cualquier situación de crisis. Además, la metodología MARGERIT, basada en la norma ISO 27001, proporciona una guía detallada para la gestión de riesgos asociados a los activos de información, lo que garantiza la protección adecuada de los datos sensibles.

El análisis de riesgos permitirá identificar y evaluar los posibles riesgos que pueden afectar los activos de información críticos de la Secretaría de Hacienda del Departamento del Amazonas. Una vez identificados los riesgos, se implementarán medidas de mitigación para reducir la probabilidad de ocurrencia y minimizar las consecuencias en caso de que ocurran **(Ver ANEXO 8).**

En resumen, la elaboración de un plan de continuidad basado en la norma ISO 22301 y la metodología MARGERIT es fundamental para garantizar la continuidad de las operaciones críticas en la Secretaría de Hacienda del Departamento del Amazonas. Esto permitirá a la entidad estar preparada para enfrentar cualquier situación de crisis y asegurar la protección adecuada de los activos de información críticos, lo que finalmente contribuirá a mejorar el servicio prestado a la ciudadanía.

6.1 IDENTIFICACION DE LOS FACTORES INTERNOS Y EXTERNOS

6.1.1 ACTIVIDAD DE LA SECRETARIA DE HACIENDA

La Secretaría de Hacienda es una entidad fundamental en la gestión financiera del Departamento del Amazonas. Se encarga de manejar los recursos económicos del departamento, tales como el presupuesto, la tesorería, la parte contable y las rentas

propias. Su función es crucial para garantizar que los recursos se utilicen de manera adecuada, transparente y eficiente.

Es importante destacar que los recursos que maneja la Secretaría de Hacienda se distribuyen según su origen y su destinación específica, lo que implica una gran responsabilidad en su gestión. Estos recursos pueden ser destinados a diferentes sectores, como el sector central, salud y educación, con el objetivo de mejorar la calidad de vida de la población.

Además, la Secretaría de Hacienda también tiene la tarea de elaborar y presentar el presupuesto anual del departamento ante las autoridades correspondientes. Este proceso implica un análisis detallado de las necesidades y requerimientos de cada sector, con el objetivo de garantizar que los recursos se asignen de manera efectiva y eficiente.

En resumen, la Secretaría de Hacienda es una entidad clave en la gestión financiera del Departamento del Amazonas, y su trabajo es fundamental para garantizar que los recursos se manejen de manera transparente y eficiente, y que se destinen a los sectores que más los necesitan, como el sector de la salud y la educación.

6.1.2 FUNCIONES DE LA SECRETARIA DE HACIENDA

Los productos que maneja la secretaria de hacienda son los siguientes:

- Dar seguimiento a los recursos que ingresan a las cuentas bancarias del Departamento del Amazonas.
- Clasificar los recursos por rubros presupuestales.
- Rendir informes de gestión y de control ante los entes de control y asambleas departamentales.
- Proyectar ordenanzas departamentales referentes a la parte financiera del Departamento del Amazonas.
- Realizar obligaciones de pago.
- Realizar revisión a las cuentas de cobros.
- Realizar pagos correspondientes a los contratos adjudicados por el Departamento del Amazonas.
- Realizar la fiscalización garantizando el ingreso de los recursos propios del Departamento.
- Entre otros.

6.1.3 SERVICIOS QUE OFRECE LA SECRETARIA DE HACIENDA

La Secretaría de Hacienda Departamental es una entidad encargada de manejar las finanzas del Departamento del Amazonas y brinda diversos servicios a la ciudadanía. Uno de los servicios más importantes que ofrece la Secretaría es el

pago de impuestos departamentales en ventanilla, incluyendo el Impuesto Automotor, el Impuesto al Registro y la Estampilla pro Universidad de la Amazonia.

Además de estos servicios, la Secretaría de Hacienda Departamental también tiene una atención al cliente especializado para consultas relacionadas con los pagos de las OPS (Órdenes de Prestación de Servicios) celebradas con el departamento. Estas órdenes se pagan mes a mes según el método de pago establecido en el contrato correspondiente.

Es importante destacar que la Secretaría de Hacienda Departamental tiene un compromiso con la transparencia y la eficiencia en el manejo de los recursos públicos. Por esta razón, se esfuerza en brindar una atención al cliente de calidad y en garantizar que los servicios que ofrece sean prestados de manera oportuna y eficaz. Además, la Secretaría cuenta con un equipo de profesionales altamente capacitados en el ámbito financiero y tributario, que están dispuestos a brindar asesoría y orientación en cualquier tema relacionado con los servicios que ofrecen.

6.1.4 REQUERIMIENTOS Y ACTIVOS DE LA SECRETARIA DE HACIENDA

La Secretaría de Hacienda es un área vital en la gestión financiera de la entidad gubernamental. Sin embargo, es preocupante que solamente el 50% de los equipos de cómputo estén debidamente licenciados con el sistema operativo Windows 10; **(Ver ANEXO 2)** Además, los otros equipos no cuentan con licencia o tienen un sistema operativo inferior, lo que compromete la seguridad de la información y la eficiencia del trabajo en esta área. Lo mismo sucede con el software de Office, que es esencial para las actividades cotidianas de la Secretaría de Hacienda. Es importante destacar que la falta de licencias puede generar problemas legales y de seguridad para la entidad.

Para mejorar la gestión de activos de información, es necesario clasificar adecuadamente los activos según el alcance definido para la implementación del MSPI. La gestión de activos debe estar alineada con el Dominio 8 Gestión de Activos del Anexo A de la norma ISO 27001:2013 y la guía de controles del modelo de seguridad y privacidad de la información. Esto ayudará a proteger los activos de información y garantizar una gestión adecuada de los mismos.

Además, es fundamental implementar medidas de seguridad para proteger la información financiera de la entidad. Esto incluye la actualización de los sistemas operativos y el software de Office, la instalación de software de seguridad, la realización de copias de seguridad y la implementación de medidas de control de acceso a la información. La Secretaría de Hacienda debe tomar medidas para

asegurar que los activos de información estén protegidos y que se garantice la integridad y confidencialidad de la información financiera de la entidad, para garantizar el cumplimiento de los puntos descritos a continuación:

6.1.5 INVENTARIO DE ACTIVOS:

Se identificaron los activos asociados con la instalación de procesamiento de información, y se eléboro y mantuvo un inventario de activos como se puede observar en el **ANEXO 2**.

6.1.5.1 PROPIEDAD DE LOS ACTIVOS:

Los activos mantenidos en el inventario están bajo el cargo del P.U (Profesional Universitario) a cargo de las oficinas (Contabilidad, Presupuesto, Tesorería, Rentas y Hacienda) como se puede ver en el **ANEXO 1**.

6.1.5.2 USO ACEPTABLE DE LOS ACTIVOS:

Se identificó, documentó e implementó reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

6.1.5.3 DEVOLUCIÓN DE ACTIVOS:

Todos los empleados y usuarios de partes externas deberán devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

6.1.5.4 CLASIFICACIÓN DE LA INFORMACIÓN:

La información se clasificó en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada como se puede ver en el **ANEXO 3.**

6.1.5.5 ETIQUETADO DE LA INFORMACIÓN:

Se desarrolló e implementó un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la Secretaría de Hacienda Departamental del Amazonas.

6.1.5.6 MANEJO DE ACTIVOS:

Se desarrolló e implementó procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la gobernación del Amazonas.

6.2 VINCULAR Y ALINEAR ESTRATÉGICAMENTE

6.2.1 POLITICAS DE LA SECRETARIA DE HACIENDA

6.2.1.1 POLITICA DEL SISTEMA DE GESTION

La Secretaría de Hacienda Departamental del Amazonas es una entidad fundamental en la administración pública del territorio, cuyo objetivo es garantizar la sostenibilidad financiera del ente territorial. Para ello, ha establecido una estructura organizacional sólida y eficiente que se adapta rápidamente a los cambios tecnológicos y sociales, a través de una cultura organizacional basada en el servicio.

La Secretaría de Hacienda Departamental del Amazonas se enfoca en la recaudación eficiente y la distribución efectiva de los recursos financieros, de manera que cumpla con los requisitos aplicables de los grupos de valor y partes interesadas. Además, está comprometida con el mejoramiento continuo y la adopción de las mejores prácticas en cuanto a la calidad del gasto público.

Es importante destacar que la Secretaría de Hacienda Departamental del Amazonas es consciente de la importancia de la transparencia en la administración pública y se esfuerza por cumplir con los estándares más altos en esta materia. Para ello, se ha enfocado en fortalecer su sistema de gestión de información financiera y su capacidad de reporte, así como en garantizar el acceso a la información para los ciudadanos y las partes interesadas.

Asimismo, la Secretaría de Hacienda Departamental del Amazonas se encuentra en constante evolución y actualización en cuanto a la adopción de tecnologías y herramientas innovadoras que le permitan mejorar la eficiencia en la gestión financiera. Además, se asegura de que todos sus colaboradores estén debidamente capacitados y actualizados para manejar dichas herramientas y tecnologías de manera efectiva y responsable.

En resumen, la Secretaría de Hacienda Departamental del Amazonas es una entidad comprometida con la sostenibilidad financiera del territorio, que trabaja de manera eficiente y transparente, con un enfoque en la recaudación eficiente y la distribución efectiva de los recursos financieros, siempre buscando mejorar su gestión mediante la adopción de las mejores prácticas y tecnologías innovadoras.

6.2.1.2 POLÍTICA DE COMUNICACIONES

La Secretaría de Hacienda Departamental del Amazonas reconoce la importancia de contar con una política de comunicaciones que garantice una gestión eficaz y eficiente de los procesos comunicativos de la Entidad Territorial. Esta política se enfoca en establecer un diálogo fluido y participativo con los diferentes grupos de interés de la organización, así como con la ciudadanía en general.

La Política de Comunicaciones busca, además, promover la transparencia en la gestión pública, brindando mayor acceso a la información y fomentando la rendición de cuentas, para generar confianza en la ciudadanía y fortalecer la imagen reputacional de la Entidad.

La implementación de esta política se rige por las directrices del Manual Estratégico de Comunicaciones en el Distrito Capital, así como por el Modelo Integrado de Planeación y Gestión (MIPG), y las normativas establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Asimismo, la Política de Comunicaciones define las estrategias y acciones comunicativas que se deben llevar a cabo para visibilizar la gestión pública y promover el bienestar común, así como para posicionar la imagen institucional en el territorio. Para ello, se establecen los canales y medios de comunicación adecuados para llegar a los diferentes públicos y se definen los mensajes y contenidos que se deben transmitir.

Por último, la Política de Comunicaciones establece una serie de indicadores que permiten evaluar el desempeño de la gestión comunicativa y que se integran al MIPG para obtener un panorama integral de la gestión de la Secretaría de Hacienda Departamental del Amazonas. De esta manera, se busca asegurar la sostenibilidad financiera del ente territorial y contribuir a la generación de confianza en la administración pública, en un marco de mejores prácticas orientadas a la calidad del gasto público.

6.2.1.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La Política de Seguridad de la Información y Seguridad Digital de la Secretaría de Hacienda Departamental del Amazonas se aplica a todos los servidores públicos, contratistas, proveedores, operadores y entidades adscritas, así como a cualquier persona o tercero que, en el cumplimiento de sus funciones en la Secretaría, comparta, utilice, recolecte, procese, intercambie o consulte información. También se aplica a las entidades de control ya cualquier otra entidad relacionada que acceda, interna o externamente, a cualquier activo de información, independientemente de su ubicación.

Esta política también se extiende a toda la información creada, procesada o utilizada por la Secretaría de Hacienda Departamental del Amazonas, sin importar el medio, formato, presentación o lugar donde se encuentre.

A través de la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Subsistema de Gestión de Seguridad de la Información, la Secretaría protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en la entidad departamental. Esto se logra mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, garantizar la continuidad de los servicios tecnológicos y cumplir con los requisitos legales, reglamentarios y regulatorios.

La Política de Seguridad de la Información y Seguridad Digital de la Secretaría de Hacienda Departamental del Amazonas está orientada a la mejora continua y al alto desempeño del Subsistema de Gestión de Seguridad de la Información, promoviendo así el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones - TIC, para mejorar la calidad de vida de los ciudadanos y el incremento sostenible del desarrollo del Departamento del Amazonas.

6.2.1.4 POLÍTICA DE ADMINISTRACIÓN DE RIESGO Y CUMPLIMIENTO

La Política de Administración de Riesgos y Cumplimiento de la Secretaría de Hacienda Departamental del Amazonas establece pautas de cumplimiento obligatorio en todas las dependencias de la Secretaría, incluyendo procesos, procedimientos, tareas e instrucciones a sus funcionarios, contratistas y particulares que ejerzan funciones públicas en la Entidad Departamental. Además, también establece lineamientos en gestión de riesgos para los particulares con los que se establecen relaciones contractuales apreciables en dinero.

Esta política se enfoca en la gestión de riesgos en todos los aspectos de la Secretaría, desde la toma de decisiones hasta la implementación de procesos y procedimientos. La política establece un marco de trabajo para la identificación, evaluación y gestión de los riesgos que enfrenta la Secretaría, y se aplica a todos los aspectos de la organización, incluyendo la planificación estratégica, la gestión de proyectos, la gestión de la seguridad de la información y el cumplimiento normativo.

La Secretaría de Hacienda Departamental del Amazonas se compromete a garantizar el cumplimiento de esta política en todos los niveles de la organización, ya asignar los recursos necesarios para implementarla efectivamente. Además, la Secretaría también se compromete a monitorear continuamente el cumplimiento de

esta política y actualizarla según sea necesario para asegurar su relevancia y eficacia en la gestión de riesgos.

6.2.1.5 POLÍTICA SUBSISTEMA DE GESTIÓN DE SEGURIDAD EN EL TRABAJO SG-SST

La Secretaría de Hacienda Departamental del Amazonas se compromete a proteger la salud y seguridad laboral de sus servidores y contratistas, así como a brindar ambientes seguros a los ciudadanos que ingresan a las sedes de trabajo de la entidad.

Para lograr este compromiso, la Secretaría implementará el Subsistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST), con la participación activa de los servidores, garantizando la aplicación de medidas de seguridad y salud en el trabajo encaminadas a mantener la salud de sus servidores.

La Secretaría anticipará, reconocerá, evaluará y controlará los riesgos a partir de la identificación de los peligros que puedan afectar la seguridad y salud en el trabajo de los servidores de la Secretaría de Hacienda Departamental y toda la entidad en general.

Asimismo, se tomarán medidas preventivas para evitar incidentes, accidentes y enfermedades laborales de los servidores públicos y contratistas a través de mecanismos definidos en los programas que conformen el Subsistema de Seguridad y Salud en el Trabajo en la Secretaría de Hacienda Departamental del Amazonas.

La Secretaría de Hacienda Departamental del Amazonas se compromete a asignar los recursos necesarios para cumplir con esta política, a monitorear continuamente el cumplimiento de las medidas de seguridad y salud en el trabajo, ya actualizar las según sea necesario para garantizar la salud y seguridad de todos los involucrados en sus actividades.

6.2.1.6 POLÍTICAS DE USO DEL DATA CENTER

La política de uso del Data Center de la Secretaría de Hacienda Departamental del Amazonas es una medida preventiva que se enfoca en la protección de la información y la infraestructura utilizada para su procesamiento. La política tiene como objetivo garantizar la confidencialidad, disponibilidad e integridad de la información y los activos de la entidad, a través de un conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información alojada en el Data Center.

La Dirección de Informática y Tecnología es responsable de establecer las políticas de uso del Data Center, basada en los principios generales de seguridad y

operación, orientados a la protección de la información, los recursos tecnológicos y el cumplimiento de la misión de la Secretaría de Hacienda Departamental del Amazonas.

Las políticas de uso del Data Center se fundamentan en principios como la confidencialidad, responsabilidad, integridad, confianza, trabajo en equipo, disponibilidad y transparencia de la Gobernación del Amazonas. Estos son esenciales para garantizar la protección de principios de la información y los activos de la entidad.

La Secretaría de Hacienda Departamental del Amazonas se compromete a asignar los recursos necesarios para implementar y mantener estas políticas, a monitorear continuamente el cumplimiento de las mismas ya actualizar las según sea necesario para garantizar la protección de la información y los activos de la entidad.

7 EVALUACIÓN DE LOS RIESGOS E IMPACTOS A LA CONTINUIDAD DEL NEGOCIO CON BASE A LOS LINEAMIENTOS DE LA ISO 22301 Y LA ISO 27001

La información manejada por la Secretaría de Hacienda Departamental del Amazonas es de vital importancia, ya que incluye aspectos presupuestales, contables, financieros y tesorales de la entidad, lo que la cataloga como crítica en caso de pérdida como se puede apreciar en el **ANEXO 4.**

Por lo tanto, es necesario llevar a cabo un Análisis de Impacto de Negocio (BIA, por sus siglas en inglés), un proceso sistemático que permita determinar y evaluar los efectos de cualquier imprevisto que pueda afectar a la continuidad del negocio.

El BIA es un análisis de las posibles consecuencias sobre las operaciones comerciales críticas, accidentes o emergencias, con el objetivo de elaborar un plan de respuesta que permita la continuidad del negocio y la seguridad de la información. Es esencial para el plan de continuidad comercial de cualquier organización y consta de dos componentes básicos: el componente exploratorio, para revelar cualquier vulnerabilidad, y el componente de planificación, para desarrollar estrategias que minimicen el riesgo.

El resultado del BIA es un informe que describe los riesgos potenciales y específicos de la organización. Uno de los supuestos básicos que hay detrás del BIA es que cada elemento que forma parte de la organización depende del funcionamiento continuo de todos los demás componentes. No obstante, algunos son más vulnerables que otros y requieren una mayor protección de fondos después de un desastre.

Por lo tanto, el BIA se diseña con el objetivo de conocer las prioridades, identificando los objetivos de tiempo de recuperación (RTO) y los objetivos de recuperación de punto de (RPO), con una fase previa a la selección de una estrategia y desarrollo de aviones Este análisis permite a la Secretaría de Hacienda Departamental del Amazonas estar preparada ante cualquier eventualidad y asegurar la continuidad de sus operaciones y la protección de su información crítica.

7.1 DESAFÍOS A TENER EN CUENTA PARA REALIZAR UN ANÁLISIS DE IMPACTO DE NEGOCIO

Cuando un profesional se encarga de realizar un Análisis de Impacto de Negocio en una organización, debe considerar una serie de cuestiones esenciales para el éxito del proceso:

Identificar los procesos o actividades críticas en cada departamento, área o unidad de negocio de la empresa y establecer el tiempo máximo que el servicio puede estar interrumpido según los procesos relacionados.

Determinar los periodos máximos admisibles de pérdida de información para garantizar la continuidad del negocio.

Establecer prioridades para la recuperación de la actividad mediante la definición de diferentes dominios.

Cuantificar el impacto que la interrupción de la actividad pueda ocasionar sobre cada unidad de negocio identificada, indicando tiempos máximos para recuperación.

Gestionar una ubicación alternativa para llevar a cabo el servicio, para lo cual es necesario conocer las necesidades de personal, sistemas de información, datos y registros esenciales, así como identificar proveedores y equipamientos necesarios.

Finalmente, implantar un sistema de herencia de máximos que garantice la continuidad del negocio en caso de interrupciones en la actividad.

Estos aspectos son esenciales para llevar a cabo un Análisis de Impacto de Negocio eficiente y efectivo, que permita identificar las vulnerabilidades en la organización y garantizar la continuidad del negocio en caso de imprevistos. De esta forma, la Secretaría de Hacienda Departamental del Amazonas podrá asegurar la protección de su información crítica y la continuidad de sus operaciones.

7.2 PUNTOS CLAVE EN EL ANÁLISIS DE IMPACTO DE NEGOCIO

Aunque no existen estándares formales para realizar un Análisis de Impacto de Negocio, la metodología utilizada suele constar de varias fases que se adaptan a las necesidades de cada organización:

Recopilación de información relevante para el negocio y análisis de los procesos críticos para identificar los componentes y sistemas que los soportan.

Evaluación de la información recopilada para determinar los posibles riesgos, impactos y efectos de una interrupción en el negocio y definir los tiempos máximos admisibles de interrupción.

Preparación de un informe que documente la recopilación y defina los objetivos de recuperación de los procesos críticos.

Presentación de los resultados a la alta dirección para obtener la aprobación de los objetivos y estrategias definidos.

Para llevar a cabo un Análisis de Impacto de Negocio, la organización puede optar por subcontratar a un tercero capacitado o bien, puede formar un equipo interno y externo para el proyecto. En cualquier caso, es importante asegurarse de que el personal encargado del proceso tenga la experiencia necesaria en la materia y la capacitación adecuada en los sistemas y procesos críticos de la organización.

El Análisis de Impacto de Negocio es un proceso esencial para garantizar la continuidad del negocio y la protección de la información crítica en caso de imprevistos. Por lo tanto, es importante que la Secretaría de Hacienda Departamental del Amazonas cuente con un plan de continuidad del negocio sólido y efectivo que permita enfrentar cualquier situación adversa con éxito.

7.3 PROCESO PARA EVALUACION DE RIESGOS Y SUS RESULTADOS.

Para poder hacer un efectuar el proceso de evaluación es necesario tener en cuenta la nomenclatura de la valoración del riesgo (Ver **ANEXO 6**) y con base en este se realiza la matriz de la valoración del riesgo de los activos de información (Ver **ANEXO 7**) que como resultado el proceso de evaluación del riesgo basados en el impacto de negocio; el proceso de evaluación de riesgos para la continuidad del negocio se divide en cuatro fases: Planear, Hacer, Verificar y Actuar. Cada una de estas fases es importante para realizar una evaluación exhaustiva y repetitiva de los activos de información a auditar y garantizar la protección de la información crítica de la organización.

La fase de Planear implica definir los objetivos y metas del proceso de evaluación de riesgos, establecer los criterios de evaluación y definir el equipo de trabajo que llevará a cabo la evaluación.

La fase de Hacer implica la recopilación de información y la identificación de los activos de información crítica de la organización, evaluando los riesgos asociados a cada uno de ellos y determinando su nivel de importancia en la continuidad del negocio.

La fase de Verificar implica la validación de los resultados obtenidos en la fase de Hacer, verificando si se han identificado todos los activos de información crítica y evaluando si los riesgos identificados son los adecuados para garantizar la continuidad del negocio.

Finalmente, la fase de Actuar implica tomar las medidas necesarias para minimizar los riesgos identificados, implementar planes de contingencia y garantizar la protección de la información crítica de la organización.

Es importante destacar que el proceso de evaluación de riesgos es repetitivo y debe realizarse de forma periódica para garantizar que los activos de información crítica de la organización se encuentren siempre protegidos y la continuidad del negocio esté asegurada ante cualquier imprevisto.

8 DISEÑO DE UN PLAN DE TRATAMIENTO DE RIESGOS PARA LA IMPLEMENTACIÓN DE CONTROLES PREVENTIVOS QUE MINIMICEN LA PROBABILIDAD DE OCURRENCIA DE LAS AMENAZAS EN LA SECRETARÍA DE HACIENDA DEPARTAMENTAL DEL AMAZONAS.

El Plan de Tratamiento de Riesgos es un componente fundamental para minimizar los riesgos identificados en el análisis de riesgos de la Secretaría de Hacienda del Departamento del Amazonas. Estos riesgos están relacionados con la pérdida de la privacidad, la integridad y la disponibilidad de los activos de información, lo que podría afectar el logro de los objetivos de la organización como se puede ver en el **ANEXO 8**.

La finalidad del Plan de Tratamiento de Riesgos es evaluar las posibles acciones que se deben tomar para minimizar los riesgos existentes. Para lograr esto, se definirán las medidas de seguridad que se implementarán, así como su nombre, objetivo, justificación, responsable y prioridad. En el caso específico de la Secretaría de Hacienda del Departamento del Amazonas, se han identificado las medidas que se aplicarán durante el primer semestre del año 2022.

Para garantizar que las medidas sean efectivas, se han basado en la información obtenida en el análisis de riesgos y en las necesidades del Proceso de Tecnología del Ministerio TIC en cuanto a la seguridad de la información. De esta manera, se han definido cada una de las características de las medidas y se han establecido los pasos a seguir para su ejecución.

Es importante tener en cuenta que el Plan de Tratamiento de Riesgos es una herramienta dinámica que debe ser actualizada de forma periódica. De esta manera, se asegura la protección de los activos de información crítica de la organización. La implementación efectiva de las medidas definidas en el Plan de Tratamiento de Riesgos permitirá reducir los riesgos y garantizar la continuidad del negocio de la Secretaría de Hacienda del Departamento del Amazonas.

Además, es importante destacar que el Plan de Tratamiento de Riesgos no solo se enfoca en la mitigación de los riesgos, sino que también permite a la organización estar preparada para posibles incidentes de seguridad de la información. Por tanto, es una herramienta clave para garantizar la sostenibilidad del negocio y la confianza de los clientes y usuarios en la organización.

En conclusión, el Plan de Tratamiento de Riesgos es una herramienta fundamental para la gestión de riesgos de la Secretaría de Hacienda del Departamento del Amazonas. Su implementación permitirá garantizar la protección de los activos de información crítica de la organización, así como la continuidad del negocio y la confianza de los clientes y usuarios en la organización.

8.1 PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es un documento esencial para la gestión de los riesgos de seguridad y privacidad de la información en una entidad como se puede apreciar en el **ANEXO 7**. Este plan establece las actividades necesarias para la implementación de controles que permiten a la entidad reducir la probabilidad y el impacto de la materialización de los riesgos, de acuerdo con lo establecido en los estándares ISO 22301 e ISO 27001. El objetivo principal de este plan es preservar la seguridad e integridad de los activos de información de la entidad.

En el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se definen directrices, fechas de ejecución y responsables para lograr un adecuado proceso de administración y evaluación de los riesgos de seguridad y privacidad de la información. Estas directrices incluyen la identificación de los activos de información críticos de la entidad, la evaluación de los riesgos asociados a cada uno de ellos, la implementación de controles para minimizar los riesgos, el monitoreo y la revisión periódica de los controles implementados, y la elaboración de planes de respuesta ante incidentes de seguridad de la información.

La implementación de este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información permite a la entidad proteger sus activos de información crítica y minimizar los riesgos asociados a la seguridad y privacidad de la información. Además, la implementación de los controles definidos en el plan ayuda a la entidad a cumplir con los requisitos de los estándares ISO 22301 e ISO 27001, lo que contribuye a mejorar la imagen y reputación de la entidad ante sus clientes y usuarios.

Es importante tener en cuenta que el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información debe ser un documento dinámico y actualizado periódicamente. Esto se debe a que los riesgos de seguridad y privacidad de la información cambian constantemente y, por lo tanto, los controles implementados también deben ser ajustados y actualizados en consecuencia. De esta manera, la entidad puede garantizar la protección continua de sus activos de información crítica y la sostenibilidad de su negocio.

En conclusión, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es un documento fundamental para la gestión de los riesgos de seguridad y privacidad de la información en una entidad. La implementación de este plan permite a la entidad proteger sus activos de información crítica y cumplir con los estándares ISO 22301 e ISO 27001. Es importante recordar que este plan debe

ser actualizado periódicamente para garantizar la protección continua de los activos de información crítica de la entidad.

8.2 OBJETIVO

desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en conformidad con los estándares ISO 22301 e ISO 27001, con el fin de identificar, evaluar y tratar los riesgos de seguridad y privacidad de la información en la infraestructura tecnológica de la entidad. El plan establecerá medidas y acciones para modificar, reducir o eliminar los riesgos identificados, con el propósito de proteger los activos de información crítica de la entidad y garantizar la continuidad del negocio.

8.3 ALCANCE

Los requisitos, lineamientos y acciones establecidos en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son aplicables de forma anualizada a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la Secretaría de Hacienda Departamental del Amazonas, incluyendo el acceso a los activos de información, sistemas de información e instalaciones físicas de la entidad, los activos de información de la entidad, lineamientos y acciones establecidos en el plan para garantizar la protección y privacidad de la información y la continuidad del negocio de la entidad."

La mejora incluye detalles sobre la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad, así como el alcance de las personas que deben cumplir con los requisitos, lineamientos y acciones establecidos en el plan. Además, se enfatiza en la responsabilidad individual de cada uno de los involucrados en el manejo o acceso a los activos de información de la entidad para garantizar la protección y privacidad de la información y la continuidad del negocio.

8.4 PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La evaluación de riesgos de seguridad y privacidad de la información se basará en la matriz de Activos de Información de la entidad, la cual se asegurará como insumo para implementar el presente Plan. El enfoque principal de la evaluación se centrará en los Activos de Información que han sido clasificados con un alto nivel de confidencialidad, integridad y disponibilidad, de acuerdo con los criterios establecidos en el Plan. Esta evaluación permitirá identificar los riesgos de seguridad y privacidad asociados a estos activos, y definir las medidas de seguridad necesarias para minimizar dichos riesgos y proteger la información de la entidad, según los siguientes criterios

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 1 Criterios de Clasificación

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

Ilustración 2 Criterios De Evaluación

8.5 SENSIBILIZACIÓN INSTITUCIONAL SOBRE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Es fundamental realizar una divulgación adecuada de las políticas y procedimientos de seguridad de la información que deben ser cumplidos por todos los usuarios del sistema en la Secretaría de Hacienda Departamental del Amazonas. Para ello, se deben establecer reglas de comportamiento apropiadas para el uso de los sistemas y la información, que deben ser comunicadas de manera clara y efectiva a todos los usuarios. procedimientos de seguridad.

Es importante destacar que cualquier incumplimiento a las políticas y procedimientos de seguridad debe ser sancionado, siempre y cuando el usuario haya sido capacitado e informado sobre todo el contenido de seguridad

correspondiente a su rol y responsabilidades dentro de la entidad. De esta manera, se garantiza la responsabilidad de cada usuario en la protección de la información y la prevención de incidentes de seguridad.

La capacitación y la información periódica sobre las políticas y procedimientos de seguridad son cruciales para garantizar el cumplimiento de las reglas de comportamiento adecuado para el uso de los sistemas y la información en la entidad. Asimismo, la imposición de sanciones en caso de incumplimiento fomento la cultura de la seguridad de la información y refuerza la importancia del cumplimiento de las políticas y procedimientos de seguridad.

En conclusión, la divulgación adecuada de las reglas de comportamiento para el uso de los sistemas y la información, así como la imposición de sanciones en caso de incumplimiento, son esenciales para garantizar la seguridad y la integridad de los activos de información de la Secretaría de Hacienda Departamental del Amazonas. Es importante que la entidad realice una capacitación periódica y efectiva a los usuarios sobre las políticas y procedimientos de seguridad, con el fin de garantizar el cumplimiento de las normas y fomentar una cultura de la seguridad de la información en toda la entidad.

8.6 ACTUALIZAR EL INVENTARIO DE ACTIVOS DE INFORMACIÓN

La Secretaría de Hacienda Departamental del Amazonas establecerá una metodología para la identificación, clasificación, mantenimiento y actualización del inventario de activos de información, como parte de la debida diligencia que se ha definido en el Modelo de Seguridad y Privacidad de la Información a nivel estratégico. Esta metodología permitirá la gestión efectiva de los activos de información críticos de la entidad y asegurará la continuidad del negocio (Ver **ANEXO 2**.

El inventario de activos de información será registrado en la matriz definida por la entidad, la cual incluirá información relevante sobre los propietarios, custodios y usuarios de los activos de inform/ación identificados en cada vigencia. Esta matriz permitirá la identificación de los activos de información críticos y su priorización en la implementación de medidas de seguridad adecuadas. Asimismo, esta matriz se actualizará de manera periódica para garantizar la actualidad de la información y la eficacia de la gestión de los activos de información.

La metodología para la identificación, clasificación, mantenimiento y actualización del inventario de activos de información es esencial para garantizar la gestión efectiva y la protección de los activos de información críticos de la entidad. La matriz definida por la entidad permitirá una visión clara de los activos de información y su gestión a lo largo del tiempo. De esta manera, se logrará un mayor nivel de

seguridad y privacidad de la información en la Secretaría de Hacienda Departamental del Amazonas.

8.7 ELABORAR PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de implementar de manera efectiva el Modelo de Seguridad y Privacidad de la Información, se realizará una revisión exhaustiva de los procedimientos actuales para identificar las necesidades de documentación y/o actualización de los mismos. Esta revisión permitirá desarrollar y formalizar procedimientos que gestionar la seguridad y privacidad de la información en todos los procesos de la entidad.

La revisión de los procedimientos se enfocará en identificar aquellos que requieren actualización o documentación adicional para cumplir con los requisitos del Modelo de Seguridad y Privacidad de la Información. Se evaluarán los procedimientos existentes y se determinará si es necesario incorporar nuevos procedimientos o ajustar los existentes para garantizar la gestión efectiva de la seguridad y privacidad de la información.

El objetivo de esta actividad es garantizar que la gestión de la seguridad y privacidad de la información esté integrada en todos los procesos de la entidad, y que se cuente con procedimientos adecuados para asegurar la protección de los activos de información crítica. La formalización de los procedimientos y su integración en todos los procesos de la entidad fomentará una cultura de la seguridad de la información y permitirá una gestión más eficiente y efectiva de los activos de información.

En conclusión, la revisión de los procedimientos actuales es un paso crucial para garantizar la implementación efectiva del Modelo de Seguridad y Privacidad de la Información en la entidad. La identificación de necesidades de documentación y/o actualización de procedimientos permitirá desarrollar y formalizar procedimientos adecuados para gestionar la seguridad y privacidad de la información en todos los procesos de la entidad.

8.8 DEFINIR METODOLOGÍA PARA LA GESTIÓN DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Es fundamental que la Secretaría de Hacienda Departamental del Amazonas defina una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que están expuestos los activos, incluyendo la declaración de aplicabilidad.

Para lograr una integración adecuada entre el Modelo de Seguridad y Privacidad de la Información (MSPI) y la guía de gestión del riesgo emitido por el DAFP, se recomienda emplear los criterios de evaluación de impacto y probabilidad, así como los niveles de riesgo emitidos por la Secretaría de Hacienda Departamental. Estos criterios y niveles permitirán una evaluación uniforme y efectiva de los riesgos de seguridad de la información en la entidad, y facilitarán la toma de decisiones para tratar estos riesgos.

La metodología de gestión del riesgo enfocada a permitirá una identificación temprana de los riesgos de seguridad de la información, su evaluación y tratamiento efectivo. Además, la declaración de aplicabilidad permitirá definir los controles de seguridad necesarios para proteger los activos de información crítica de la entidad.

En conclusión, la definición de una metodología de gestión del riesgo enfocada a procesos es esencial para garantizar la gestión efectiva de los riesgos de seguridad de la información en la Secretaría de Hacienda Departamental del Amazonas. La integración de los criterios de evaluación y los niveles de riesgo emitidos por la entidad y la guía del DAFP permitirá una evaluación uniforme y efectiva de los riesgos de seguridad de la información en la entidad, y garantizará la protección de los activos de información críticos de la entidad.

8.9 DEFINIR HERRAMIENTA DEL ANÁLISIS DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN PARA LA IMPLEMENTACIÓN DEL RIESGO

La definición de una herramienta de gestión del riesgo enfocada a procesos es esencial para la Secretaría de Hacienda Departamental del Amazonas. Esta herramienta permitirá la localización y visualización de los recursos de la entidad que se encuentran más en peligro de sufrir daños por algún impacto negativo , y permitirá la toma de decisiones y medidas adecuadas para la reducción de las amenazas.

La herramienta de gestión del riesgo enfocada a procesos debe permitir la identificación temprana de los riesgos de seguridad de la información y su evaluación efectiva. Esta herramienta permitirá una gestión efectiva de los riesgos de seguridad de la información en la entidad, y garantizará la protección de los activos de información crítica.

La visualización de los recursos de la entidad que se encuentran más en peligro de sufrir daños por algún impacto negativo permitirá una priorización adecuada de los recursos y medidas de seguridad necesarias para su protección. Además, la herramienta de gestión del riesgo enfocada a procesos permitirá una evaluación uniforme y efectiva de los riesgos de seguridad de la información en la entidad, y facilitará la toma de decisiones para tratar estos riesgos.

En conclusión, la definición de una herramienta de gestión del riesgo enfocada a procesos es fundamental para garantizar la gestión efectiva de los riesgos de seguridad de la información en la Secretaría de Hacienda Departamental del Amazonas. La herramienta permitirá una identificación temprana de los riesgos de seguridad de la información, su evaluación efectiva y la toma de decisiones adecuadas para su tratamiento y reducción. De esta manera, se garantizará la protección de los activos de información crítica de la entidad.

8.10 ESTABLECER CONTEXTO ESTRATÉGICO

La definición del contexto estratégico debe estar en línea con la misión institucional y objetivos de la entidad, y se enfoca en determinar las amenazas y debilidades que podrían afectar el cumplimiento de dicha misión y objetivos. Esta etapa es orientadora y constituye la base para la identificación del riesgo, ya que de su análisis se obtiene información relevante sobre las causas del riesgo.

Es importante destacar que la administración del riesgo debe ser considerada como una herramienta gerencial y no como algo aislado del accionar administrativo. La definición del contexto estratégico permite una comprensión adecuada del entorno y de los factores internos y externos que pueden generar riesgos, lo que permite la toma de decisiones informadas y la adopción de medidas preventivas y correctivas adecuadas.

En conclusión, la definición del contexto es esencial para la Secretaría de Hacienda Departamental del Amazonas, ya que contribuye al control de la exposición al riesgo y permite una gestión estratégica efectiva de los riesgos de seguridad de la información. La identificación de las amenazas y debilidades permite una comprensión adecuada del entorno y una toma de decisiones informadas, lo que garantiza la protección de los activos de información crítica de la entidad.

8.11 ESTABLECER EQUIPO DE TRABAJO CON ASIGNACIÓN RESPONSABILIDADES

Para una adecuada identificación de los riesgos de seguridad de la información, es necesario que cada responsable de proceso del Sistema Integrado de Gestión identifique a los funcionarios que, por su competencia, pueden ser consideradas claves dentro de cada una de las dependencias que participan en el proceso. Para la selección de estos funcionarios se deben considerar factores como su conocimiento y nivel de toma de decisiones sobre el proceso.

Una vez identificados los funcionarios clave, se debe convocar a una reunión inicial en la que se seguirá el propósito de la actividad y se explicará la importancia de su participación en la identificación de los riesgos de seguridad de la información.

Durante esta reunión, se deberán establecer los objetivos, alcances y metodologías para la identificación de los riesgos de seguridad de la información.

Es importante que se promueva la participación activa de los funcionarios seleccionados en el proceso de identificación de los riesgos de seguridad de la información, ya que esto garantizará una mayor precisión en la identificación de los riesgos y permitirá una gestión efectiva de los mismos. Además, se deben establecer los roles y responsabilidades de cada uno de los participantes en la identificación de los riesgos de seguridad de la información.

En conclusión, la identificación de los riesgos de seguridad de la información requiere la participación activa de los funcionarios clave de cada proceso. La convocatoria a una reunión inicial y la definición de objetivos, alcances y metodologías son fundamentales para el éxito del proceso de identificación de los riesgos. La participación activa de los funcionarios seleccionados garantizará una mayor precisión en la identificación de los riesgos y permitirá una gestión efectiva de los mismos.

8.12 IDENTIFICACIÓN DE RIESGOS

La etapa de identificación de riesgos es fundamental para conocer los eventos potenciales que ponen en riesgo el logro de la misión de la entidad pública, ya sea que estén o no bajo su control. Durante esta etapa, se deben identificar las causas y consecuencias de la ocurrencia del riesgo, lo que permite una comprensión adecuada del riesgo y una gestión efectiva del mismo.

Es importante destacar que la identificación de riesgos debe ser una actividad sistemática y rigurosa, que involucre a todos los responsables de los procesos de la entidad pública. Durante esta etapa, se deben considerar los eventos internos y externos que pueden afectar el logro de la misión de la entidad, así como los factores que pueden generar riesgos en los procesos críticos de la entidad.

La identificación de riesgos también permite la definición de los criterios de evaluación y clasificación de los riesgos, lo que facilita su tratamiento y gestión efectiva. Es importante que se realice una revisión periódica de la identificación de riesgos, con el fin de mantenerla actualizada y garantizar la protección de los activos de información crítica de la entidad.

En conclusión, la identificación de riesgos es una etapa fundamental en la gestión de riesgos de seguridad de la información en una entidad pública. Esta etapa permite una comprensión adecuada del riesgo y una gestión efectiva del mismo, lo que garantiza la protección de los activos de información crítica de la entidad.

8.13 ANÁLISIS DE RIESGOS

El análisis del riesgo es una etapa clave en la gestión de riesgos de seguridad de la información, ya que permite establecer la probabilidad de ocurrencias del riesgo y sus consecuencias, calificándolos y evaluándolos para obtener información relevante que permita establecer el nivel de riesgo.

Durante el análisis del riesgo, se deben tener en cuenta dos aspectos fundamentales: la probabilidad y el impacto. La probabilidad se refiere a la posibilidad de ocurrencias del riesgo, la cual puede ser medida con criterios de frecuencia, si el riesgo se ha materializado en el pasado, o de factibilidad, teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado aún.

Por otro lado, el impacto se refiere a las consecuencias que la materialización del riesgo puede ocasionar a la Secretaría de Hacienda Departamental del Amazonas. Estas consecuencias pueden ser económicas, operativas, legales o reputacionales, entre otras.

Es importante destacar que el análisis del riesgo debe ser una actividad rigurosa y sistemática, que involucre a todos los responsables de los procesos críticos de la entidad pública. Es necesario establecer criterios claros para la calificación y evaluación de los riesgos identificados, lo que facilitará la toma de decisiones y la definición de medidas de control y mitigación adecuadas.

En conclusión, el análisis del riesgo es una etapa fundamental en la gestión de riesgos de seguridad de la información en una entidad pública. La consideración de la probabilidad y el impacto permite establecer el nivel de riesgo y definir medidas de control y mitigación adecuada para proteger los activos de información crítica de la entidad.

8.14 VALORACIÓN DE RIESGOS

La etapa de evaluación y tratamiento de riesgos es fundamental en la gestión de riesgos de seguridad de la información en una entidad pública. Esta etapa busca identificar los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencias o el impacto del riesgo, confrontando la evaluación del riesgo con los controles de los procesos críticos de la entidad.

Durante la evaluación de los controles, se deben identificar aquellos que son efectivos y aquellos que deben ser mejorados o mejorados para garantizar una gestión efectiva del riesgo. Es importante tener en cuenta que la evaluación de los controles debe ser sistemática y rigurosa, involucrando a todos los responsables de los procesos críticos de la entidad pública.

Una vez evaluados los controles, se debe determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Esta opción puede ser aceptar el riesgo, implementar controles adicionales, transferir el riesgo a un tercero o evitar el riesgo mediante la eliminación de la fuente del mismo.

Es importante destacar que la evaluación y tratamiento de riesgos debe ser una actividad periódica y actualizada, con el fin de garantizar la protección de los activos de información crítica de la entidad pública.

En conclusión, la evaluación y tratamiento de riesgos es una etapa fundamental en la gestión de riesgos de seguridad de la información en una entidad pública. Esta etapa busca identificar los controles efectivos y definir la opción de manejo del riesgo, garantizando la protección de los activos de información crítica de la entidad.

8.15 EVALUACIÓN DE CONTROLES

La evaluación de los controles identificados es una etapa fundamental en la gestión de riesgos de seguridad de la información en una entidad pública. Esta etapa permite determinar en qué medida los controles están contribuyendo a disminuir los niveles de probabilidad e impacto del riesgo.

Durante la evaluación de los controles, se debe verificar su documentación, aplicación y efectividad. Es importante asegurarse de que los controles estén bien documentados, se estén aplicando de manera adecuada y efectiva en los procesos críticos de la entidad pública.

Para evaluar la efectividad de los controles, se pueden realizar pruebas o simulaciones para verificar si están funcionando correctamente y si son capaces de reducir el riesgo de manera efectiva. Además, se debe involucrar a los responsables de los procesos críticos de la entidad pública en la evaluación de los controles para asegurar que se está evaluando la realidad de los procesos y los riesgos asociados.

La evaluación de los controles debe ser sistemática y rigurosa, asegurando la calidad de los resultados obtenidos y la toma de decisiones efectivas. Los resultados de la evaluación de los controles deben ser utilizados para definir la evaluación del riesgo residual y definir la opción de manejo del riesgo.

En conclusión, la evaluación de los controles es una etapa clave en la gestión de riesgos de seguridad de la información en una entidad pública. Esta etapa permite verificar la documentación, aplicación y efectividad de los controles identificados y determinar su capacidad para mitigar el riesgo. Los resultados obtenidos en la evaluación de los controles son utilizados para definir la evaluación del riesgo residual y definir la opción de manejo del riesgo.

8.16 SOCIALIZACIÓN Y COMUNICACIÓN POLÍTICAS DE RIESGOS

La divulgación de las políticas de tratamiento de riesgos de seguridad y privacidad de la información es una actividad fundamental en la gestión de riesgos de la Secretaría de Hacienda Departamental del Amazonas. Esta actividad tiene como objetivo dar a conocer a funcionarios, contratistas y terceros de la entidad las políticas y procedimientos de seguridad de la información que deben cumplirse para reducir los riesgos identificados.

La divulgación de las políticas y procedimientos de seguridad de la información se puede realizar mediante charlas y el uso de herramientas de comunicación disponibles en la entidad, como correos electrónicos, videos, infografías, entre otros. Es importante asegurarse de que la información sea clara, concisa y accesible para todos los involucrados en los procesos críticos de la entidad.

Es recomendable que la divulgación se realice de manera periódica para asegurarse de que todos los funcionarios, contratistas y terceros estén actualizados sobre las políticas y procedimientos de seguridad de la información de la entidad. Además, se debe realizar un seguimiento para asegurarse de que se están cumpliendo las políticas y procedimientos establecidos y, en caso de incumplimientos, se deben aplicar las sanciones correspondientes.

En conclusión, la divulgación de las políticas y procedimientos de seguridad de la información es una actividad clave en la gestión de riesgos de la Secretaría de Hacienda Departamental del Amazonas. Esta actividad permite que todos los involucrados en los procesos críticos de la entidad conozcan las políticas y procedimientos de seguridad de la información que deben cumplirse para reducir los riesgos identificados. Es importante realizar la divulgación de manera periódica y realizar un seguimiento para asegurarse de que se están cumpliendo las políticas y procedimientos establecidos.

8.17 MONITOREO Y REVISIÓN AL TRATAMIENTO DE LOS RIEGOS

El monitoreo y revisión de las acciones establecidas en los mapas de riesgo son fundamentales para asegurar que se están llevando a cabo y evaluar su eficacia en la gestión de riesgos de la Secretaría de Hacienda Departamental del Amazonas. Esta actividad permite adelantar revisiones sobre la marcha para evidenciar situaciones o factores que puedan influir en la implementación de acciones preventivas.

Durante el monitoreo y revisión, se deben evaluar los avances y resultados obtenidos en la implementación de las acciones preventivas establecidas en los mapas de riesgo. Es importante revisar la efectividad de los controles implementados y verificar si se están cumpliendo los objetivos establecidos. En caso

de que se detecten desviaciones, se deben tomar acciones correctivas para asegurar que se están cumpliendo los procedimientos y políticas establecidas.

Es recomendable que el monitoreo y revisión se realice de manera periódica, para garantizar que las acciones preventivas están siendo implementadas de manera efectiva y para identificar nuevos riesgos que puedan surgir. Además, es importante involucrar a todos los actores relevantes en la gestión de riesgos de la entidad, para asegurarse de que todos están alineados y comprometidos con la gestión de riesgos.

En conclusión, el monitoreo y revisión son actividades clave en la gestión de riesgos de la Secretaría de Hacienda Departamental del Amazonas. Estas actividades permiten evaluar la efectividad de las acciones preventivas establecidas en los mapas de riesgo y tomar acciones correctivas en caso de desviaciones. Es importante realizar el monitoreo y revisión de manera periódica e involucrar a todos los actores relevantes en la gestión de riesgos de la entidad.

8.18 TERMINOLOGÍA

Los siguientes términos son utilizados en el contexto de la gestión de la seguridad de la información y aplican para todas sus fases y momentos, incluyendo la gestión de riesgos.

8.19 ADMINISTRACIÓN DEL RIESGO:

La administración del riesgo se refiere al conjunto de elementos de control que, al interrelacionarse, brindarán a la entidad la capacidad de emprender acciones necesarias para manejar eventos que puedan afectar negativamente el logro de los objetivos institucionales y proteger la de los efectos ocasionados por su ocurrencia.

Esta práctica de gestión implica la identificación, evaluación y tratamiento de riesgos, y se aplica en todos los niveles de la organización. Se busca minimizar la probabilidad y el impacto de los riesgos en la entidad, y para ello se utilizan diferentes estrategias de tratamiento, como la transferencia, reducción, retención o eliminación del riesgo.

La administración del riesgo también implica la implementación de controles preventivos y correctivos para reducir la probabilidad de ocurrencias de los eventos negativos y reducir su impacto. Estos controles pueden ser de diferentes tipos, como técnicos, físicos, administrativos o legales.

En resumen, la administración del riesgo es una práctica de gestión integral que busca proteger a la entidad de los efectos negativos de los eventos que pueden afectar su desempeño y logro de objetivos. Se basa en la identificación, evaluación, tratamiento y control de los riesgos en todos los niveles de la organización.

8.20 ACTIVO DE INFORMACIÓN:

La Política de Seguridad de la Información y Seguridad Digital de la Secretaría de Hacienda Departamental del Amazonas se aplica a todos sus servidores públicos, contratistas, proveedores, operadores, entidades adscritas y cualquier persona o tercero que, en razón del cumplimiento de sus funciones en la Secretaría, compartan, utilicen, recolecten, procesen, intercambien o consulten su información. Esto incluye a las entidades de control y demás entidades relacionadas que acceden, ya sea interna o externamente, a cualquier activo de información, independientemente de su ubicación.

Asimismo, esta política se aplica a toda la información creada, procesada o utilizada por la Secretaría de Hacienda Departamental del Amazonas, sin importar el medio, formato, presentación o lugar en el que se encuentre.

La Política de Seguridad de la Información y Seguridad Digital de la Secretaría de Hacienda Departamental del Amazonas tiene como objetivo la adopción e implementación del Modelo de Seguridad y Privacidad de la Información en el marco del Subsistema de Gestión de Seguridad de la Información. Este modelo protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en la Entidad Departamental, conforme a lo estipulado en el mapa de procesos. Se realiza mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, garantizar la continuidad de la operación de los servicios tecnológicos y cumplir con los requisitos legales, reglamentarios y regulatorios.

Esta política está orientada a la mejora continua y al alto desempeño del Subsistema de Gestión de Seguridad de la Información, promoviendo el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones (TIC) a través de políticas y programas que busquen mejorar la calidad de vida de los ciudadanos y el incremento sostenible del desarrollo del Departamento del Amazonas.

8.21 ANÁLISIS DE RIESGOS:

El análisis de riesgos es esencial para garantizar la seguridad de la información y proteger los activos críticos de una organización. Este proceso no solo implica identificar los riesgos, sino también evaluar su probabilidad de ocurrencias y su impacto en la organización, para así poder tomar medidas adecuadas para minimizar o eliminar las consecuencias negativas.

Es importante destacar que el análisis de riesgos es un proceso continuo, que debe ser revisado y actualizado periódicamente para asegurar que las medidas de seguridad sigan siendo efectivas y adecuadas ante los posibles cambios en el entorno de la organización.

La norma ISO/IEC 27000 brinda una guía útil para la realización del análisis de riesgos en el contexto de la seguridad de la información. Esta norma establece los principios y directrices que se deben seguir para llevar a cabo un análisis de riesgos efectivo, incluyendo la participación activa y colaborativa de los diferentes niveles de la organización y la definición de medidas adecuadas para minimizar los riesgos identificados.

En resumen, el análisis de riesgos es una herramienta clave para la gestión de la seguridad de la información, que permite a las organizaciones identificar y evaluar los riesgos y tomar las medidas adecuadas para minimizarlos. La norma ISO/IEC 27000 establece los principios y directrices que se deben seguir para llevar a cabo un análisis de riesgos efectivo y garantizar la protección de los activos críticos de la organización.

8.21.1 AMENAZA:

La identificación de las fuentes de riesgo permite a la organización entender mejor las posibles amenazas que enfrenta en su entorno y en su operación diaria, lo que a su vez facilita la definición de medidas de seguridad y la implementación de controles adecuados. Es importante que la identificación de las fuentes de riesgo sea un proceso continuo, ya que las condiciones y amenazas cambien constantemente, y lo que podría haber sido una fuente de riesgo baja en el pasado, podría convertirse en un riesgo significativo en el futuro. La norma ISO/IEC 27001 establece los requisitos para la identificación y evaluación de las fuentes de riesgo en el contexto de la seguridad de la información.

8.21.2 CAUSA:

En el contexto de la gestión de riesgos, se define una causa como cualquier elemento o factor que pueda dar origen a un evento no deseado o situación de riesgo para la organización. Las causas pueden provenir de diversas fuentes o agentes generadores, tales como personas, métodos, herramientas, entorno, aspectos económicos, insumos, materiales, entre otros. Es importante identificar y evaluar adecuadamente estas causas para implementar medidas preventivas o correctivas que reduzcan la probabilidad o el impacto de la materialización del riesgo.

8.21.3 CONFIDENCIALIDAD:

Es una de las tres principales propiedades de la seguridad de la información, junto con la integridad y la disponibilidad. La confidencialidad se refiere a la capacidad de proteger la información de revelarse o ser accedida por personas, entidades o procesos no autorizados. Esta propiedad se aplica a cualquier tipo de información, ya sea personal, financiera, de negocios, gubernamental, entre otros.

8.21.4 CRITERIOS DEL RIESGO:

Son los criterios o estándares según los cuales se evalúa la importancia de un riesgo. Estos términos establecen los parámetros para la evaluación de los riesgos y permiten determinar su nivel de relevancia y prioridad en relación con los objetivos y metas de la organización.

8.21.5 CONTROL:

Medida que modifica el riesgo. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

8.21.6 DECLARACIÓN DE APLICABILIDAD:

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

8.21.7 DISPONIBILIDAD:

Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

8.21.8 EVENTO:

Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico. Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

8.21.9 EVITACIÓN DEL RIESGO:

Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

8.21.10 FACTORES DE RIESGO:

Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

8.21.11 GESTIÓN DEL RIESGO:

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

9 POLÍTICAS Y MEDIDAS DE SEGURIDAD

A continuación, se procede con la elaboración de la política general de seguridad de la información, contempla los principios básicos a tener en cuenta en su elaboración dentro de la planeación del sistema de gestión de seguridad de la información en una entidad.

9.1 OBJETIVOS COMERCIALES:

9.1.1 MEJORAR LA CONTINUIDAD DEL NEGOCIO:

Garantizar que la Secretaría de Hacienda Departamental del Amazonas pueda mantener sus operaciones incluso en escenarios críticos, minimizando interrupciones y pérdidas económicas.

9.1.2 FORTALECER LA CONFIANZA DEL CLIENTE:

Asegurar a los ciudadanos y las partes interesadas externas que la información y los recursos gestionados por la Secretaría de Hacienda están protegidos y disponibles de manera confiable, lo que contribuye a la confianza en los servicios gubernamentales.

9.1.3 CUMPLIR CON REQUISITOS LEGALES Y REGULATORIOS:

Asegurarse de que la Secretaría cumple con todas las normativas y regulaciones relacionadas con la seguridad de la información y la continuidad del negocio, evitando posibles sanciones o penalizaciones.

9.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN:

9.2.1 MEJORAR LA DETECCIÓN DE INCIDENTES:

Implementar sistemas y herramientas de monitoreo avanzados que permitan la detección temprana de posibles amenazas y actividades sospechosas en los sistemas de información.

9.2.2 OPTIMIZAR LA RESPUESTA A INCIDENTES:

Establecer procedimientos claros y eficaces para responder de manera oportuna y efectiva a incidentes de seguridad, minimizando su impacto y reduciendo los tiempos de recuperación.

9.2.3 GARANTIZAR LA RECUPERACIÓN DE DATOS CRÍTICOS:

Desarrollar planes de recuperación ante desastres que aseguren la disponibilidad y la integridad de los datos y sistemas esenciales para la Secretaría de Hacienda.

9.3 REQUISITOS DE LAS PARTES INTERESADAS:

9.3.1 PARTES INTERESADAS INTERNAS:

El personal de la Secretaría debe estar capacitado en seguridad de la información y ser consciente de las políticas y procedimientos de respuesta a incidentes.

9.3.2 PARTES INTERESADAS EXTERNAS:

Los ciudadanos, proveedores y otras partes interesadas externas pueden requerir información sobre las medidas de seguridad implementadas y la capacidad de recuperación de la Secretaría en caso de incidentes.

9.3.3 ENTIDADES REGULADORAS:

Cumplir con los requisitos de entidades reguladoras y autoridades gubernamentales que supervisan y regulan la seguridad de la información y la continuidad del negocio en el sector público.

Estos objetivos y requisitos proporcionan una base sólida para el desarrollo de políticas y medidas de seguridad que mejoren la detección, respuesta y recuperación de incidentes críticos en la Secretaría de Hacienda Departamental del Amazonas.

9.4 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La implementación de un sistema de gestión de seguridad de la información es una iniciativa clave para garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la Secretaría de Hacienda Departamental del Amazonas. Esta medida busca no solo cumplir con las leyes y la aplicación correspondiente, sino también establecer un marco de confianza y transparencia en la gestión de la información, lo que a su vez contribuirá al fortalecimiento de la imagen y la reputación de la entidad ante los ciudadanos y otros organismos públicos. La implementación de este sistema de gestión de seguridad de la información refleja el compromiso de la dirección de la Secretaría de Hacienda Departamental del Amazonas en la protección de los activos de información y la minimización de los riesgos asociados a su gestión. Este compromiso se traduce en la definición de políticas y procedimientos claros para la gestión de la información, la identificación

y evaluación de los riesgos asociados a los activos de información, la definición de medidas preventivas y correctivas, y la capacitación y sensibilización del personal en materia de seguridad de la información.

Para La Secretaria De Hacienda Departamental Del Amazonas, la protección de la información es una prioridad, y busca garantizar la integridad, confidencialidad y disponibilidad de sus activos de información, de acuerdo con las necesidades de los diferentes grupos de interés identificados. Con este objetivo en mente, se han establecido los principios siguientes para el desarrollo de acciones y toma de decisiones en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

Minimizar el riesgo en las funciones más importantes de la entidad.

Cumplir con los principios de seguridad de la información.

Cumplir con los principios de la función administrativa.

Mantener la confianza de clientes, socios y empleados.

Apoyar la innovación tecnológica.

Proteger los activos tecnológicos.

Establecer políticas, procedimientos e instructivos en materia de seguridad de la información.

Fortalecer la cultura de seguridad de la información en funcionarios, terceros, aprendices, practicantes y clientes.

Garantizar la continuidad del negocio frente a incidentes.

La Secretaria De Hacienda Departamental Del Amazonas ha decidido definir, implementar, operar y mejorar de forma continua en SGSI, alineado a las necesidades del negocio y los requerimientos regulatorios.

Además, para cumplir con los objetivos del proyecto del SGSI, se han establecido otras políticas específicas de seguridad y privacidad de la información, tales como la gestión de activos, seguridad física y ambiental, control de accesos, entre otras. Estas políticas están descritas en la "Guía de políticas específicas de seguridad y privacidad de la información", y son necesarias y primordiales para garantizar una gestión integral de la seguridad de la información en la entidad.

9.5 PRINCIPIOS DE SEGURIDAD QUE RESPALDAN EL SGSI DE LA SECRETARÍA DE HACIENDA DEPARTAMENTAL DEL AMAZONAS

Las responsabilidades en relación con la seguridad de la información serán definidas, comunicadas, publicadas y aceptadas por todos los empleados, proveedores, socios de negocio y terceros.

La Secretaría protegerá la información generada, procesada o resguardada por sus procesos de negocio, infraestructura tecnológica y activos frente a riesgos derivados del acceso obtenido a terceros (por ejemplo, proveedores o clientes) o como resultado de servicios internos subcontratados (outsourcing).

La Secretaría protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio para minimizar los impactos financieros, operativos o legales debido a un uso inadecuado de la misma. Para ello, es esencial aplicar controles según la clasificación de la información de su propiedad o bajo custodia.

La Secretaría protegerá su información de las amenazas provenientes del personal.

La Secretaría protegerá las instalaciones de procesamiento y la infraestructura tecnológica que respaldarán sus procesos críticos.

La Secretaría controlará la operación de sus procesos de negocio, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

La Secretaría implementará controles de acceso a la información, sistemas y recursos de red.

La Secretaría garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La Secretaría garantizará la mejora efectiva de su modelo de seguridad mediante una adecuada gestión de eventos de seguridad y debilidades asociadas con los sistemas de información.

La Secretaría garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación, considerando el impacto que pueden generar los eventos.

La Secretaría garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

9.6 FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la Secretaria de Hacienda Departamental del Amazonas.

9.7 IMPORTANCIA DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la Secretaria de Hacienda Departamental del Amazonas.

9.8 FASES DE IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

9.8.1 DESARROLLO DE LAS POLÍTICAS:

En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

9.8.2 JUSTIFICACIÓN DE LA CREACIÓN DE POLÍTICA:

Debe identificarse el por qué la Secretaria de Hacienda Departamental del Amazonas requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.

9.8.3 ALCANCE:

Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?

9.8.4 ROLES Y RESPONSABILIDADES:

Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

9.8.5 REVISIÓN DE LA POLÍTICA:

Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.

9.8.6 APROBACIÓN DE LA POLÍTICA:

Se debe determinar al interior de la entidad Departamental, la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de las mismas. Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.

9.9 CUMPLIMIENTO:

Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

9.10 COMUNICACIÓN:

Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas y/o terceros de la Secretaria de Hacienda Departamental del Amazonas debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

9.11 MONITOREO:

Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

9.12 MANTENIMIENTO:

Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

9.13 RETIRO:

Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Secretaria de Hacienda Departamental. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

9.14 POLÍTICAS ESPECÍFICAS RECOMENDADAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

En este documento presenta algunas recomendaciones de políticas de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para la Secretaria de Hacienda Departamental del Amazonas. Este conjunto de recomendaciones no es exhaustivo, se aconseja que la SH genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar. A continuación, se agruparán las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la secretaria.

9.14.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información. Debe tener los siguientes elementos:

¿Quiénes conforman el comité directivo de seguridad de la información?

Objetivos: Se deben especificar los objetivos del comité como por ejemplo el mejoramiento continuo de los programas o las distintas actividades que se realizarán en dichos comités, verificación de avance de los distintos proyectos, la revisión del documento de la política de seguridad etc…

Cumplimiento: Debe establecerse que dicho comité verifique el cumplimiento de las políticas.

9.15 GESTIÓN DE ACTIVOS

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

9.15.1 IDENTIFICACIÓN DE ACTIVOS:

Esta política debe determinar la periodicidad con la cual se va a realizar al interior de la secretaria la identificación y/o actualización del inventario de Activos de Información, la política debe determinar el responsable de realizar la actividad, se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.

9.15.2 CLASIFICACIÓN DE ACTIVOS:

La Secretaria Departamental del Amazonas debe determinar la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma. En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Secretaria, algunos ejemplos: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo a la naturaleza.

9.15.3 ETIQUETADO DE LA INFORMACIÓN:

Esta política debe determinar el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.

9.15.4 DEVOLUCIÓN DE LOS ACTIVOS:

Esta política debe determinar el instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Secretaria de Hacienda Departamental del Amazonas.

9.15.5 GESTIÓN DE MEDIOS REMOVIBLES:

Esta política debe contemplar los usos y permisos que tienen los usuarios y/o funcionarios de la Secretaria de Hacienda Departamental del Amazonas frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. Esta política debe describir detenidamente en qué casos se autoriza y en los que no, el uso de medios removibles y los procedimientos en los cuales se

determinen las autorizaciones; adicionalmente debe describir el responsable de las autorizaciones y responsabilidades de aquellas personas que tienen autorización para el uso del dicho medio de almacenamiento. El uso de medios removibles en la entidad debe ir alineados a las clasificaciones de activos dispuestas en la política de “Clasificación de Activos”.

9.15.6 DISPOSICIÓN DE LOS ACTIVOS:

Esta política debe determinar la obligatoriedad para la construcción y cumplimiento de un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos. Esta política debe determinar la toma de backup de los activos evitando así el acceso o borrado no autorizado de la información, la política debe indicar quien es el responsable de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.

9.15.7 DISPOSITIVOS MÓVILES:

Esta política debe determinar los funcionarios, contratistas o terceros que pueden tener acceso a las redes inalámbricas, quiénes pueden realizar instalación de chats corporativos y/o correos electrónicos de la entidad mediante el uso de este tipo de dispositivos, adicionalmente debe describir las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles así como como los controles de seguridad que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

9.16 CONTROL DE ACCESO

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales la Secretaria de Hacienda Departamental del Amazonas determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos; las políticas relacionadas con el control de acceso deben contemplar como mínimo:

9.16.1 CONTROL DE ACCESO CON USUARIO Y CONTRASEÑA:

Se debe elaborar una política sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la Secretaria de Hacienda Departamental del Amazonas, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. La política debe enunciar las responsabilidades que los funcionarios, contratistas o terceros tienen al contar con un usuario o contraseña de

la entidad, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La entidad debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.

9.16.2 SUMINISTRO DEL CONTROL DE ACCESO:

Esta política debe determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la Secretaria de Hacienda Departamental del Amazonas.

9.16.3 GESTIÓN DE CONTRASEÑAS:

Esta política debe definir los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la Secretaria de Hacienda Departamental del Amazonas. Esta política debe indicar a los funcionarios, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña, debe determinar que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.

9.16.4 PERÍMETROS DE SEGURIDAD:

La política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuáles no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

9.16.5 ÁREAS DE CARGA:

La política debe definir las condiciones e instalaciones físicas en las cuales se va a realizar despacho y carga de paquetes físicos para bodegas o espacios definidos de carga, esto con el fin de evitar el acceso no autorizado a otras áreas de la Secretaria de Hacienda Departamental del Amazonas. Esta política debe determinar el seguimiento que se debe realizar para garantizar el cumplimiento de dicha política y sus correspondientes responsables.

9.17 NO REPUDIO

La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción. La política deberá incluir mínimo los siguientes aspectos:

9.18 TRAZABILIDAD:

Se implementará una política de trazabilidad de acciones para realizar un seguimiento detallado de la creación, origen, recepción, entrega y otras acciones relacionadas con la información. Esto permitirá garantizar la transparencia y la integridad en el manejo de la información, así como la identificación y solución de posibles errores o fallas en el proceso. Se establecerán procedimientos claros y precisos para la documentación y registro de las acciones, así como la eliminación de responsabilidades para cada etapa del proceso. De esta manera, se podrá garantizar una gestión eficiente y eficaz de la información, en cumplimiento con los objetivos y multas de la entidad.

9.18.1 RETENCIÓN:

La política debe establecer el período de retención o almacenamiento de las acciones realizadas por los usuarios en los sistemas de información y plataformas digitales de la Secretaría de Hacienda Departamental del Amazonas. Este período deberá ser informado de manera oportuna a todos los funcionarios, contratistas y terceros que tengan acceso a dicha información, con el fin de garantizar el cumplimiento de las normas legales y reglamentarias aplicables en materia de protección de datos personales y seguridad de la información. Asimismo, se deberán establecer los procedimientos necesarios para la eliminación segura y definitiva de la información una vez que se cumpla el periodo de retención establecido en la política.

9.18.2 AUDITORÍA:

La política realizó la realización de auditorías continuas como un procedimiento para verificar que las partes implicadas no nieguen haber realizado alguna acción y así garantizar la transparencia y la honestidad en el manejo de la información.

9.18.3 INTERCAMBIO ELECTRÓNICO DE INFORMACIÓN:

La política de seguridad de la información de la Secretaría de Hacienda Departamental del Amazonas debe incluir la consideración de los servicios de intercambio electrónico de información como una herramienta de garantía de no repudio en los casos que aplique. Esto implica que se debe establecer un protocolo de uso de estos servicios y garantizar que se cumplan los estándares de seguridad necesarios para garantizar la autenticidad, integridad y disponibilidad de la

información intercambiada. Asimismo, se deben establecer procedimientos para la verificación de las transacciones realizadas a través de estos servicios y la resolución de cualquier controversia que pudiera surgir. Es importante destacar que la inclusión de estos servicios en la política de seguridad de la información debe ser complementada con medidas de seguridad adicionales,

9.18.4 PRIVACIDAD Y CONFIDENCIALIDAD

La política debe incluir una descripción detallada de las políticas de tratamiento y protección de datos personales, las cuales deben ser aplicadas de acuerdo con la normatividad vigente. Asimismo, es importante que la política de privacidad contemple al menos los siguientes aspectos:

9.19 ÁMBITO DE APLICACIÓN

El ámbito de aplicación de la política de privacidad y protección de datos personales para todos los funcionarios, contratistas y terceros que tengan acceso a la información será personal y datos sensibles de los ciudadanos que son gestionados por la Secretaría de Hacienda Departamental del Amazonas. La política también se aplicará a todas las actividades y procesos en los cuales se maneje información personal y datos sensibles, ya sea en formato físico o digital.

9.19.1 EXCEPCIÓN AL ÁMBITO DE APLICACIÓN DE LAS POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

Las excepciones al ámbito de aplicación de las políticas de tratamiento de datos personales están contempladas en la normatividad vigente y pueden variar de acuerdo a la legislación de cada país. En general, estas excepciones se refieren a situaciones en las que el tratamiento de datos personales está permitido sin necesidad de contar con el consentimiento del titular de los datos, como por ejemplo cuando se trata de datos relacionados con la seguridad nacional, defensa y orden público, o cuando se requiera el tratamiento de datos para el cumplimiento de una obligación legal o contractual. Sin embargo, es importante tener en cuenta que estas excepciones deben ser interpretadas de manera restrictiva y en consonancia con los principios de protección de datos personales y la normatividad aplicable.

9.19.2 PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

Los del tratamiento de datos personales son un conjunto de reglas éticas y legales que fundamentan cómo deben ser manejados los datos personales de las personas. Estos son esenciales para garantizar la protección de los principios personales fundamentales de los titulares de los datos y para que las empresas, organizaciones y entidades gubernamentales puedan cumplir con las normas establecidas en la

materia. Los principales principios del tratamiento de datos personales son los siguientes:

9.19.2.1 PRINCIPIO DE LA LEGALIDAD:

El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.

9.19.2.2 PRINCIPIO DE FINALIDAD:

Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.

9.19.2.3 PRINCIPIO DE LIBERTAD:

El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.

9.19.2.4 PRINCIPIO DE VERACIDAD O CALIDAD:

La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

9.19.2.5 PRINCIPIO DE TRANSPARENCIA:

Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.

9.20 PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA:

El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.

9.20.1 PRINCIPIO DE SEGURIDAD:

La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

9.20.2 PRINCIPIO DE CONFIDENCIALIDAD:

Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

9.21 AUTORIZACIÓN DEL TITULAR

La política debe establecer los procedimientos para obtener la autorización del titular de los datos personales para su tratamiento, garantizando que se cumplan todos los requisitos legales y que se respeten los derechos de los titulares. Asimismo, la política debe definir las excepciones en las cuales no se requiere la autorización del titular para el tratamiento de sus datos personales, en cumplimiento de lo establecido en la normatividad vigente. Es importante que los procedimientos para obtener la autorización y las excepciones estén debidamente documentados y se informe a los titulares de los datos personales.

9.21.1 DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO

La política debe indicar cuales son los deberes de los responsables y/o encargados del tratamiento de los datos personales.

9.21.2 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

La presente política establece la importancia de garantizar la confidencialidad y autenticidad de la información que circula o se genera a través de los diferentes sistemas de información de la Secretaría de Hacienda Departamental del Amazonas. Para ello, se establece un compromiso o acuerdo de confidencialidad que todo oficial, contratista y/o tercero vinculado a la entidad debe firmar, en el cual se compromete a no divulgar la información interna y externa que conozca de la entidad, así como la relacionada con las funciones que realiza en la misma.

Este acuerdo de confidencialidad es de carácter obligatorio y deberá ser firmado por todo oficial, contrato y/o tercero en el momento de su vinculación o ingreso a la entidad. Su vigencia será durante el tiempo en que se mantenga la relación laboral o contractual con la entidad, y se extenderá incluso después de su terminación.

La política también establece las medidas necesarias para garantizar la autenticidad de la información, a través de la implementación de controles de acceso y la identificación y autenticación de los usuarios que acceden a la información. De esta forma, se busca prevenir la divulgación no autorizada de la información y asegurar su integridad y confiabilidad.

Es responsabilidad de todo el personal de la Secretaría de Hacienda Departamental del Amazonas cumplir con las medidas de seguridad y confidencialidad establecidas en la presente política, así como garantizar la protección de la información y datos personales de los titulares, de acuerdo con lo establecido en la normatividad vigente en materia de protección de datos personales.

9.22 INTEGRIDAD

La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que forman parte de la Secretaría de Hacienda Departamental del Amazonas. Esta política se refiere al manejo íntegro e integral de la información, tanto interna como externa, que es conocida o administrada por ellos.

De esta manera, toda la información verbal, física o electrónica debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente y exclusivamente a las personas correspondientes ya través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y /o responsable de dicha información. En el caso de vinculación contractual, el compromiso de administración y manejo íntegro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

La política de aparato también debe establecer la vigencia del compromiso, de acuerdo con el tipo de vinculación del personal al que se aplica el cumplimiento.

9.23 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La Secretaría de Hacienda Departamental del Amazonas debe implementar un plan de continuidad del negocio para garantizar la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y los procesos misionales, en caso de un incidente de seguridad de la información. La política de disponibilidad debe incluir, como mínimo, los siguientes aspectos:

9.23.1 NIVELES DE DISPONIBILIDAD:

La política de disponibilidad debe asegurar el cumplimiento de los niveles de disponibilidad de servicios e información acordada con clientes, proveedores y/o terceros, en función de las necesidades de la Entidad, los acuerdos de nivel de servicio ofrecidos y las evaluaciones de riesgos correspondientes. Para garantizar la continuidad del negocio y minimizar los tiempos de inactividad en caso de un incidente de seguridad de la información, se deberá establecer los procedimientos y protocolos necesarios para la recuperación de los sistemas, aplicaciones y datos críticos. Además, se debe garantizar que los recursos necesarios estén disponibles para la implementación y el mantenimiento del plan de continuidad del negocio.

9.23.2 PLANES DE RECUPERACIÓN:

La política de disponibilidad debe incluir la elaboración de planes de recuperación que contemplan las necesidades de disponibilidad del negocio, con el objetivo de

minimizar los impactos y tiempos de recuperación ante la ocurrencia de un evento de seguridad de la información o cualquier otra contingencia que pueda afectar la disponibilidad de los servicios y sistemas de la Secretaría de Hacienda Departamental del Amazonas. Estos planes de recuperación deben ser actualizados y probados periódicamente para asegurar su efectividad y eficacia en la restauración de los servicios y sistemas en caso de un incidente. Asimismo, deben ser comunicados a los funcionarios, contratistas y terceros que tengan acceso a la información y servicios de la entidad.

9.23.3 INTERRUPCIONES:

La política debe garantizar que la gestión de interrupciones de mantenimiento de los servicios sea realizada de manera planificada y coordinada, de forma que se minimice el impacto en la disponibilidad de los mismos. Se deben establecer los procedimientos y controles necesarios para la gestión de dichas interrupciones, así como la comunicación efectiva con los usuarios afectados para minimizar el impacto en su actividad. Además, se deben establecer medidas de contingencia que permitan mantener la disponibilidad del servicio en caso de interrupciones no planificadas.

9.23.4 ACUERDOS DE NIVEL DE SERVICIO:

La política de disponibilidad debe tener en cuenta los acuerdos de niveles de servicios (ANS) establecidos con los clientes, proveedores y/o terceros, a fin de garantizar la disponibilidad del servicio en caso de interrupciones. Es importante establecer procedimientos para notificar a los usuarios afectados, los tiempos estimados de recuperación y los pasos que se tomarán para garantizar la disponibilidad del servicio. Además, se debe contar con un plan de contingencia que permita la recuperación rápida y efectiva del servicio en caso de interrupciones planificadas o no planificadas, teniendo en cuenta los ANS establecido.

9.24 SEGREGACIÓN DE AMBIENTES:

La política debe establecer la segregación de ambientes para minimizar los riesgos asociados con la puesta en funcionamiento durante cambios y nuevos desarrollos, con el fin de reducir al mínimo el impacto de cualquier indisponibilidad del servicio las fases de desarrollo, pruebas y producción. La segregación de ambientes permitirá el desarrollo y pruebas de nuevas aplicaciones, sin afectar los sistemas en producción. Además, la política deberá establecer los procedimientos necesarios para garantizar que los cambios y desarrollos se implementen adecuadamente y se verifiquen antes de pasar a la fase de producción, con el fin de evitar posibles fallas en el servicio.

9.25 GESTIÓN DE CAMBIOS:

La política debe establecer un proceso formal de gestión de cambios que garantice la mínima afectación de la disponibilidad del servicio durante los cambios realizados en los sistemas, aplicaciones y plataformas de la Secretaría de Hacienda Departamental del Amazonas. Este proceso debe ser ejecutado bajo condiciones controladas y con la participación de todas las áreas implicadas, para garantizar la calidad y la continuidad del servicio. Además, debe establecerse un registro documentado de los cambios realizados para su posterior evaluación y mejora continua.

9.26 REGISTRO Y AUDITORÍA

Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

Esta política deberá contener:

9.26.1 RESPONSABILIDAD:

Incluir la responsabilidad de la Oficina de Control Interno y similares, acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.

9.26.2 ALMACENAMIENTO DE REGISTROS:

La política debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.

9.26.3 NORMATIVIDAD:

La política de auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Secretaria de Hacienda Departamental del Amazonas.

9.26.4 GARANTÍA CUMPLIMIENTO:

La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Secretaria de Hacienda Departamental del Amazonas; así como recomendar las deficiencias detectadas.

9.26.5 PERIODICIDAD:

La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Secretaria de Hacienda Departamental del Amazonas, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

9.26.6 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

La entidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información. La política debe contemplar para su elaboración los siguientes parámetros:

Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.

9.27 VISIÓN GENERAL:

¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?

En cuanto a qué se debe informar, es necesario informar cualquier incidente de seguridad de la información que afecte la confidencialidad, integridad y disponibilidad de los datos personales y la información en general. Esto incluye, pero no se limita a, accesos no autorizados, pérdida o robo de dispositivos que contengan información confidencial, virus informáticos, ataques informáticos, y cualquier otro incidente que pueda comprometer la seguridad de la información.

En cuanto quién debe reportarse, esto debe estar claramente establecido en la política de seguridad de la información de la organización. Por lo general, se debe informar al responsable de seguridad de la información la persona designada para recibir los informes de incidentes de seguridad. Además, también se puede requerir informar a otras entidades externas como autoridades competentes en materia de protección de datos personales y otros reguladores.

En cuanto a los medios que se pueden emplear para hacer el informe, esto también debe estar establecido en la política de seguridad de la información de la organización. En general, se pueden utilizar medios como correo electrónico, formularios en línea, líneas telefónicas de emergencia, entre otros. Es importante que la organización brinde múltiples opciones para hacer el reporte de incidentes de seguridad para asegurar que los usuarios puedan informar de manera oportuna y efectiva cualquier incidente que prevenga.

9.28 DEFINIR RESPONSABLES:

Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.

En términos generales, los responsables de gestionar los eventos serán aquellos funcionarios y/o contratistas designados por la Secretaría de Hacienda Departamental del Amazonas para tal fin. Estos serán los encargados de identificar, analizar y gestionar los eventos relacionados con la seguridad de la información, con el fin de minimizar su impacto y garantizar la continuidad de los procesos de la entidad. Es importante que la política establezca las responsabilidades y funciones de los encargados de la gestión de eventos y la forma en que se llevará a cabo dicha gestión.

9.29 ACTIVIDADES:

Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.

El proceso de gestión de incidentes es un conjunto de actividades diseñadas para detectar, registrar, clasificar, investigar y resolver cualquier interrupción o falla que se presente en los sistemas de información y servicios de la organización.

El proceso comienza con el informe del incidente, que puede ser realizado por cualquier persona que detecte un problema. Una vez recibido el informe, se inicia la fase de registro y clasificación del incidente, donde se identifica la naturaleza del problema, su impacto en la operación del negocio y su prioridad.

Luego, se inicia la fase de investigación y diagnóstico del incidente, donde se analizan las posibles causas del problema y se determina las acciones necesarias para resolverlo. En esta fase, puede ser necesario coordinar con otras áreas de la organización o incluso con proveedores externos para obtener soporte técnico especializado.

Una vez que se ha identificado la solución al incidente, se procede a implementarla y verificar su eficacia. En caso de que la solución no haya sido efectiva, se pueden explorar otras opciones o se puede escalar el incidente a un nivel superior de gestión.

Finalmente, se cierra el incidente con la documentación correspondiente y se realiza una evaluación para identificar oportunidades de mejora en el proceso de gestión de incidentes. Es importante destacar que todo el proceso debe ser documentado e informado a los interesados de acuerdo a los lineamientos de la política de seguridad de la información de la organización.

9.30 DOCUMENTACIÓN:

Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.

La documentación del esquema de gestión y los procedimientos de la Secretaría de Hacienda Departamental del Amazonas son esenciales para la gestión eficaz de la seguridad de la información y deben estar disponibles para consulta y revisión por parte del personal involucrado en la gestión de la seguridad de la información Esta documentación debe incluir una descripción detallada del esquema de gestión y de los procedimientos que se deben seguir para garantizar la seguridad de la información, así como los roles y responsabilidades de cada uno de los involucrados en el proceso.

La documentación del esquema de gestión debe describir los procesos y procedimientos específicos que se deben seguir en caso de incidentes de seguridad de la información, desde la detección y reporte hasta la resolución y seguimiento. Es importante que se definan claramente las etapas del proceso de gestión de incidentes, los roles y responsabilidades de los involucrados en cada etapa, los tiempos de respuesta esperados y los medios de comunicación que se deben emplear para informar sobre el incidente y su resolución.

La documentación también debe incluir los procedimientos de gestión de cambios y las políticas de control de acceso a la información, así como cualquier otra política o procedimiento relevante para la seguridad de la información. Esta documentación debe estar actualizada y revisada periódicamente para garantizar su eficacia y adecuación a los requisitos de seguridad de la información de la Secretaría de Hacienda Departamental del Amazonas.

9.31 DESCRIPCIÓN DEL EQUIPO QUE MANEJARÁ LOS INCIDENTES:

Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.

La estructura general para la gestión de incidentes y vulnerabilidades de seguridad en la Secretaría de Hacienda Departamental del Amazonas puede incluir los siguientes elementos:

Responsable de la gestión de incidentes y vulnerabilidades: Un funcionario designado como el responsable de la gestión de incidentes y vulnerabilidades, encargado de liderar el proceso de gestión y tomar decisiones en caso de incidentes o vulnerabilidades.

Equipo de gestión de incidentes y vulnerabilidades: Un equipo designado para apoyar al responsable de la gestión de incidentes y vulnerabilidades en la ejecución

del proceso de gestión, incluyendo la identificación, análisis, evaluación y respuesta a los incidentes y vulnerabilidades de seguridad.

Procedimientos de gestión de incidentes y vulnerabilidades: Documentos que describen los procedimientos que deben seguirse en caso de incidentes o vulnerabilidades, incluyendo la forma en que deben reportarse, registrar, analizar, evaluar y responder a los mismos.

Herramientas de gestión de incidentes y vulnerabilidades: Herramientas tecnológicas para ayudar en la gestión y seguimiento de los incidentes y vulnerabilidades, incluyendo software para la gestión de tickets, monitoreo de seguridad, detección de intrusiones, entre otros.

Comité de seguridad de la información: Un comité encargado de supervisar la implementación y cumplimiento del esquema de gestión de incidentes y vulnerabilidades, así como de establecer políticas y directrices para la gestión de la seguridad de la información en la Secretaría de Hacienda Departamental del Amazonas.

Es importante mencionar que la estructura general para la gestión de incidentes y vulnerabilidades puede variar de acuerdo con las necesidades y particularidades de cada organización, y que la Secretaría de Hacienda Departamental del Amazonas puede ajustar su estructura y procesos de gestión de acuerdo a sus necesidades y evolución de la tecnología y riesgos de seguridad.

9.32 ASPECTOS LEGALES:

Deben citarse los aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento.

Algunos aspectos legales que deben tenerse en cuenta en la gestión de incidentes y vulnerabilidades de seguridad en la Secretaría de Hacienda Departamental del Amazonas pueden incluir:

Ley 1581 de 2012: Regula el tratamiento de datos personales y establece las obligaciones que tienen las entidades que manejan información personal.

Decreto 1074 de 2015: Establece las normas para el uso de medios electrónicos en la administración pública y define los requisitos técnicos que deben cumplir los sistemas de información.

Ley 1273 de 2009: Establece los delitos informáticos y las penas correspondientes a cada uno de ellos.

Ley 1755 de 2015: Regula el uso y protección de la información en Colombia, así como la creación de políticas de seguridad de la información en las entidades públicas y privadas.

Decreto 514 de 2017: Establece los requisitos mínimos de seguridad de la información para las entidades públicas y privadas que manejan información de interés nacional.

Es importante que la Secretaría de Hacienda Departamental del Amazonas cumpla con todas las obligaciones legales relacionadas con la gestión de incidentes y vulnerabilidades de seguridad, ya que de lo contrario podría incurrir en sanciones y multas.

9.33 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La política de formación en seguridad de la información esencial es para minimizar las vulnerabilidades y amenazas que pueden surgir a través de la actuación del personal de la Secretaría de Hacienda Departamental del Amazonas.

Es responsabilidad de la alta dirección destinar los recursos necesarios para la implementación de programas de formación que aborden temas relevantes y actualizados en cuanto a la seguridad de la información, así como también promover una cultura de seguridad en toda la organización.

Se debe establecer claramente quiénes serán los destinatarios de estos programas de formación y sensibilización, incluyendo tanto a los empleados como a los contratistas y terceros que trabajan con la Secretaría. Además, se debe establecer la obligación de asistir a estos eventos de formación por parte de todos los usuarios.

La revisión periódica de los resultados de la capacitación es necesaria para mejorar continuamente los procesos de formación y garantizar que se estén cumpliendo los objetivos previstos.

También se deben definir los roles y responsabilidades de quienes diseñarán y comunicarán los programas de formación, incluyendo los requisitos mínimos de los instructores y los métodos de evaluación de los resultados de la formación.

Es importante que se documenten los planes de estudio y desarrollo de los programas de formación, y que se definan los compromisos y obligaciones que asumirán los empleados capacitados.

Además, se deben incluir políticas adicionales relacionadas directamente con el comportamiento de los usuarios, como la Política de Escritorio Limpio, la Política de Uso Aceptable y la Ética Empresarial. Esto garantizará una mayor conciencia y

responsabilidad de los usuarios en cuanto al manejo de la información y su comportamiento en el entorno laboral.

En resumen, la política de formación en seguridad de la información debe ser integral, establecer objetivos claros y definir las responsabilidades de cada parte involucrada en el proceso de formación, con el fin de garantizar la seguridad y protección de la información en la Secretaría de Hacienda Departamental del Amazonas.

10 CONCLUSIONES

Contribución a la Continuidad del Negocio: La implementación de un análisis y gestión de riesgos informáticos basado en las normas ISO 27001 e ISO 22301 desempeña un papel fundamental en la preservación de la continuidad del negocio en la Secretaría de Hacienda Departamental del Amazonas. Estas normas proporcionan un marco estructurado para identificar y mitigar riesgos, lo que permite a la organización estar mejor preparada para enfrentar eventos adversos como ciberataques, desastres naturales o pandemias.

Garantía de la Disponibilidad, Integridad y Confidencialidad de la Información: La adopción de estas normas asegura la protección integral de la información crítica de la Secretaría de Hacienda. La disponibilidad, integridad y confidencialidad de la información se convierten en pilares fundamentales para mantener la operatividad y la confianza de las partes interesadas. Las normas ISO 27001 e ISO 22301 ofrecen directrices específicas para salvaguardar estos aspectos clave de la información.

Enfoque en la Gestión Proactiva de Riesgos: La gestión de riesgos informáticos basada en estas normas no solo se limita a reaccionar ante amenazas, sino que se enfoca en una gestión proactiva. Esto implica la identificación anticipada de riesgos potenciales y la implementación de medidas preventivas y de contingencia para minimizar su impacto en las operaciones.

Cumplimiento Normativo: Estas normas son reconocidas internacionalmente y cumplen con los requisitos regulatorios relacionados con la seguridad de la información y la continuidad del negocio. La implementación adecuada de estos estándares garantiza que la Secretaría de Hacienda esté alineada con las mejores prácticas y normativas vigentes.

Mejora Continua: La gestión de riesgos informáticos basada en ISO 27001 e ISO 22301 promueve una cultura de mejora continua. La organización realiza evaluaciones periódicas, actualiza sus controles y políticas, y se adapta a las cambiantes amenazas y condiciones del entorno empresarial.

La correcta identificación y gestión de los activos de información es fundamental para garantizar la seguridad y protección de los datos que maneja la Secretaría de Hacienda. La implementación de los lineamientos de la norma ISO 27001 es una herramienta útil para llevar a cabo este proceso, ya que proporciona un marco de referencia para la gestión de la seguridad de la información. Es importante destacar que, además de los activos tangibles como equipos informáticos, servidores y dispositivos de almacenamiento, también se deben tener en cuenta los activos intangibles como los datos, sistemas y aplicaciones. Estos activos pueden ser iguales de valiosos y necesitan ser protegidos de manera adecuada. Por lo tanto,

es necesario que la Secretaría de Hacienda realice una evaluación periódica de los activos de información para identificar posibles riesgos y vulnerabilidades. De esta forma, se pueden implementar medidas de seguridad adecuadas para minimizar los riesgos y asegurar la protección de los datos. En conclusión, la correcta gestión de los activos de información es fundamental para garantizar la seguridad y protección de los datos de la Secretaría de Hacienda. Siguiendo los lineamientos de la norma ISO 27001 y evaluando periódicamente los activos de información, se pueden implementar medidas de seguridad adecuadas para minimizar los riesgos y proteger los datos.

Después de realizar la matriz de evaluación de riesgos correspondiente para este proyecto aplicado, se ha identificado un alto riesgo debido a la falta de un plan de contingencia para la salvaguardia de la información. Por lo tanto, resulta de vital importancia la aplicación de la norma ISO 27001, ya que no solo contribuirá a la seguridad de la información, sino que también propuso una metodología sólida para garantizar la integridad y confidencialidad de los datos. Al implementar esta norma, se pueden reducir significativamente los riesgos identificados y establecer medidas preventivas y correctivas para proteger los activos de información de la Secretaría de Hacienda.

El Plan de tratamiento de Riesgos implementado ha sido clave para mitigar los riesgos identificados en la Secretaría de Hacienda Departamental del Amazonas, logrando reducir significativamente los índices de pérdida de confidencialidad, integridad y disponibilidad de los activos de información. De esta manera, se ha prevenido la ocurrencia de desastres en la seguridad de la información y se ha logrado garantizar un adecuado nivel de protección de los datos de la entidad.

Tras la aplicación del Plan de Tratamiento de Riesgos en los activos de información de la Secretaría de Hacienda Departamental del Amazonas, se definirán las acciones necesarias para evaluar y reducir los riesgos existentes mediante la implementación de medidas de seguridad adecuadas. Las políticas de seguridad establecidas en este proyecto aplicado, enfocadas en los activos de información vulnerables con un alto índice de riesgo, se aplicarán con éxito, siguiendo los estándares presentados por el MINTIC para las entidades públicas y empleando la metodología de la norma ISO 27001. Esto ha permitido garantizar la integridad, disponibilidad y confidencialidad de los activos de información de la Secretaría de Hacienda, reduce significativamente los riesgos asociados a la seguridad de la información.

Tras la implementación de las medidas de seguridad basadas en la norma ISO 27001 y los estándares proporcionados por el MINTIC en la Secretaría de Hacienda Departamental del Amazonas, se puede afirmar que se modificó una mejora significativa en la protección de la privacidad, integridad y disponibilidad la información La norma ISO 27001 se ha demostrado como una guía completa y eficaz para garantizar la seguridad de la información, y su aplicación en la entidad

ha permitido un enfoque prioritario en la protección de la información sensible. Asimismo, se destaca la importancia de seguir manteniendo las medidas de seguridad implementadas y llevar a cabo revisiones periódicas para asegurar su adecuado funcionamiento y su capacidad para adaptarse a nuevas amenazas o vulnerabilidades.

En resumen, el análisis y gestión de riesgos informáticos basados en las normas ISO 27001 e ISO 22301 son esenciales para mantener la continuidad del negocio y garantizar la protección integral de la información en la Secretaría de Hacienda Departamental del Amazonas. Estas normas proporcionan un marco sólido y efectivo para abordar los desafíos actuales y futuros relacionados con la seguridad de la información y la resiliencia operativa.

11 RECOMENDACIONES

Una gestión adecuada de los activos de información es fundamental para garantizar la seguridad y confidencialidad de los datos que maneja la Secretaría de Hacienda Departamental del Amazonas. Por ello, se recomienda implementar un inventario detallado de todos los activos de información de la entidad, incluyendo tanto los tangibles como los intangibles.

Este inventario debe incluir información detallada sobre cada activo, como su ubicación, su importancia para la entidad, su estado actual, el nivel de protección que requiere, entre otros. Esta información permitirá a la Secretaría de Hacienda Departamental del Amazonas tener un mayor control sobre sus activos de información y tomar medidas para protegerlos de manera adecuada.

Además, se recomienda establecer un sistema de seguimiento y monitoreo continuo de los activos de información, de manera que se pueda detectar cualquier actividad sospechosa o inusual. Esto puede lograrse mediante la implementación de herramientas de monitoreo y análisis de seguridad, y la definición de políticas y procedimientos claros para la gestión de incidentes de seguridad.

Es importante que se lleve un control riguroso de los activos de información, ya que esto permitirá tener una mayor visibilidad y control sobre ellos, y en caso de alguna eventualidad, será más fácil y rápido actuar para minimizar el impacto. La Norma ISO 27001 es una buena referencia para establecer las mejores prácticas en este ámbito.

La realización de copias de seguridad es fundamental para garantizar la disponibilidad y la integridad de la información, ya que permite recuperarla en caso de algún fallo o problema en los sistemas. Es necesario establecer una política de copias de seguridad y realizarlas periódicamente para tener siempre una copia actualizada de la información.

La matriz de riesgos es una herramienta muy útil para identificar los activos más críticos y vulnerables, y establecer las medidas necesarias para reducir los riesgos asociados a ellos. Es recomendable revisar periódicamente los resultados de la matriz de riesgos y actualizar las medidas de seguridad en consecuencia.

Además, es importante seguir las políticas y medidas de seguridad planteadas en el proyecto aplicado, ya que estas son una guía para establecer las mejores prácticas de seguridad de la información y reducir los riesgos identificados en la matriz de riesgos. Es necesario que todos los miembros de la organización estén alineados y comprometidos en la implementación de estas políticas y medidas para garantizar una mayor seguridad y confidencialidad de la información.

Por último, se recomienda realizar auditorías periódicas de seguridad de la información con el fin de evaluar la efectividad de las medidas de seguridad implementadas y detectar posibles debilidades o vulnerabilidades que deban ser corregidas. Estas auditorías pueden ser realizadas a cabo por personal interno o externo, y deben ser realizadas de manera independiente y objetiva para garantizar su eficacia.

12 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de PLAN DE GESTIÓN DE CONTINUIDAD DE NEGOCIO BASADO EN EL ESTÁNDAR ISO 22301 E ISO 27001 PARA MITIGAR LOS RIESGOS DE LOS ACTIVOS DE INFORMACIÓN EN LA SECRETARÍA DE HACIENDA DEPARTAMENTAL DEL AMAZONAS, puedan acceder al documento.

BIBLIOGRAFÍA

Business Continuity Management GOOD PRACTICE GUILDELINES 2008. Determining BCM Strategy, Bussiness Continuity Institute (BCI).

Business Continuity Management GOOD PRACTICE GUILDELINES 2008. Developing and Implementing a BCM Response, Bussiness Continuity Institute (BCI).

Business Continuity Management GOOD PRACTICE GUILDELINES 2008. Exercising, Maintaining y Reviewing BCM Arrangemens, Bussiness Continuity Institute (BCI).

Business Continuity Management GOOD PRACTICE GUILDELINES 2008. Policy y Programme Management, Bussiness Continuity Institute (BCI).

Business Continuity Management GOOD PRACTICE GUILDELINES 2008. Understanding the Organization, Bussiness Continuity Institute (BCI).

Bussiness and IT Continuity: Overview and Implementtion Principles. European Network and Information Security Agency, ENISA, (Febrero de 2008).

CASTRO, Duván. ROJAS, Angela. Riesgos, Amenazas y vulnerabilidades de los sistemas informáticos geográfica, Bogotá. 2013. Trabajo de Investigación. Universidad Católica de Colombia, Facultad de Ingeniería, Programa de Ingeniería de Sistemas.

CONTRALORIA GENERAL DE ANTIOQUIA. Manual de continuidad tecnológica para la Contraloría General de Antioquia. (Versión 01, Agosto de 2017).
De la teoría a la práctica: Cobit aplicado para asegurar la continuidad de las operaciones. 2017. Jose Angel Peña.

DISASTER RECOVERY DRJOURNAL En Español. El Plan de Continuidad del Negocio. citado el 15 de octubre del 2021. (10 de septiembre de 2020). [Consulta: marzo de 2022] Disponible en: https://drjenespanol.com/recursos/el-plan-de-continuidad-del-negocio/.

GlobalSUITEsolutions. ¿Cómo elaborar un plan de continuidad?. citado el 15 de octubre del 2021. (10 de septiembre de 2020). [consulta: abril de 2022]. https://www.globalsuitesolutions.com/es/como-elaborar-un-plan-de-continuidad/.

GOBIERNO DE COLOMBIA. Escuela superior de Administración Pública. Plan de continuidad del negocio BCP. citado el 15 de octubre del 2021. 2018. [consulta: marzo de 2022] Disponible en: https://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-continuidad-del-negocio-v1.pdf.

GOBIERNO DE COLOMBIA. Función Pública, Documento Técnico del Plan de Continuidad del Negocio. (2 de octubre 2020). [consultado: abril de 2022] Disponible en: https://www.funcionpublica.gov.co/documents/34645357/34702994/Plan_continuidad_de_funcion_publica.xlsx/937700b4-0ee6-d6e5-213d-5fcf190e9d3b?t=1594256700028.

GOBIERNO DE COLOMBIA. Función Pública, Plan de Continuidad del Negocio. 2021 [consultado: marzo de 2022] Disponible en: https://www.funcionpublica.gov.co/plan-de-continuidad.

Hiles, A. Bussiness Continuity Best Practices. Connecticut: Rothstein Associates, Inc. (2004).

IBAÑEZ, Roller. Gestión de continuidad del negocio un enfoque resilente basado en estándar ISO 22301. Editorial OWASP The Open Application Security Proyect. 2020.

ISO 22301: 2012, Sistemas de Gestión y Continuidad del Negocio.

ISO 22301: 2012. Seguridad de la sociedad: Sistemas de Continuidad Tecnológica – Requisitos.

ISO 27001: 2005. Alexander, A. Diseño de un Sistema de Gestión de Seguridad de Información. 2007. óptica Alfaomega.

ISO 27002 como parte de un marco de Gobierno y Control de TI, Roberto C, Arbelaez, XXVI SALON INFORMATICA. Integrando ITIL, COBIT.

ISO 27005 Tecnología de la Información. Técnicas de seguridad Gestión de Riesgos de seguridad de la información. Norma Técnica colombiana. 2011.
ISO 27031 – DE198-13, Tecnología de la Información, Técnica de Seguridad, Directrices para la continuidad del negocio.

ISO/IEC 22301:2012. Organización Internacional de la Normalización y la Comisión Electrotécnica Internacional. Seguridad de la Sociedad: Sistemas de Continuidad Tecnológica – Requisitos.

ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.

ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements.

ISO/IEC 27001: 2005. Tecnología de la información, Técnicas de seguridad, sistemas de gestión de seguridad de la información -Requerimientos.

ISO/IEC 27001:2006, Norma Técnica NTC-ISO/IEC Colombiana, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

ISO/IEC 27002, Information Technology. Security Techniques. Code of practice for information security management.

ISO/IEC 27005, Information Technology. Security Techniques. Information security risk Management.

ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident imanagement.

Ministerio de las Tecnologías de la Información y las Comunicaciones, Guía para la preparación de las TIC para la Continuidad Tecnológica. Guía N°10 versión 1.0.0. 2015.

MINTIC, Seguridad y privacidad de la información – guía para la preparación de las tic para la continuidad del negocio. 2018.

NAE, Claves para un plan de continuidad de negocio (BCP). citado el 15 de octubre del 2021, (10 de junio de 2020). [Consulta: marzo de 2022] Disponible en: https://nae.global/es/claves-para-un-plan-de-continuidad-de-negocio-bcp/.

Piranirisk. Guía para gestionar un plan de continuidad de negocio. según la ISO 22301. citado el 15 de octubre del 2021. (19 de abril del 2021). [Consulta: marzo 2022] Disponible en: https://www.piranirisk.com/es/academia/especiales/guia-para-gestionar-un-plan-de-continuidad-de-negocio-segun-la-iso-22301.

Presidencia de la Republica. Decreto 1078 del 26 de mayo de 2015. Por medo del cual se expide el Decreto Único reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Risk Management Guide for IT Systems, National Institute of Standards and Technology, (Julio de 2018).

RODRIGO FERRER V. Metodología para la Gestión de la Continuidad del Negocio. Editorial CINTEL PROYECTOS TIC INNOVADORES. 2015.
SUPERSALUD, guía de cumplimento de continuidad de negocio, proceso Código GGGUO4, Bogotá 2018.

The New Business Continuity Model. Version 1.0, Dan Wilder. (Octubre 6 de 2008).

Unidad Nacional para la Gestion del Riesgo de Desastres. Plan de Continuidad de Negocio ante el COVID 19, un componente para la resiliencia empresarial, (Bogotá 27 de mayo del 2020). [Consulta: marzo de 2022]. Disponible en: http://portal.gestiondelriesgo.gov.co/Paginas/Noticias/2020/Continuidad-del-negocio-ante-el-COVID19-un-componente-para-la-resiliencia-empresarial.aspx.

Welivesecurity. 4 pasos para armar un plan de continuidad del negocio que asegure el futuro digital de la empresa. citado el 15 de octubre del 2021. (14 de mayo del 2014). [Consulta: abril de 2022] disponible en: https://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/.

ANEXOS

ANEXO 1. PERSONAL Y DEPENDENCIAS

Personal y Dependencias			
NOMBRES	**DEPENDENCIA**	**CARGO**	**TIPO DE VINCULACIÓN**
Antonio José Monsalve Prada	**DESPACHO DE HACIENDA**	**Secretario de Hacienda**	Libre Nombramiento y Remoción
Cristian Muñoz	**DESPACHO DE HACIENDA**	**P.U Contratista Contador Publico**	Prestación de Servicios
Víctor Polo	**DESPACHO DE HACIENDA**	**Tecnólogo de Apoyo en Contabilidad**	Prestación de Servicios
Gloria Acosta	**DESPACHO DE HACIENDA**	**Técnico de Apoyo en Administración**	Prestación de Servicios
Fabian Correa	**DESPACHO DE HACIENDA**	**Técnico de Apoyo en Sistemas**	Prestación de Servicios
Ana María Carvajal	**DESPACHO DE HACIENDA**	**P.U Especializado en Derecho**	Prestación de Servicios
Fabiola Morales	**DESPACHO DE HACIENDA**	**Técnico de Apoyo en Contabilidad**	Prestación de Servicios
Sergio Torres	**DESPACHO DE HACIENDA**	**P.U de Apoyo en Electrónica**	Prestación de Servicios
Paula Rocha Fonseca	**OFICINA DE RENTAS**	**P.U Grado 05 Jefe de Rentas**	Nombramiento de Carrera Administrativa
Marleny Rengifo	**OFICINA DE RENTAS**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Ricardo Cubillos	**OFICINA DE RENTAS**	**P.U Grado 03**	Nombramiento Provisional
Viviana Holanda	**OFICINA DE RENTAS**	**Auxiliar de Apoyo en contabilidad**	Prestación de Servicios
Yadira Rivas	**OFICINA DE RENTAS**	**Técnico de Apoyo en Archivo**	Prestación de Servicios
Ana Miraña	**OFICINA DE RENTAS**	**Tecnico de Apoyo en Contabilidad**	Prestación de Servicios
Gladys Santana	**OFICINA DE CONTABILIDAD**	**P.U Grado 07 Jefe de Contabilidad**	Nombramiento Provisional

Anyi Pinto	**OFICINA DE CONTABILIDAD**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Rosario Gil	**OFICINA DE CONTABILIDAD**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
José María Córdoba	**OFICINA DE CONTABILIDAD**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Xiomara Oyola	**OFICINA DE CONTABILIDAD**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Yurisan Tabares	**OFICINA DE CONTABILIDAD**	**Profesional de Apoyo en Contabilidad**	Prestación de Servicios
Milton Fuentes	**OFICINA DE CONTABILIDAD**	**Profesional especializado en Contabilidad**	Prestación de Servicios
Diego Bardales	**OFICINA DE CONTABILIDAD**	**Tecnico de Apoyo en Contabilidad**	Prestación de Servicios
Carlos Vega	**OFICINA DE CONTABILIDAD**	**Tecnico de Apoyo en Contabilidad**	Prestación de Servicios
Leonardo Rocha	**OFICINA DE CONTABILIDAD**	**Profesional de Apoyo en Administración**	Prestación de Servicios
Anderson Bravo	**OFICINA DE CONTABILIDAD**	**Profesional de Apoyo en Administración**	Prestación de Servicios
KHATERINE CHICO	**OFICINA DE TESORERIA**	**P.U Grado 07 Tesorera General**	Nombramiento Provisional
Beverly Gil	**OFICINA DE TESORERIA**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Nubia Lozano	**OFICINA DE TESORERIA**	**Técnico Administrativo Grado 06**	Nombramiento Provisional
Diomara Arteaga	**OFICINA DE TESORERIA**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Angie Rivas	**OFICINA DE TESORERIA**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Erick Rojas	**OFICINA DE TESORERIA**	**Tecnólogo de Apoyo en Contabilidad**	Prestación de Servicios

Brandon Hipuchima	**OFICINA DE TESORERIA**	**Técnico de Apoyo en Administración**	Prestación de Servicios
Neidy del Águila	**OFICINA DE TESORERIA**	**P.U de Apoyo en Administración**	Prestación de Servicios
Darwin Perea	**OFICINA DE TESORERIA**	**Técnico de Apoyo en Contabilidad**	Prestación de Servicios
Cristian Rubio	**OFICINA DE TESORERIA**	**P.U de Apoyo en Estadística**	Prestación de Servicios
Natali peña	**OFICINA DE TESORERIA**	**P.U de Apoyo en Administración**	Prestación de Servicios
Leticia Sangama	**OFICINA DE TESORERIA**	**P.U de Apoyo en Administración**	Prestación de Servicios
Carolina Piris	**OFICINA DE TESORERIA**	**P.U de apoyo en Contabilidad**	Prestación de Servicios
Karen Luna	**OFICINA DE PRESUPUESTO**	**P.U Grado 07 Jefe de Presupuesto**	Nombramiento Provisional
Rosa Pinto	**OFICINA DE PRESUPUESTO**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Martha Muñoz	**OFICINA DE PRESUPUESTO**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Juliana Botáis	**OFICINA DE PRESUPUESTO**	**Auxiliar Administrativo Grado 04**	Nombramiento Provisional
Gisela León	**OFICINA DE PRESUPUESTO**	**P.U de apoyo en Contabilidad**	Prestación de Servicios
Viviana Holanda	**OFICINA DE PRESUPUESTO**	**Tecnólogo de Apoyo en Contabilidad**	Prestación de Servicios
Grecia Samudio	**OFICINA DE PRESUPUESTO**	**P.U de apoyo en Contabilidad**	Prestación de Servicios
Juan Carlos Guvas	**OFICINA DE PRESUPUESTO**	**P.U de apoyo en Contabilidad**	Prestación de Servicios
Victoria Gutiérrez	**OFICINA DE PRESUPUESTO**	**Técnico de Apoyo en Administración**	Prestación de Servicios
Hilary Vargas	**OFICINA DE PRESUPUESTO**	**Auxiliar de Apoyo**	Prestación de Servicios
Adriana Docarmo	**OFICINA DE PRESUPUESTO**	**Técnico de Apoyo en Archivo**	Prestación de Servicios

ANEXO 2. INVENTARIO DE ACTIVOS

INFORMACIÓN DE LOS ACTIVOS			
No.	DATOS DEL ACTIVO DE INFORMACION		
	NOMBRE DEL ACTIVO	**PROCESO PROPIETARIO DEL ACTIVO**	**TIPO DE ACTIVO**
1	Computador Portátil I5, Gen 8, 1TB HDD, 14 pulgadas.	Antonio José Monsalve Prada	HARDWARE
2	Escáner Epson DS-420	Antonio José Monsalve Prada	HARDWARE
3	Impresora Epson L3250	Antonio José Monsalve Prada	HARDWARE
4	Windows 10 Profesional	Antonio José Monsalve Prada	SOFTWARE
5	Office 2016 Profesional	Antonio José Monsalve Prada	SOFTWARE
6	PCTG ENTERPRISE	Antonio José Monsalve Prada	SOFTWARE
7	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Cristian Muñoz	HARDWARE
8	Windows 10 Profesional	Cristian Muñoz	SOFTWARE
9	Office 2016 Profesional	Cristian Muñoz	SOFTWARE
10	PCTG ENTERPRISE	Cristian Muñoz	SOFTWARE
11	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Víctor Polo	HARDWARE
12	Windows 10 Profesional	Víctor Polo	SOFTWARE
13	Office 2016 Profesional	Víctor Polo	SOFTWARE
14	PCTG ENTERPRISE	Víctor Polo	SOFTWARE
15	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Gloria Acosta	HARDWARE
16	Windows 10 Profesional	Gloria Acosta	SOFTWARE
17	Office 2016 Profesional	Gloria Acosta	SOFTWARE
18	PCTG ENTERPRISE	Gloria Acosta	SOFTWARE
19	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Fabian Correa	HARDWARE
20	Windows 10 Profesional	Fabian Correa	SOFTWARE
21	Office 2016 Profesional	Fabian Correa	SOFTWARE
22	PCTG ENTERPRISE	Fabian Correa	SOFTWARE
23	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Ana María Carvajal	HARDWARE
24	Windows 10 Profesional	Ana María Carvajal	SOFTWARE
25	Office 2016 Profesional	Ana María Carvajal	SOFTWARE
26	PCTG ENTERPRISE	Ana María Carvajal	SOFTWARE

27	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Fabiola Morales	HARDWARE
28	Windows 10 Profesional	Fabiola Morales	SOFTWARE
29	Office 2016 Profesional	Fabiola Morales	SOFTWARE
30	PCTG ENTERPRISE	Fabiola Morales	SOFTWARE
31	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Sergio Torres	HARDWARE
32	Windows 10 Profesional	Sergio Torres	SOFTWARE
33	Office 2016 Profesional	Sergio Torres	SOFTWARE
34	PCTG ENTERPRISE	Sergio Torres	SOFTWARE
35	Servidor PCTG	Sergio Torres	HARDWARE
36	Router	Sergio Torres	HARDWARE
37	Plataformas	Sergio Torres	DATOS
38	internet	Sergio Torres	SERVICIOS
39	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Paula Rocha Fonseca	HARDWARE
40	Windows 10 Profesional	Paula Rocha Fonseca	SOFTWARE
41	Office 2016 Profesional	Paula Rocha Fonseca	SOFTWARE
42	PCTG ENTERPRISE	Paula Rocha Fonseca	SOFTWARE
43	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Marleny Rengifo	HARDWARE
44	Windows 10 Profesional	Marleny Rengifo	SOFTWARE
45	Office 2016 Profesional	Marleny Rengifo	SOFTWARE
46	PCTG ENTERPRISE	Marleny Rengifo	SOFTWARE
47	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Ricardo Cubillos	HARDWARE
48	Windows 10 Profesional	Ricardo Cubillos	SOFTWARE
49	Office 2016 Profesional	Ricardo Cubillos	SOFTWARE
50	PCTG ENTERPRISE	Ricardo Cubillos	SOFTWARE
51	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	vivina Holanda	HARDWARE
52	Windows 10 Profesional	vivina Holanda	SOFTWARE
53	Office 2016 Profesional	vivina Holanda	SOFTWARE
54	PCTG ENTERPRISE	vivina Holanda	SOFTWARE
55	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Yadira Rivas	HARDWARE
56	Windows 10 Profesional	Yadira Rivas	SOFTWARE
57	Office 2016 Profesional	Yadira Rivas	SOFTWARE
58	PCTG ENTERPRISE	Yadira Rivas	SOFTWARE
59	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Ana Miraña	HARDWARE
60	Windows 10 Profesional	Ana Miraña	SOFTWARE
61	Office 2016 Profesional	Ana Miraña	SOFTWARE

62	PCTG ENTERPRISE	Ana Miraña	SOFTWARE
63	Todo en Uno I7, Gen 10, 1TB SDD, 14 pulgadas.	Gladys Santana	HARDWARE
64	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Anyi Pinto	HARDWARE
65	Computador Portátil I5, Gen 10, 1TB HDD, 14 pulgadas.	Rosario Gil	HARDWARE
66	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	José María Córdoba	HARDWARE
67	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Xiomara Oyola	HARDWARE
68	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Yurisan Tabares	HARDWARE
69	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Milton Fuentes	HARDWARE
70	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Diego Bardales	HARDWARE
71	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Carlos Vega	HARDWARE
72	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Leonardo Rocha	HARDWARE
73	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Anderson Bravo	HARDWARE
74	Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	KHATERINE CHICO	HARDWARE
75	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Beverly Gil	HARDWARE
76	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Nubia Lozano	HARDWARE
77	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Diomara Arteaga	HARDWARE
78	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Angie Rivas	HARDWARE
79	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Erick Rojas	HARDWARE
80	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Brandon Hipuchima	HARDWARE
81	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Neidy del Águila	HARDWARE
82	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Darwin Perea	HARDWARE
83	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Cristian Rubio	HARDWARE

84	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Nataly peña	HARDWARE
85	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Leticia Sangama	HARDWARE
86	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Carolina Piris	HARDWARE
87	Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	Karen Luna	HARDWARE
88	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Rosa Pinto	HARDWARE
89	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Martha Muñoz	HARDWARE
90	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Juliana Botáis	HARDWARE
91	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Gisela León	HARDWARE
92	Computador Portátil I5 Gen 8, 500 GB, 14 Pulgadas	Viviana Holanda	HARDWARE
93	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Grecia Samudio	HARDWARE
94	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Juan Carlos Guvas	HARDWARE
95	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Victoria Gutiérrez	HARDWARE
96	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Hilary Vargas	HARDWARE
97	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Adriana Docarmo	HARDWARE

ANEXO 3. MATRIZ DE INVENTARIO, CLASIFICACION Y RIESGOS DE ACTIVOS DE INFORMACION

MATRIZ DE INVENTARIO, CLASIFICACIÓN Y RIESGO DE ACTIVOS DE INFORMACIÓN

Gobernación del Amazonas

RESUMEN EJECUTIVO

Clasificación general y Número de activos

Tipo de activo	Cantidad
Tipo Dato	1
Tipo Claves Criptograficas	0
Tipo Servicio	1
Tipo Software	42
Tipo Hardware	53
Tipo Comunicaciones	0
Tipo Soporte de Información	0
Tipo Equipamento Auxiliar	0
Tipo Instalaciones	0
Tipo Personal	1
Total de Activos	**98**

Clasificación según impacto a la seguridad

Leve	2
Importante	74
Grave	21

Resumen de nivel de riesgo en los activos

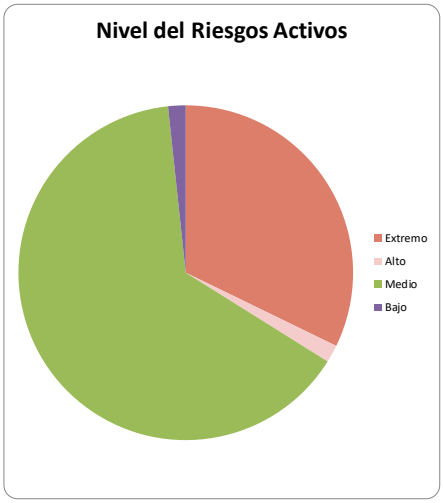
Extremo	19
Alto	1
Medio	38
Bajo	1

Clasificación de activos según su valor

Número de activos de clientes o terceros que deben protegerse	35
Activos de información que deben ser restringidos a un número limitado de empleados	97
Número de activos de información que deben ser restringidos a personas externas	83
Activos de información que pueden ser alterados o comprometidos para fraudes o corrupción	7
Número de activos de información que son muy críticos para las operaciones internas	81
Número de activos de información que son muy críticos para el servicio hacia terceros	81

Ubicación

Fisica	53
Electrónica	45



ANEXO 4. VALORACIÓN DE ACTIVOS

Valoración de los activos

Nombre	Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor
Computador Portátil I5, Gen 8, 1TB HDD, 14 pulgadas.	EXTREMO	9	6	9	8
Escáner Epson DS-420	BAJO	3	3	3	3
Impresora Epson L3250	MEDIO	3	6	6	5
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7

Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Servidor PCTG	EXTREMO	9	9	9	9
Router	ALTO	6	6	6	6
Plataformas	ALTO	6	6	6	6
internet	ALTO	6	6	6	6
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6

PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	9	5	6	7
Windows 10 Profesional	MEDIO	6	6	3	5
Office 2016 Profesional	ALTO	5	6	6	6
PCTG ENTERPRISE	EXTREMO	9	9	9	9
Todo en Uno I7, Gen 10, 1TB SDD, 14 pulgadas.	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Computador Portátil I5, Gen 10, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	5	5	6	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	6	6	5	6
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5

Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	6	5	6	6
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	6	5	6	6
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	6	5	6	6
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	6	6	5	6
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	5	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	6	5	6	6
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	ALTO	6	5	6	6
Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	EXTREMO	9	9	9	9
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Computador Portátil I5 Gen 8, 500 GB, 14 Pulgadas	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5
Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	MEDIO	6	5	5	5

ANEXO 5. ACTIVOS Y VALORACION CUALITATIVA

Activos y Valoración Cualitativa																				
MATRIZ DE LEVANTAMIENTO DE INFORMACION DE ACTIVOS SEGÚN METODOLOGIA MAGERIT Y NORMA ISO 27001:2013																				
Empresa:	**Gobernación del Amazonas**																			
INFORMACIÓN DE LOS ACTIVOS																				
No.	**DATOS DEL ACTIVO DE INFORMACION**			**DIMENSION**					**ATRIBUTOS**										**UBICACIÓN**	
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
1	Computador Portátil I5, Gen 8, 1TB HDD, 14 pulgadas.	Antonio José Monsalve Prada	HARDWARE	MA	A	MA	A	MA	SI	SI	SI	SI	SI	SI			X	X	X
2	Escáner Epson DS-420	Antonio José Monsalve Prada	HARDWARE	B	B	B	B	B	NO	SI	SI	NO	NO	NO	X			X	

3	Impresora Epson L3250	Antonio José Monsalve Prada	HARD WARE	B	B	B	A	A	NO	SI	SI	NO	NO	NO	X			X	
4	Windows 10 Profesional	Antonio José Monsalve Prada	SOFT WARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
5	Office 2016 Profesional	Antonio José Monsalve Prada	SOFT WARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
6	PCTG ENTERPRISE	Antonio José Monsalve Prada	SOFT WARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
7	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Cristian Muñoz	HARD WARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
8	Windows 10 Profesional	Cristian Muñoz	SOFT WARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
9	Office 2016 Profesional	Cristian Muñoz	SOFT WARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
10	PCTG ENTERPRISE	Cristian Muñoz	SOFT WARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
11	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Víctor Polo	HARD WARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
12	Windows 10 Profesional	Víctor Polo	SOFT WARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
13	Office 2016 Profesional	Víctor Polo	SOFT WARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
14	PCTG ENTERPRISE	Víctor Polo	SOFT WARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
15	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Gloria Acosta	HARD WARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	

16	Windows 10 Profesional	Gloria Acosta	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
17	Office 2016 Profesional	Gloria Acosta	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
18	PCTG ENTERPRISE	Gloria Acosta	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
19	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Fabian Correa	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
20	Windows 10 Profesional	Fabian Correa	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
21	Office 2016 Profesional	Fabian Correa	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
22	PCTG ENTERPRISE	Fabian Correa	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
23	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Ana María Carvajal	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
24	Windows 10 Profesional	Ana María Carvajal	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
25	Office 2016 Profesional	Ana María Carvajal	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
26	PCTG ENTERPRISE	Ana María Carvajal	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
27	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Fabiola Morales	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
28	Windows 10 Profesional	Fabiola Morales	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
29	Office 2016 Profesional	Fabiola Morales	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X

30	PCTG ENTERPRISE	Fabiola Morales	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
31	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Sergio Torres	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
32	Windows 10 Profesional	Sergio Torres	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
33	Office 2016 Profesional	Sergio Torres	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
34	PCTG ENTERPRISE	Sergio Torres	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
35	Servidor PCTG	Sergio Torres	HARDWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X	X	
36	Router	Sergio Torres	HARDWARE	A	A	A	A	A	SI	SI	SI	SI	SI	SI		X		X	
37	Plataformas	Sergio Torres	DATOS	A	MA	A	A	A	SI	SI	SI	SI	SI	SI			X		X
38	internet	Sergio Torres	SERVICIOS	MA	A	A	A	A	SI	SI	SI	SI	SI	SI			X		X
39	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Paula Rocha Fonseca	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
40	Windows 10 Profesional	Paula Rocha Fonseca	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
41	Office 2016 Profesional	Paula Rocha Fonseca	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
42	PCTG ENTERPRISE	Paula Rocha Fonseca	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
43	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Marleny Rengifo	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	

44	Windows 10 Profesional	Marleny Rengifo	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
45	Office 2016 Profesional	Marleny Rengifo	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
46	PCTG ENTERPRISE	Marleny Rengifo	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
47	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Ricardo Cubillos	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
48	Windows 10 Profesional	Ricardo Cubillos	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
49	Office 2016 Profesional	Ricardo Cubillos	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
50	PCTG ENTERPRISE	Ricardo Cubillos	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
51	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	vivina Holanda	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
52	Windows 10 Profesional	vivina Holanda	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
53	Office 2016 Profesional	vivina Holanda	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
54	PCTG ENTERPRISE	vivina Holanda	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
55	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Yadira Rivas	HARDWARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
56	Windows 10 Profesional	Yadira Rivas	SOFTWARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
57	Office 2016 Profesional	Yadira Rivas	SOFTWARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
58	PCTG ENTERPRISE	Yadira Rivas	SOFTWARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X

59	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Ana Miraña	HARD WARE	A	A	MA	M	A	SI	SI	SI	SI	SI	SI		X		X	
60	Windows 10 Profesional	Ana Miraña	SOFT WARE	A	M	A	A	B	NO	SI	SI	SI	NO	NO		X			X
61	Office 2016 Profesional	Ana Miraña	SOFT WARE	A	M	M	A	A	NO	SI	NO	SI	SI	SI		X			X
62	PCTG ENTERPRISE	Ana Miraña	SOFT WARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
63	Todo en Uno I7, Gen 10, 1TB SDD, 14 pulgadas.	Gladys Santana	HARD WARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X	X	
64	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Anyi Pinto	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
65	Computador Portátil I5, Gen 10, 1TB HDD, 14 pulgadas.	Rosario Gil	HARD WARE	A	M	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
66	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	José María Córdoba	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
67	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Xiomara Oyola	HARD WARE	MA	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
68	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Yurisan Tabares	HARD WARE	A	A	M	M	A	NO	SI	SI	SI	SI	SI		X		X	
69	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Milton Fuentes	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
70	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Diego Bardales	HARD WARE	A	A	A	A	M	NO	SI	SI	SI	SI	SI		X		X	
71	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Carlos Vega	HARD WARE	A	M	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
72	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Leonardo Rocha	HARD WARE	A	A	A	M	A	NO	SI	SI	SI	SI	SI		X		X	

73	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Anderson Bravo	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
74	Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	KHATERINE CHICO	HARD WARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X	X	
75	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Beverly Gil	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
76	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Nubia Lozano	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
77	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Diomara Arteaga	HARD WARE	MA	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
78	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Angie Rivas	HARD WARE	A	A	A	M	A	NO	SI	SI	SI	SI	SI		X		X	
79	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Erick Rojas	HARD WARE	A	M	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
80	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Brandon Hipuchima	HARD WARE	A	A	A	M	A	NO	SI	SI	SI	SI	SI		X		X	
81	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Neidy del Águila	HARD WARE	M	M	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
82	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Darwin Perea	HARD WARE	A	A	A	A	M	NO	SI	SI	SI	SI	SI		X		X	
83	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Cristian Rubio	HARD WARE	A	A	M	M	M	NO	SI	SI	SI	SI	SI		X		X	
84	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Natali peña	HARD WARE	M	M	A	M	A	NO	SI	SI	SI	SI	SI		X		X	
85	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Leticia Sangama	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
86	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Carolina Piris	HARD WARE	A	A	A	M	A	NO	SI	SI	SI	SI	SI		X		X	

87	Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	Karen Luna	HARD WARE	MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI			X	X	
88	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Rosa Pinto	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
89	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Martha Muñoz	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
90	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Juliana Botáis	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
91	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Gisela León	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
92	Computador Portátil I5 Gen 8, 500 GB, 14 Pulgadas	Viviana Holanda	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
93	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Grecia Samudio	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
94	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Juan Carlos Guvas	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
95	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Victoria Gutiérrez	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
96	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Hilary Vargas	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	
97	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	Adriana Docarmo	HARD WARE	A	A	A	M	M	NO	SI	SI	SI	SI	SI		X		X	

ANEXO 6. NOMENCLATURA DE LA VALORACION DEL RIESGO

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

ANEXO 7. MATRIZ VALORACION DEL RIESGO DE LOS ACTIVOS DE INFORMACION

	Matriz Valoración de Riesgos de los Activo							
No	**Nombre**	**Riesgo**	**AUTENTICIDAD**	**TRAZABILIDAD**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**VALOR**
1	Computador Portátil I5, Gen 8, 1TB HDD, 14 pulgadas.	CRITICO	25	20	25	20	25	23
2	Escáner Epson DS-420	BAJO	9	9	9	9	9	9
3	Impresora Epson L3250	APRECIABLE	9	9	9	20	20	13
4	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
5	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
6	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
7	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20

8	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
9	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
10	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
11	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
12	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
13	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
14	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
15	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
16	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
17	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
18	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
19	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
20	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
21	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
22	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
23	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
24	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
25	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
26	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
27	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
28	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
29	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
30	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25

31	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
32	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
33	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
34	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
35	Servidor PCTG	CRITICO	25	25	25	25	25	25
36	Router	IMPORTANTE	20	20	20	20	20	20
37	Plataformas	CRITICO	20	25	20	20	20	21
38	internet	CRITICO	25	20	20	20	20	21
39	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
40	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
41	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
42	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
43	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
44	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
45	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
46	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
47	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
48	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
49	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
50	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
51	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
52	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
53	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18

54	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
55	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
56	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
57	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
58	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
59	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	25	15	20	20
60	Windows 10 Profesional	IMPORTANTE	20	15	20	20	9	17
61	Office 2016 Profesional	IMPORTANTE	20	15	15	20	20	18
62	PCTG ENTERPRISE	CRITICO	25	25	25	25	25	25
63	Todo en Uno I7, Gen 10, 1TB SDD, 14 pulgadas.	CRITICO	25	25	25	25	25	25
64	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
65	Computador Portátil I5, Gen 10, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	15	20	15	15	17
66	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
67	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	25	20	20	15	15	19
68	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	15	15	20	18
69	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
70	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	20	15	19
71	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	15	20	15	15	17
72	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	20	19

73	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
74	Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	CRITICO	25	25	25	25	25	25
75	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
76	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
77	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	25	20	20	15	15	19
78	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	20	19
79	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	15	20	15	15	17
80	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	20	19
81	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	15	15	20	15	15	16
82	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	20	15	19
83	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	15	15	15	17
84	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	15	15	20	15	20	17
85	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
86	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	20	19
87	Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	CRITICO	25	25	25	25	25	25
88	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
89	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18

90	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
91	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
92	Computador Portátil I5 Gen 8, 500 GB, 14 Pulgadas	IMPORTANTE	20	20	20	15	15	18
93	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
94	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
95	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
96	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18
97	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	IMPORTANTE	20	20	20	15	15	18

ANEXO 8. GESTION DEL RIESGO Y PLAN DE TRATAMIENTO

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual	Plan de Tratamiento						
															control a aplicar a partir de la norma ISO 27001					
														Transefir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL

1	HARD WARE	Computador Portátil I5, Gen 8, 1TB HDD, 14 pulgadas.	**23**	[E2] Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	**5**	**4**	**4**	**2**	**4**	**3**	**3**	**2**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.1 Políticas para la seguridad de la información --Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
2	HARD WARE	Escáner Epson DS-420	**9**	[I2] Daños por agua	escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	**2**	**1**	**1**	**1**	**2**	**2**	**1**	**1**	**x**		**x**		DOMINIO_A6	OBJETIVO_A6_1	A6.1.3 Contacto con las autoridades --Control: Se deben mantener contactos apropiados con las autoridades pertinentes.
3	HARD WARE	Impresora Epson L3250	**13**	[A25] Robo	a sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.	**3**	**2**	**2**	**2**	**1**	**2**	**2**	**2**			**x**	**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

4	SOFTWARE	Windows 10 Profesional	**17**	[E19] Fugas de información	Incontinencia verbal, medios electrónicos, soporte papel, etc.	**4**	**3**	**3**	**2**	**1**	**2**	**2**	**1**				**x**	DOMINIO_A15	OBJETIVO_A15_1	A15.1.3 Cadena de suministro de tecnología de información y comunicación --Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
5	SOFTWARE	Office 2016 Profesional	**18**	[A18] Destrucción de información	eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	**2**	**3**	**3**	**3**	**2**	**3**	**2**	**1**				**x**	DOMINIO_A8	OBJETIVO_A8_1	A8.1.3 Uso aceptable de los activos --Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
6	SOFTWARE	PCTG ENTERPRISE	**25**	[E21] Errores de mantenimiento / actualización de programas (software)	defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	**5**	**4**	**5**	**4**	**4**	**3**	**3**	**4**				**x**	DOMINIO_A10	OBJETIVO_A10_1	A10.1.1 Política sobre el uso de controles criptográficos --Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
7	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[A23] Manipulación de los equipos	alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	**3**	**3**	**3**	**2**	**3**	**3**	**2**	**3**		**x**		**x**	DOMINIO_A6	OBJETIVO_A6_2	A6.2.1 Política para dispositivos móviles --Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
8	SOFTWARE	Windows 10 Profesional	**17**	[A8] Difusión de software dañino	propagación intencionada de virus, espías (spyware), gusanos,	**4**	**3**	**3**	**2**	**1**	**2**	**2**	**1**				**x**	DOMINIO_A14	OBJETIVO_A14_1	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones. --Control: La información involucrada en

					troyanos, bombas lógicas, etc.														las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
9	SOFT WARE	Office 2016 Profesional	**18**	[E9] Errores de [re-]encaminamiento	envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	**2**	**3**	**3**	**3**	**2**	**2**	**2**	**1**	**x**				DOMINIO_A11	OBJETIVO_A11_1	A11.1.6 Áreas de carga, despacho y acceso público --Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
10	SOFT WARE	PCTG ENTERPRISE	**25**	[A5] Suplantación de la identidad del usuario	cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por	**4**	**5**	**3**	**4**	**3**	**2**	**3**	**3**			**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.

					personal contratado temporalmente.															
11	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[I7] Condiciones inadecuadas de temperatura o humedad	deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad,	**3**	**3**	**2**	**3**	**2**	**3**	**1**	**1**				**x**	DOMINIO_A8	OBJETIVO_A8_1	A8.1.1 Inventario de activos --Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
12	SOFT WARE	Windows 10 Profesional	**17**	[A18] Destrucción de información	eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	**4**	**3**	**3**	**2**	**1**	**2**	**2**	**1**			**x**	**x**	DOMINIO_A11	OBJETIVO_A11_1	A11.1.5 Trabajo en áreas seguras. --Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
13	SOFT WARE	Office 2016 Profesional	**18**	[A19] Divulgación de información	revelación de información.	**2**	**3**	**3**	**3**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A12	OBJETIVO_A12_4	A12.4.2 Protección de la información de registro --Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
14	SOFT WARE	PCTG ENTERPRISE	**25**	[A6] Abuso de privilegios de acceso	cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	**4**	**3**	**2**	**1**	**3**	**2**	**2**	**2**		**x**		**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.

15	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[I2] Daños por agua	escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	**3**	**2**	**3**	**2**	**3**	**2**	**1**	**1**				**x**	DOMINIO_A17	OBJETIVO_A17_1	A17.1.1 Planificación de la continuidad de la seguridad de la información --Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
16	SOFT WARE	Windows 10 Profesional	**17**	[A6] Abuso de privilegios de acceso	cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	**4**	**3**	**3**	**2**	**1**	**2**	**2**	**1**				**x**	DOMINIO_A6	OBJETIVO_A6_1	A6.1.1 Roles y responsabilidades para la seguridad de la información --Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
17	SOFT WARE	Office 2016 Profesional	**18**	[E8] Difusión de software dañino	propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	**2**	**3**	**3**	**3**	**2**	**2**	**2**	**1**		**x**		**x**	DOMINIO_A8	OBJETIVO_A8_1	A8.1.3 Uso aceptable de los activos --Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
18	SOFT WARE	PCTG ENTERPRISE	**25**	[A7] Uso no previsto	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de	**3**	**3**	**2**	**3**	**2**	**2**	**1**	**1**		**x**		**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

					datos personales, etc.														
19	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[I5] Avería de origen físico o lógico	fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	**3**	**3**	**3**	**2**	**3**	**2**	**2**	**2**				**x**	DO MIN IO_ A8	OBJ ETI VO_ A8_ 1	A8.1.3 Uso aceptable de los activos --Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
20	SOFT WARE	Windows 10 Profesional	**17**	[E2] Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	**4**	**3**	**3**	**2**	**1**	**2**	**2**	**1**				**x**	DO MIN IO_ A10	OBJ ETI VO_ A10 _1	A10.1.2 Gestión de llaves --Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
21	SOFT WARE	Office 2016 Profesional	**18**	[A15] Modificación deliberada de la información	alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	**2**	**3**	**3**	**3**	**2**	**2**	**2**	**1**		**x**		**x**	DO MIN IO_ A14	OBJ ETI VO_ A14 _1	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones. --Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de

																			mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
22	SOFTWARE	PCTG ENTERPRISE	**25**	[E21] Errores de mantenimiento / actualización de programas (software)	defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	**4**	**2**	**2**	**2**	**2**	**2**	**1**	**1**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
23	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[I2] Daños por agua	escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	**2**	**3**	**2**	**1**	**2**	**2**	**1**	**1**				**x**	DOMINIO_A6	OBJETIVO_A6_1	A6.1.3 Contacto con las autoridades --Control: Se deben mantener contactos apropiados con las autoridades pertinentes.
24	SOFTWARE	Windows 10 Profesional	**17**	[A8] Difusión de software dañino	propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	**4**	**3**	**3**	**2**	**1**	**2**	**2**	**1**		**x**		**x**	DOMINIO_A18	OBJETIVO_A18_1	A18.1.3 Protección de registros --Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
25	SOFTWARE	Office 2016 Profesional	**18**	[A8] Difusión de software dañino	propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	**2**	**3**	**3**	**3**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A18	OBJETIVO_A18_2	A18.2.2 Cumplimiento con las políticas y normas de seguridad --Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

26	SOFT WARE	PCTG ENTERPRISE	**25**	[A7] Uso no previsto	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	**4**	**3**	**2**	**2**	**3**	**2**	**1**	**1**			**x**	**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
27	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[A6] Abuso de privilegios de acceso	cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	**2**	**2**	**3**	**3**	**2**	**2**	**2**	**1**		**x**		**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
28	SOFT WARE	Windows 10 Profesional	**17**	[A18] Destrucción de información	eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	**4**	**3**	**3**	**2**	**1**	**2**	**2**	**1**				**x**	DOMINIO_A9	OBJETIVO_A9_1	A9.1.2 Acceso a redes y a servicios en red --Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
29	SOFT WARE	Office 2016 Profesional	**18**	[A7] Uso no previsto	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas	**2**	**3**	**3**	**3**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos --Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

					personales, almacenamiento de datos personales, etc.															
30	SOFTWARE	PCTG ENTERPRISE	**25**	[A18] Destrucción de información	eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	**4**	**2**	**2**	**3**	**2**	**2**	**1**	**2**			**x**	**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
31	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[I1] Fuego	incendio: posibilidad de que el fuego acabe con los recursos del sistema.	**2**	**4**	**2**	**2**	**2**	**3**	**1**	**1**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
32	SOFTWARE	Windows 10 Profesional	**17**	[E2] Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	**4**	**3**	**3**	**2**	**1**	**2**	**2**	**1**				**x**	DOMINIO_A9	OBJETIVO_A9_1	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.
33	SOFTWARE	Office 2016 Profesional	**18**	[E18] Destrucción de información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	**2**	**3**	**3**	**3**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A8	OBJETIVO_A8_1	A8.1.2 Propiedad de los activos --Control: Los activos mantenidos en el inventario deben tener un propietario.

34	SOFT WARE	PCTG ENTERPRISE	**25**	[A22] Manipulación de programas	alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	**4**	**3**	**2**	**3**	**2**	**2**	**2**	**1**			**x**	**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
35	SOFT WARE	Servidor PCTG	**25**	[E1] Errores de los usuarios	equivocaciones de las personas cuando usan los servicios, datos, etc.	**4**	**3**	**4**	**3**	**4**	**3**	**2**	**2**			**x**	**x**	DOMINIO_A10	OBJETIVO_A10_1	A10.1.2 Gestión de llaves --Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
36	HARD WARE	Router	**20**	[N2] Daños por agua	inundaciones: posibilidad de que el agua acabe con recursos del sistema.	**3**	**2**	**2**	**3**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
37	DATOS	Plataformas	**21**	[E19] Fugas de información	Incontinencia verbal, medios electrónicos, soporte papel, etc.	**4**	**3**	**3**	**4**	**2**	**3**	**2**	**1**		**x**		**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
38	SERVICIOS	internet	**21**	[E19] Fugas de información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay	**3**	**4**	**3**	**3**	**2**	**3**	**2**	**2**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.5 Respuesta a incidentes de seguridad de la información --Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

					amenazas específicas.															
39	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[A11] Acceso no autorizado	el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	**3**	**3**	**2**	**3**	**3**	**3**	**2**	**3**				**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
40	SOFT WARE	Windows 10 Profesional	**17**	[A8] Difusión de software dañino	propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	**3**	**3**	**3**	**2**	**3**	**3**	**3**	**2**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
41	SOFT WARE	Office 2016 Profesional	**18**	[A15] Modificación deliberada de la información	alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	**3**	**2**	**3**	**3**	**2**	**3**	**3**	**2**				**x**	DOMINIO_A18	OBJETIVO_A18_2	A18.2.3 Revisión del cumplimiento técnico -- Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.
42	SOFT WARE	PCTG ENTERPRISE	**25**	[E2] Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	**4**	**2**	**3**	**3**	**2**	**3**	**2**	**1**		**x**		**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su

																				conveniencia, adecuación y eficacia continuas.
43	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[A24] Denegación de servicio	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	**2**	**3**	**1**	**2**	**3**	**3**	**2**	**1**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
44	SOFT WARE	Windows 10 Profesional	**17**	[E9] Errores de [re-]encaminamiento	envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	**2**	**3**	**2**	**1**	**2**	**2**	**2**	**1**			**x**	**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
45	SOFT WARE	Office 2016 Profesional	**18**	[A7] Uso no previsto	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas	**3**	**3**	**2**	**2**	**1**	**2**	**2**	**2**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren

					personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.														cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
46	SOFT WARE	PCTG ENTERPRISE	**25**	[A19] Divulgación de información	revelación de información.	**3**	**2**	**3**	**2**	**2**	**2**	**2**	**2**				**x**	DOMINIO_A18	OBJETIVO_A18_2	A18.2.3 Revisión del cumplimiento técnico --Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.
47	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[A25] Robo	a sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.	**3**	**3**	**3**	**2**	**3**	**3**	**2**	**2**		**x**		**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

48	SOFT WARE	Windows 10 Profesional	**17**	[E10] Errores de secuencia	alteración accidental del orden de los mensajes transmitidos.	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**				**x**	DO MIN IO_ A5	OBJ ETI VO_ A5_ 1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
49	SOFT WARE	Office 2016 Profesional	**18**	[A8] Difusión de softwar e dañino	propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	**2**	**2**	**2**	**3**	**2**	**2**	**1**	**1**				**x**	DO MIN IO_ A5	OBJ ETI VO_ A5_ 1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
50	SOFT WARE	PCTG ENTERPRISE	**25**	[A15] Modific ación delibera da de la informa ción	alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	**4**	**3**	**4**	**4**	**2**	**4**	**2**	**2**				**x**	DO MIN IO_ A5	OBJ ETI VO_ A5_ 1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
51	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[I1] Fuego	incendio: posibilidad de que el fuego acabe con los recursos del sistema.	**3**	**2**	**3**	**2**	**2**	**2**	**1**	**2**				**x**	DO MIN IO_ A16	OBJ ETI VO_ A16 _1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

52	SOFT WARE	Windows 10 Profesional	**17**	[E21] Errores de mantenimiento / actualización de programas (software)	defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	**3**	**2**	**3**	**2**	**2**	**2**	**1**	**1**				**x**	DOMINIO_A17	OBJETIVO_A17_1	A17.1.2 Implementación de la continuidad de la seguridad de la información --Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
53	SOFT WARE	Office 2016 Profesional	**18**	[A5] Suplantación de la identidad del usuario	cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	**3**	**3**	**2**	**3**	**2**	**2**	**1**	**1**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
54	SOFT WARE	PCTG ENTERPRISE	**25**	[A19] Divulgación de información	revelación de información.	**4**	**3**	**2**	**3**	**3**	**2**	**2**	**1**		**x**		**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
55	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[I3] Contaminación mecánica	vibraciones, polvo, suciedad	**3**	**2**	**3**	**3**	**3**	**2**	**3**	**2**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión

																				apropiados, tan pronto como sea posible.
56	SOFT WARE	Windows 10 Profesional	**17**	[A18] Destrucción de información	eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	**3**	**2**	**3**	**3**	**2**	**2**	**2**	**2**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
57	SOFT WARE	Office 2016 Profesional	**18**	[A8] Difusión de software dañino	propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	**2**	**3**	**2**	**2**	**1**	**2**	**2**	**2**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
58	SOFT WARE	PCTG ENTERPRISE	**25**	[A19] Divulgación de información	revelación de información.	**4**	**3**	**3**	**3**	**3**	**3**	**1**	**2**		**x**		**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
59	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**20**	[A25] Robo	a sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El	**2**	**3**	**2**	**3**	**1**	**2**	**3**	**2**				**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia

					robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.															suficiente para cumplir los requisitos de disponibilidad.
60	SOFT WARE	Windows 10 Profesional	**17**	[A22] Manipulación de programas	alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	**2**	**2**	**3**	**2**	**2**	**2**	**1**	**1**				**x**	DOMINIO_A18	OBJETIVO_A18_2	A18.2.3 Revisión del cumplimiento técnico -- Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.
61	SOFT WARE	Office 2016 Profesional	**18**	[A6] Abuso de privilegios de acceso	cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	**2**	**3**	**2**	**1**	**1**	**2**	**2**	**2**				**x**	DOMINIO_A14	OBJETIVO_A14_1	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones. --Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

62	SOFTWARE	PCTG ENTERPRISE	**25**	[E2] Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	**3**	**2**	**3**	**2**	**1**	**2**	**2**	**2**		**x**		**x**	DOMINIO_A10	OBJETIVO_A10_1	A10.1.2 Gestión de llaves --Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
63	HARDWARE	Todo en Uno I7, Gen 10, 1TB SDD, 14 pulgadas.	**25**	[I4] Contaminación electro magnética	interferencias de radio, campos magnéticos, luz ultravioleta, ...	**4**	**3**	**2**	**3**	**3**	**3**	**2**	**1**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
64	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[E24] Caída del sistema por agotamiento de recursos	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	**2**	**2**	**1**	**2**	**3**	**2**	**1**	**2**		**x**		**x**	DOMINIO_A12	OBJETIVO_A12_4	A12.4.2 Protección de la información de registro --Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
65	HARDWARE	Computador Portátil I5, Gen 10, 1TB HDD, 14 pulgadas.	**17**	[E2] Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	**2**	**3**	**2**	**1**	**1**	**2**	**1**	**2**				**x**	DOMINIO_A10	OBJETIVO_A10_1	A10.1.2 Gestión de llaves --Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
66	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[A25] Robo	a sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes	**2**	**3**	**2**	**1**	**2**	**2**	**1**	**1**		**x**		**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

					de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.															
67	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**19**	[I2] Daños por agua	escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	**3**	**2**	**2**	**2**	**1**	**2**	**2**	**2**		**x**		**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
68	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[I11] Emanaciones electro magnéticas	hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero	**2**	**1**	**2**	**2**	**2**	**2**	**1**	**1**			**x**	**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

					frecuentemente, ataque TEMPEST (del inglés “Transiten Electromagnética Pulse Standard”). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "TEMPEST protección", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.														
69	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[A24] Denegación de servicio	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	**3**	**2**	**1**	**2**	**2**	**2**	**1**	**1**		**x**		**x**	DOMINIO_A18	OBJETIVO_A18_2	A18.2.3 Revisión del cumplimiento técnico -- Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.
70	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**19**	[E24] Caída del sistema por agotami	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	**3**	**2**	**3**	**2**	**2**	**2**	**1**	**2**	**x**			**x**	DOMINIO_A12	OBJETIVO_A12_4	A12.4.2 Protección de la información de registro -- Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

				ento de recursos															
71	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**17**	[A25] Robo	a sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.	**2**	**2**	**3**	**2**	**3**	**2**	**1**	**1**			**x**	**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
72	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**19**	[I1] Fuego	incendio: posibilidad de que el fuego acabe con los recursos del sistema.	**2**	**3**	**2**	**2**	**2**	**2**	**1**	**2**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

73	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[I4] Contaminación electro magnética	interferencias de radio, campos magnéticos, luz ultravioleta, ...	**2**	**3**	**2**	**1**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A14	OBJETIVO_A14_1	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones. --Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
74	HARD WARE	Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	**25**	[I11] Emanaciones electro magnéticas	hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés “Transiten Electromagnética Pulse Standard”). Abusando del significado primigenio, es	**3**	**2**	**1**	**2**	**1**	**2**	**2**	**1**		**x**		**x**	DOMINIO_A14	OBJETIVO_A14_1	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones. --Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

					frecuente oír hablar de que un equipo disfruta de "TEMPEST protección", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.														
75	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[E23] Errores de mantenimiento / actualización de equipos (hardware)	defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	**3**	**2**	**1**	**2**	**2**	**2**	**1**	**1**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
76	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[A24] Denegación de servicio	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	**3**	**2**	**1**	**2**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A18	OBJETIVO_A18_2	A18.2.3 Revisión del cumplimiento técnico -- Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

77	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**19**	[E24] Caída del sistema por agotamiento de recursos	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	**2**	**1**	**2**	**1**	**2**	**2**	**1**	**2**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
78	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**19**	[I3] Contaminación mecánica	vibraciones, polvo, suciedad	**3**	**2**	**1**	**1**	**1**	**2**	**2**	**2**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
79	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**17**	[A24] Denegación de servicio	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	**3**	**2**	**3**	**2**	**2**	**2**	**2**	**1**		**x**		**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
80	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**19**	[E23] Errores de mantenimiento / actualización de equipos (hardware)	defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	**2**	**2**	**2**	**1**	**3**	**2**	**3**	**2**			**x**	**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
81	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**16**	[E2] Errores del	equivocaciones de personas con responsabilidades de	**2**	**2**	**2**	**3**	**2**	**2**	**1**	**1**				**x**	DOMINIO_A10	OBJETIVO_	A10.1.2 Gestión de llaves --Control: Se debe desarrollar e implementar una política sobre el uso, protección y

				administrador	instalación y operación													A10_1	tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
82	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**19**	[A23] Manipulación de los equipos	alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	**2**	**2**	**2**	**3**	**3**	**2**	**1**	**2**				**x**	DOMINIO_A12	OBJETIVO_A12_4	A12.4.2 Protección de la información de registro -- Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
83	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**17**	[A24] Denegación de servicio	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	**2**	**3**	**2**	**1**	**2**	**2**	**1**	**2**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
84	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**17**	[E2] Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	**3**	**2**	**1**	**1**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A18	OBJETIVO_A18_2	A18.2.3 Revisión del cumplimiento técnico -- Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.
85	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[A26] Ataque destructivo	Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**2**				**x**	DOMINIO_A12	OBJETIVO_A12_4	A12.4.2 Protección de la información de registro -- Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
86	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**19**	[A26] Ataque destructivo	Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para

																			para asegurar su conveniencia, adecuación y eficacia continuas.
87	HARDWARE	Todo en Uno I7, Gen 12, 1TB SDD, 17 pulgadas.	**25**	[A25] Robo	a sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.	**3**	**3**	**2**	**2**	**2**	**3**	**2**	**3**		**x**		**x**	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
88	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[A11] Acceso no autorizado	el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	**3**	**2**	**3**	**3**	**2**	**2**	**1**	**1**			**x**	**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

89	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[N1] Fuego	incendios: posibilidad de que el fuego acabe con recursos del sistema.	**1**	**1**	**2**	**2**	**3**	**2**	**1**	**2**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
90	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[I2] Daños por agua	escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	**2**	**3**	**2**	**1**	**1**	**2**	**1**	**1**				**x**	DOMINIO_A6	OBJETIVO_A6_1	A6.1.3 Contacto con las autoridades --Control: Se deben mantener contactos apropiados con las autoridades pertinentes.
91	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[A11] Acceso no autorizado	el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	**2**	**3**	**2**	**2**	**1**	**2**	**2**	**2**				**x**	DOMINIO_A18	OBJETIVO_A18_2	A18.2.3 Revisión del cumplimiento técnico -- Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.
92	HARDWARE	Computador Portátil I5 Gen 8, 500 GB, 14 Pulgadas	**18**	[E2] Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	**1**	**2**	**2**	**3**	**2**	**2**	**2**	**1**				**x**	DOMINIO_A10	OBJETIVO_A10_1	A10.1.2 Gestión de llaves -- Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
93	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[A26] Ataque destructivo	Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	**1**	**2**	**3**	**2**	**3**	**2**	**1**	**2**				**x**	DOMINIO_A5	OBJETIVO_A5_1	A5.1.2 Revisión de las políticas para la seguridad de la información. --Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.

94	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[I2] Daños por agua	escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	**2**	**1**	**2**	**3**	**2**	**2**	**1**	**1**				**x**	DO MIN IO_ A12	OBJ ETI VO_ A12 _4	A12.4.2 Protección de la información de registro --Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
95	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[I3] Contaminación mecánica	vibraciones, polvo, suciedad	**2**	**3**	**2**	**2**	**2**	**2**	**1**	**2**				**x**	DO MIN IO_ A12	OBJ ETI VO_ A12 _4	A12.4.2 Protección de la información de registro --Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
96	HARD WARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[A25] Robo	a sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.	**2**	**3**	**3**	**3**	**2**	**2**	**1**	**1**				**x**	DO MIN IO_ A17	OBJ ETI VO_ A17 _2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

97	HARDWARE	Todo en Uno I5, Gen 8, 1TB HDD, 14 pulgadas.	**18**	[I7] Condiciones inadecuadas de temperatura o humedad	deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad,	**2**	**3**	**1**	**2**	**1**	**2**	**2**	**1**				**x**	DOMINIO_A16	OBJETIVO_A16_1	A16.1.2 Reporte de eventos de seguridad de la información --Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.