INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN GRUPO DE INVESTIGACIÓN FICB-PG

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA DE PUERTO ASÍS EN SU FASE DE DIAGNOSTICO Y PLANIFICACIÓN

PRESENTA:

MAURICIO SIERRA CUBIDES
CÓDIGO 1111070706
JHONY ALBERTO HURTADO CASTRILLON
CÓDIGO 1612010831

ASESOR TEMÁTICO:
WILMAR JAIMES FERNANDEZ MAGISTER

Mayo 2018

Tabla de contenido

ÍNDICE DE TABLAS 4

Índice de ilustraciones 5

RESUMEN 6

ABSTRACT 6

PALABRAS CLAVE 7

KEY WORDS 7

1. INTRODUCCIÓN 8

2. Descripción de la situación de interés 9

3. Planteamiento del problema 9

4. Objetivos del proyecto 11

4.1. Objetivo general 11

4.2. Objetivos específicos 11

5. Alcance 12

5.1 Plan de trabajo 12

6. Entregables 13

7. Estado del arte 13

8. Estrategia metodológica 14

9. RESULTADOS 16

9.1 ESTADO ACTUAL DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 16

..... 17

10 . Metodología para la definición de activos de información y gestión de riesgos. 18

11. Determinación de criticidad de los activos: 22

12. VALORACION RIESGOS ACTIVOS DE INFORMACION 24

13. ANALISIS DE RIESGO INHERENTE 29
14. MAPA DE CALOR 33
15. Mapa de riesgo inherente 36
16. CONTROLES 37
17. CONCLUSIONES 40
18. Lista de referencias 42
19. Anexos 43

ÍNDICE DE TABLAS

Tabla 1 Plan de trabajo 12
Tabla 2 Escala de valoración de controles anexo 1..... 16
Tabla 3 Tipos de activos de información de la Alcaldía de Puerto Asís. 19
Tabla 4 Inventario de activos de información Alcaldía de Puerto Asís general. 20
Tabla 5 Valoración de activos de información. 21
Tabla 6 Preguntas para determinar la criticidad del activo. 22
Tabla 7 Criticidad de los activos de información. 22
Tabla 8 categorización del nivel criticidad para activos información. 23
Tabla 9 **Activos de información seleccionados**. 23
Tabla 10 Activos de información agrupados de acuerdo con el contenedor. 24
Tabla 11 Riesgos y principios de seguridad afectados. 25
Tabla 12 **Amenazas que pueden afectar los activos**..... 26
Tabla 13 Vulnerabilidad asociado a las amenazas de activo..... 28
Tabla 14 Probabilidad de ocurrencia. 29
Tabla 15 Valoración del impacto..... 30
Tabla 16 Valoración del riesgo. 31
Tabla 17 Valoración de riesgo inherente. 32
Tabla 18 Riesgo inherente por tipo de riesgo. 33
Tabla 19 Mapa de calor a usar. 35
Tabla 20 Controles y riesgo inherente. 39

Índice de ilustraciones

Ilustración 1 Etapas previas de implementación 15
Ilustración 2 Brecha tomado de herramienta de diagnóstico MINTIC ISO 27001: 2013 ANEXO 1..... 18
Ilustración 3 Mapa de riesgo inherente. 36

RESUMEN

El presente trabajo está orientado hacia una entidad del sector publico la cual es la Alcaldía de Puerto Asís Putumayo, las entidades públicas deben cumplir lineamientos establecidos por el gobierno nacional para el caso nuestro estamos hablando de los lineamientos establecidos por el MINTICS atreves del programa gobierno en línea. El MINTIC establece un modelo para darle tratamiento a la seguridad y privacidad de la información dentro de las entidades públicas, en el desarrollo de este trabajo se usará dicho modelo para su fase de planificación. Para esto se empezará con las etapas previas a la implementación para conocer el estado actual de la entidad, identificar el nivel de madurez y el levantamiento de información. Basados en esta información y en un análisis de riesgos se procederá con la fase de panificación la cual involucra los siguientes elementos; contexto de la entidad, liderazgo, planeación y soporte.

ABSTRACT

This work is oriented towards an entity of the public sector which is the Mayor of Puerto Asís Putumayo, public entities must comply with guidelines established by the national government for our case we are talking about the guidelines established by the Ministry through the government program in line. The MINTIC establishes a model to treat the security and privacy of information within public entities, in the development of this work that model will be used for its planning phase. This will begin with the stages prior to implementation to know the current state of the entity, identify the level of maturity and the collection of information. Based on this information and a risk analysis will proceed with the baking phase which involves the following elements; context of the entity, leadership, planning and support.

PALABRAS CLAVE

Seguridad, privacidad, información, política, gobierno en línea, modelo de seguridad y privacidad de la información MSPI, riesgos, vulnerabilidades, entidad, MINTIC.

KEY WORDS

Security, privacy, information, policy, online government, MSPI, risks, vulnerabilities, entity, MINTIC.

1. INTRODUCCIÓN

El mundo organizacional tanto del sector público como privado se al continuo cambio de las nuevas tecnologías, esta trae beneficios para las organizaciones en cuanto a su forma de operar ya que las TIC son recursos muy importantes para el manejo de información y que hace que los procesos organizacionales sean cada vez más sistemáticos y eficientes. Por otra parte de la mano de esta revolución de las TIC también hay un avance de los piratas informáticos quienes buscan sacar beneficio de estas nuevas tecnologías para robar nuestra información o entorpecer nuestro procesos organizacionales, es por tal motivo que debemos estar preparados en los dos sentidos, avanzar a la vanguardia de los avances TIC y de esta manera ser más eficientes y competitivos y por el otro lado protegernos por medio de la implementación de planes y políticas robustas de aseguramiento de la información que incluyan un mejoramiento y actualización continua.

En este trabajo se realiza la aplicación del modelo de seguridad del ministerio de las tecnologías de la información y las comunicaciones MINTIC en su fase de planificación, con la finalidad de cumplir con este componente el cual se encuentra establecido dentro del programa gobierno en línea que deben implementar las entidades públicas colombianas.

Para esto se hace una etapa previa a la implementación en la cual se evalúa la entidad para conocer su estado actual en lo correspondiente a seguridad y privacidad de la información, para tener un punto de partida basado en un inventario de información y un análisis de riesgos de información.

2. Descripción de la situación de interés

El plan de gobierno en línea direccionada desde el MINTIC busca que las entidades públicas sean más transparentes en la prestación de sus trámites y servicios y que los ciudadanos estén más cerca de las entidades publicar y puedan interactuar con ellas por diferentes canales. La implementación de esta estrategia dentro de las entidades públicas está establecida en el manual de gobierno en línea. La estrategia gobierno en línea tiene un componente de seguridad y privacidad de la información el cual tiene unas fases para su implementación dentro de las entidades las cuales están establecidas en un modelo. Para el desarrollo de nuestro trabajo aplicaremos el modelo en su fase de planificación dentro de la alcaldía de Puerto Asís.

Por otro lado, los modelos de implantación de MINTIC tienen un retraso en la implementación, ya que estos se encuentran aprobados hace mas de 10 años, lo que por ahora no se obliga su implementación y la adopción del sistema si se deben adelantar tareas de iniciar a evaluar los activos que hacen parte de la entidad.

Muchas de las entidades gubernamentales no ven la necesidad de acatar dicho esquema, ya que no se ven representados de manera cuantitativa para la alcaldía, pero si se refleja en temas de seguridad al momento de protección de activos de información y su sensibilidad para el tratamiento y los que estas hacen de la imagen en la gestión pública.

La tarea del levantamiento de la información no se limita de manera física, sino va más allá de un tema de cultura organizacional, en el evento de adoptar hábitos en el manejo de la información, acompañado de entrenamiento mensual y seguimiento a los distintos controles implementados.

Con la entrada en función del decreto 2693 del 2012, donde se promueve la implementación de los SGSI, se destacan distintas guías que permiten actuar en el ordenamiento de la participación para las distintas entidades gubernamentales, ya que para el 2013, se tuvieron en cuenta distintas entidades como promotoras y ejemplo de implementación de los SGSI, siendo como referencia el sector legislativo y judicial.

3. Planteamiento del problema

Dentro de la entidad Alcaldía de Puerto Asís no existen controles para el tratamiento de la información, esto ha ocasionado fugas de información sensible, perdidas de información digital y física, fallas en el servidor, los funcionarios no cuentan con ningún tipo de capacitación para el manejo adecuado de la información.

Se hace necesaria la puesta en marcha de un modelo de seguridad en su fase de planificación para la entidad, ya que esta no cuenta con políticas definas para salvaguardar su información y tampoco cuenta con un análisis de riesgos para la misma viéndose seriamente comprometidos sus objetivos estratégicos organizacionales.

Un plan de seguridad y privacidad para la información permite establecer políticas, procesos, procedimientos y establecer controles para el aseguramiento de la información.

La información es un activo muy importante dentro de la entidad, el cual debemos proteger y poder mantener la continuidad en la atención a los trámites y servicios que se prestan a los ciudadanos.

En la entidad Alcaldía de Puerto Asís se vienen presentando problemas de fuga de información sensible y pérdida de información, esta problemática ocasiona que los procesos de la entidad se vean afectados puesto que los funcionarios no cuentan con ningún tipo de orientación para el tratamiento de la información y tampoco se tienen políticas establecidas para la seguridad de la información.

Es por este motivo que se debe realizar una planificación para la implementación de un sistema de privacidad y seguridad de la información de acuerdo con las necesidades de la entidad, el cual me proporcione confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad y de esta manera poder tener la información con un tratamiento adecuado y poder reducir al mínimo los riesgos para la información dentro de la entidad.

Dado el enunciado inicial, la relevancia del manejo de la información dentro de las alcaldías del país, juega un papel de seguridad e imagen para la gestión pública, por medio de la segmentación disponibilidad y manejo de la privacidad de datos, se garantiza la ejecución y actualización de datos para el ejercicio de rendición de cuentas en las distintas jornadas que dicha entidad desarrolla mensualmente.

Por otro lado al no tener un sistema único referenciado del manejo de información se hace vulnerable en el manejo de proyectos y ejercicios que emanen la ejecución del presupuesto gubernamental, al no tener una clasificación que organice la importancia y cultura organizacional sobre el manejo de datos.

4. Objetivos del proyecto

4.1. Objetivo general

Definición de metodología para el plan de seguridad de la información basado en el modelo de seguridad y privacidad de la información del MINTIC en su fase de planificación dentro de la alcaldía de Puerto Asís.

4.2. Objetivos específicos

a) Hacer una evaluación de la situación actual dentro de la Alcaldía de Puerto Asís en cuanto a seguridad y privacidad de la información.
b) Establecer la metodología para el análisis de riesgos para los activos de información y establecimiento de controles.

5. Alcance

Como resultado de este proyecto tendremos un documento con la metodología para la implementación del modelo de seguridad y privacidad de la información en su fase de planificación, basados en una evaluación previa con la realización de un inventario de activos de información y una metodología para el análisis de riesgos de entidad.

5.1 Plan de trabajo

Fases del proyecto	Tiempo requerido
Fase 1: **Diagnóstico de seguridad de la información de la entidad** ✓ Reunión con la dirección y control Interno. ✓ Reunión con área de sistemas.	15 días
Fase 2: **Aplicación del modelo de seguridad de la información en su fase de planificación.** ✓ Definición de activos de información de la entidad. ✓ Metodología para el análisis de riesgos de información.	Dos meses

Tabla 1 Plan de trabajo

6. Entregables

- Evaluación de la situación actual de la entidad en seguridad de la información.
- Metodología para el análisis de riesgos de información.

7. Estado del arte

Encontramos que con el uso y masificación de las tecnologías de la información y las comunicaciones dentro del sector privado como público se ha creado la necesidad de proteger la información frente a las diferentes amenazas tanto físicas como digitales. Es por esto que se han establecido normas que permiten estructurar políticas de seguridad para la información dentro de las entidades permitiendo de esta manera reducir a un mínimo la posibilidad de que una amenaza se materialice.

En la actualidad la mayoría de las entidades territoriales caso específico de las Alcaldías en municipios de sexta categoría no cuentan con políticas definidas para seguridad de la información, aunque dentro del programa del gobierno en línea se establece que se debe elaborar un sistema de seguridad de la información, son pocas las entidades que le han dado cumplimiento hasta la fecha, ya sea por falta de asesoría o por desinterés en el tema.

Encontramos casos de alcaldías de ciudades capitales las cuales, si cuentan con sistemas de gestión para seguridad de la información, es el caso de la implementación del modelo de seguridad y privacidad de la información de las entidades distritales en Bogotá. (Alta consejería distrital de TIC, 2016)

Se desarrolló un trabajo de grado para la Alcaldía de Fusagasugá que consistió en un modelo para la implementación del sistema general de seguridad informática basados en gestión de riesgo informático. (Repositorio UNAD, 2016). Tiene relación con el trabajo que queremos realizar, pero en este caso ellos establecieron un modelo para el establecimiento de políticas de seguridad de la información y para nuestro caso lo que se va a hacer es seguir en modelo de seguridad y privacidad de la información que establece MINTIC en su fase de planificación.

De igual forma se tiene referencias de la implementación de políticas de seguridad en la información en entidades como:

El banco de la republica también tiene establecidas las políticas generales de seguridad de la información. (Banco de la república)

Encontramos también el modelo de la política de seguridad de la información para organismos de la administración pública nacional (Administración Pública Nacional, 2015)

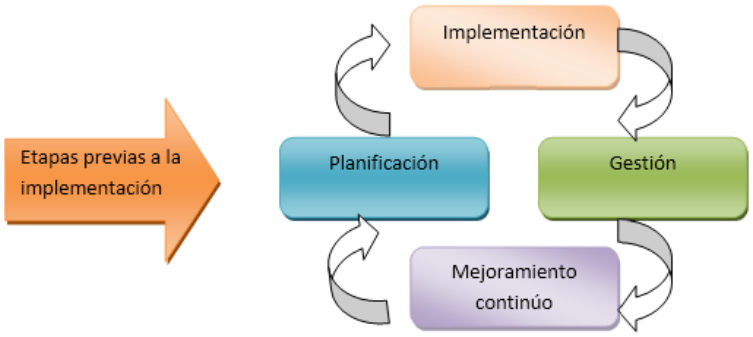
Secretaria de educación Bogotá, diseña un sistema de gestión de seguridad (S.G.S) para el área de talento humano para contratación.

Sistema de gestión de seguridad de la información (S.G.S.I.) para el centro de datos de la personería de Bogotá D.C. bajo las normas NTC-ISO-IEC 27001:2013 y NTC-ISO-IEC 27002:2013, el cual desarrollo como objetivo contribuir al mejoramiento de la seguridad del centro de datos de la Personería de Bogotá D.C., cumpliendo con la NTC-ISO-IEC 27001:2013 y GTC-ISO-IEC 27002:2015.

8. Estrategia metodológica

La estrategia metodológica consiste en realizar una evaluación dentro de la entidad para la determinación del estado actual de en cuanto a seguridad y privacidad para la información, para esto disponemos del instrumento de evaluación del MINTIC, el cual se aplicará en la entidad en compañía del jefe de sistemas en las dependencias de la Alcaldía de Puerto Asís.

Luego de tener la valoración de la situación actual en seguridad para la información se procede a realizar la definición de activos de información mediante una metodología que me permita hacer la valoración de riesgos y establecer una clasificación para el establecimiento de controles que me permitan salvaguardar mis activos de información y una posterior implementación del modelo del MINTIC en trabajos futuros figura 1**.**



Fases del modelo privacidad y seguridad y privacidad de la información MPSI.
Fuente: MSPI-MinTic - 2016

Ilustración 1 Etapas previas de implementación

De este modo tendremos definas las etapas previas a la implementación y una metodología que me va a permitir desarrollar la fase de planificación de este modelo.

Por otro lado es fundamental la adaptación de dichos modelos ya que permiten cuidar el activo más importante para la entidad t con esto cuidar su imagen ante el gobierno departamental ya que el estar atentos al desarrollo e implantación de dichos procesos hace que la alcaldía se un ente confiable y que cumple la norma vigente en cuanto al manejo de la información y adelantando a otras en el desarrollo de mejores prácticas que le permitan tener mejores incentivos ante la gobernación al ser imagen y mostrar orden y cumplimiento ante las nuevas exigencias del manejo de información.

Dado el instrumento de evaluación propuesto de MSPI, se hace presente la formulación y evaluación del estado de madurez del proyecto de evaluación, con el fin de desarrollar controles técnicos y de administración pública sobre las entidades gubernamentales, teniendo en cuenta que el ministerio de TICS, ha dejado la ruta a seguir como los modelos que pueden mejorar el funcionamiento y maximizar el erario publico impidiendo la comercialización del mismo.

9. RESULTADOS

9.1 ESTADO ACTUAL DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Para la evaluación del estado actual en seguridad y privacidad de la información se usaron las herramientas establecida para tal fin por MINTIC y su programa gobierno en línea.

Tabla 2 Escala de valoración de controles anexo 1.

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Teniendo en cuenta la valoración de la tabla 2 se realizó el levantamiento de información del cuyo resultado se encuentra en el anexo 1, permitiendo obtener la evaluación de efectividad de controles presentados en la tabla 2.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	1	60	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	1	60	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	20	60	INICIAL
A.8	GESTIÓN DE ACTIVOS	1	60	INEXISTENTE
A.9	CONTROL DE ACCESO	20	60	INICIAL
A.10	CRIPTOGRAFÍA	1	60	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	22	60	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	20	60	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	17	60	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	60	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	10	60	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	60	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	17	60	INICIAL
A.18	CUMPLIMIENTO	20	60	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		12	60	INICIAL

Tabla 3 Evaluación de efectividad de controles – tomado de herramienta de diagnóstico MINTIC ISO 27001: 2013 ANEXO 1

De acuerdo al análisis hecho mediante la herramienta de diagnóstico para seguridad y privacidad de la información en la alcaldía de Puerto Asís encontramos que se tiene un promedio de 12 sobre 100, teniendo de este modo un nivel de madurez inicial del modelo de seguridad y privacidad de la información, concluyendo con esto que no se cuenta con una identificación de activos que permitan una gestión de riesgos de información, respecto a la seguridad y privacidad por lo tanto los controles no están definidos hacia la preservación de la confidencialidad, integridad, disponibilidad y privacidad.

Ilustración 2 Brecha tomado de herramienta de diagnóstico MINTIC ISO 27001: 2013 ANEXO 1

Basados en estos resultados de diagnóstico nos damos cuenta que la alcaldía de Puerto Asís está en un nivel crítico en cuanto a de seguridad de la información exponiéndose a todo tipo de circunstancias a nivel de sus activos de información además de que puede recibir sanciones por parte de entes de control por no implementar las políticas establecidas por el MINTIC, es de este modo que de aquí en adelante nuestro trabajo consisten en establecer una metodología de identificación de activos de información y análisis de riesgo que le permita a la entidad iniciar un proceso para definir la fase de planificación dentro del modelo de seguridad.

10. Metodología para la definición de activos de información y gestión de riesgos.

Dentro de la metodología para la definición de activos de información y gestión de riesgos encontramos lo siguiente:

- Se identificarán los activos.
- Se hará la descripción de cada activo.
- Se identificarán los contenedores para cada activo.
- Se hará la identificación de los activos de información.
- Se asociarán los activos de acuerdo con cada contenedor.
- Se hará la valoración de los activos.
- Se identificarán los activos más críticos de los procesos.

Tipo de activo	Descripción
Servicios	Contempla servicios prestados por el sistema
Datos / información	Ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad.
Software	Programas, aplicativos, desarrollos, software base, sistema de información
Equipos informáticos	Hardware. Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización
Personal	Personas relacionadas con los sistemas de información.
Redes de comunicaciones	Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro
Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente
Equipamiento auxiliar	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones

Tabla 3 Tipos de activos de información de la Alcaldía de Puerto Asís.

Para el caso ejemplo de uso de la metodología definida, se toman los siguientes activos de información a trabajar:

- **Central principal de proceso:** Instalación física donde residen los Rack de comunicación.

- **Servidores de aplicación:** Servidores que soportan las aplicaciones y sistemas de información. Encontramos el software contable compuconta con el cual se maneja en todas las secretarias de la entidad para gestión de proyectos y procesos contables, además de la liquidación de impuestos.

- **Servidores de bases de datos:** equipos servidores que soportan motores pertenecientes a bases de datos. Aquí la información de la ciudadanía, proyectos, contabilidad, inventarios, información de personal entre otros.
- **Plataforma de correo electrónico:** Servidor que soporta la plataforma y servicio de correo electrónico. Toda la información que se comparte entre las dependencias

de la entidad además la que se comparte con otras entidades pasa a través de la plataforma de correo.

No	Nombre del Activo	Descripción del Activo	Tipo de Activo	Contenedor
A1	Central principal de proceso	Instalación física donde residen los Rack de comunicación.	Instalaciones	Cuartos rack
A2	Servidores de aplicación	Servidores que soportan las aplicaciones y sistemas de información	Equipos informáticos	Data center
A3	Servidores de bases de datos	Servidores que soportan motores de bases de datos	Equipos informáticos	Data center
A4	Plataforma de correo electrónico	Servidor que soporta la plataforma y servicio de correo electrónico.	Equipos informáticos	Data center

Tabla 4 Inventario de activos de información Alcaldía de Puerto Asís general.

Identificados los activos de información tabla 4, hacemos la valoración de grado de importancia y además de criticidad en la organización presentado en la tabla 5.

Aspecto	Criterio de valoración	Criterio de valoración	Valor a asignar
Financiero	Pérdidas económicas para la empresa (porcentaje calculado sobre la utilidad operacional)	Menor o igual a 0.25%	1
		Mayor a 0.25% y menor o igual a 5%	2
		Mayor a 5% y menor o igual a 20%	3
		Mayor a 20% y menor o igual a 50%	4
		Mayor al 50%	5
Legal	Incumplimiento de normatividad y legislación	No tiene repercusión frente a normatividad y contratos.	1
		Genera llamados de atención por parte de los entes de control.	2
		Genera posibles sanciones menores por parte de los entes de control y/o reclamos por parte de terceros.	3
		Genera sanciones económicas por parte de los entres de control y/o demandas por parte de terceros.	4
		Genera sanciones mayores por parte de entes de control, cancelación de contratos, suspensión de licencias, cierre de líneas de negocios.	5
Imagen	Afectación de la imagen de la empresa	Conocido solo de manera interna de la empresa pero no de interés publico	1
		Atención de algunas partes interesadas a nivel local que potencialmente puede afectar a la empresa	2
		Media atención de las partes interesadas a nivel local y regional.	3
		Alta Atención de las partes interesadas a nivel local, regional y nacional.	4
		Conocimiento general a nivel nacional e internacional.	5

Tabla 5 Valoración de activos de información.

11. Determinación de criticidad de los activos:

Criterio	Factor Afectado	Pregunta
Disponibilidad	Financiero	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control o demandas de terceros?
	Imagen	¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad?
Integridad	Financiero	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad?
Confidencialidad	Financiero	¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras?
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de regulaciones impartidas por entes de control o puede generar demandas de terceros?
	Imagen	¿Su divulgación no autorizada puede afectar la imagen de la entidad?

Tabla 6 Preguntas para determinar la criticidad del activo.

Con el fin de obtener la determinación del nivel de criticidad para el activo se utilizaron los siguientes criterios de valoración.

Criterio de Evaluación	Valor criticidad activo	Nivel criticidad
La gestión del activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información de la empresa.	>= 4	Alto
La gestión del activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información.	> 2 y < 4	Medio
La gestión del activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información de la empresa.	> 0 y <= 2	Bajo
La gestión del activo no compromete la integridad, confidencialidad y disponibilidad de la información de la empresa	Igual a 0	No aplica

Tabla 7 Criticidad de los activos de información.

No	Nombre del activo	Valoracion Nivel de Criticidad del Archivo													Nivel de criticidad
		Confidencialidad			Integridad			Disponibilidad							
		Financiero	Legal	Imagen	Financiero	Legal	Imagen	Financiero	Legal	Imagen	Confidencialidad	Integridad	Disponibilidad	Valor Total	
A1	Central principal de proceso	5	4	3	5	4	3	5	4	4	5	5	5	5	Alto
A2	Servidores de aplicación	4	3	2	4	2	2	4	2	2	4	4	4	4	Alto
A3	Servidores de bases de datos	4	3	2	4	2	2	4	2	2	4	4	4	4	Alto
A4	Plataforma de correo electrónico	3	3	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 8 categorización del nivel criticidad para activos información.

Trabajamos con los activos de información seleccionados para dar una orientación a la metodología.

No	Activo de Informacion	Nivel de criticidad	Contenedor
A1	Central principal de proceso	Alto	Cuartos rack
A2	Servidores de aplicación	Alto	Data center
A3	Servidores de bases de datos	Alto	Data center
A4	Plataforma de correo electrónico	Medio	Data center

Tabla 9 ***Activos de información seleccionados.***

Agrupamos los activos de información de acuerdo con el contenedor.

No	Activo de Informacion	Nivel de criticidad	Contenedor
A1	Central principal de proceso	Alto	Cuartos rack
A2	Servidores de aplicación	Alto	Data center
A3	Servidores de bases de datos	Alto	
A4	Plataforma de correo electrónico	Medio	

Tabla 10 Activos de información agrupados de acuerdo con el contenedor.

12. VALORACION RIESGOS ACTIVOS DE INFORMACION

Se continúa con la valoración de riesgos a los cuales se encuentran expuestos los activos de información identificados para esto se defienden las siguientes actividades dentro de la metodología:

- Identificar el riesgo.
- Analizar el riesgo residual.
- Construcción de la matriz de riesgo residual.
- Calificación a controles que hay para atenuar los riesgos residuales.
- Demarcación del riesgo residual.
- Construcción de la matriz para el riesgo residual.

Riesgos	Principios afectados		
	Confidencialidad	Integridad	Disponibilidad
Abuso de privilegios de acceso	x	x	
Acceso no autorizado	x	x	
Auditorias débiles			
Cambio de privilegios sin autorización	x	x	x
Denegación de Servicio			x
Divulgación o robo de información de autenticación			x
Divulgación no autorizada de información del negocio	x		
Ejecución de ingeniería social	x		
Errores del administrador	x	x	x
Instalación de software no autorizado		x	x
Interceptación no autorizada de información en tránsito	x		
Manipulación de la configuración	x		
Modificación sin autorización		x	
Pérdida o robo de información	x		x
Suplantación de identidad de usuarios	x	x	
Uso inadecuado de sistemas para generar fraudes	x	x	
Uso inadecuado de sistemas que generan interrupción			x

Tabla 11 Riesgos y principios de seguridad afectados.

De acuerdo con los riesgos y principios de seguridad afectados tabla 11 se identifican las amenazas con las cuales se ve comprometido el activos de información tabla 12.

Amenazas	Activo de informacion que puede ser afectado
Ataques Externos /internos (hacking)	Central principal de proceso , Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Acceso no aurorizado	Central principal de proceso , Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Cambio de privilegios sin autorizacion	Central principal de proceso , Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Desastres Naturales	Central principal de proceso
Error de admintracion	Central principal de proceso , Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Interceptacion no autorizada de informacion en transito	Plataforma de correo
Interrupcion en los servicios	Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Modificacion sis autorizacion	Central principal de proceso , Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Robo de informacion	Central principal de proceso , Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Suplantacion de identidad de usuarios	Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Uso inadecuado de sistemas para generar fraudes	Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico
Uso inadecuado de sistemas que generan interrupcion	Servidores de aplicación, Servidores de bases de datos,Plataforma de correo electrónico

Tabla 12 **Amenazas que pueden afectar los activos**.

De este modo se establecen las amenazas y vulnerabilidades asociadas a para el activo de información.

Amenazas	Activos	Vulnerabilidades
Ataques Externos /internos (hacking)	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Inadecuada plataforma de seguridad perimetral. -* inadecuada asignación de roles y permisos. * Falta de configuración en la red. -* Falta de seguridad en los puertos de red.
Acceso no autorizado	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Inadecuada plataforma de seguridad perimetral. -* Inadecuada asignación de roles y permisos. * Falta de configuración en la red. -* Contraseñas inseguras. -* Falta de seguridad en los puertos de red.
Cambio de privilegios sin autorización	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Contraseñas inseguras. -* Inadecuada asignación de roles y permisos. -* Inadecuada administración de seguridad. -* Políticas no aplicada o no existencia de seguridad.
Desastres Naturales	Central principal de proceso	-* Ausencia de un sistema de continuidad de negocio. -* Ubicación física de los equipos. -* Ubicación física del centro de cómputo -* Políticas no aplicada o no existencia de seguridad física.
Error de administración	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Inadecuada Administración de Seguridad. -* Contraseñas no seguras. -* Políticas no aplicada o no existencia de seguridad -*Inadecuada Administración o Asignación de roles y permisos. -* Inadecuado mecanismo de cifrado.
Interceptación no autorizada de información en transito	Plataforma de correo	-* Políticas no aplicada o no existencia de seguridad -* Inadecuado mecanismo de cifrado.

Interrupción en los servicios	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Inadecuada Configuración y Capacidad de los ambientes. -* Ausencia o inadecuado procedimiento de control de cambios. -* Falta de mantenimiento de equipos.
Modificación sin autorización	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Políticas no aplicada o no existencia de seguridad. -* Inadecuada Administración o Asignación de roles y permisos. -* Inadecuado mecanismo de cifrado.
Robo de información	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Inadecuada Administración de Seguridad -* Ausencia o Inadecuada plataforma de Seguridad Perimetral. -* Políticas no aplicada o no existencia de seguridad -* Inadecuada Administración o Asignación de roles y permisos. -* Inadecuado mecanismo de cifrado.
Suplantación de identidad de usuarios	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-*Contraseñas no seguras. -* Cuentas de usuario sin auditar. -* Ausencia o inadecuada plataforma de vigilancia física. -* Inadecuado mecanismo de cifrado.
Suplantación de identidad de usuarios	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-*Contraseñas no seguras. -* Cuentas de usuario sin auditar. -* Ausencia o inadecuada plataforma de vigilancia física. -* Inadecuado mecanismo de cifrado.
Uso inadecuado de sistemas para generar fraudes	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Inadecuada Administración de Seguridad. -* Cuentas de usuario sin auditar. -* Inadecuada Administración o Asignación de roles y permisos.
Uso inadecuado de sistemas que generan interrupción	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	-* Inadecuada Administración de Seguridad. -*Cuentas de usuario sin auditar. -* Inadecuada Administración o Asignación de roles y permisos. -* Políticas no aplicada o no existencia de seguridad.

Tabla 13 Vulnerabilidad asociado a las amenazas de activo.

13. ANALISIS DE RIESGO INHERENTE

Cuando hablamos de riesgo inherente nos enfocamos en el riesgo propio, sin tener en cuenta sus efectos de dichos controles iniciales, con el fin de tener éxito en la identificación y reducir el riesgo a niveles controlables, pasando por un proceso de un desarrollo de actividades continuas que fortalezcan el análisis de sobrepasar las opciones asumibles o trasladables del negocio.

Es fundamental dentro del proceso mantener una comunicación sencilla y enfocada a una ejecución manejable, que permita la integración de la cultura organizacional para generar un compromiso de la alta gerencia.

Partiendo de lo anterior, debemos identificar la probabilidad de que dicho riesgo ocurra con respecto a la probabilidad, teniendo valores cuantitativos o cualitativos para realizar el cálculo basados en función del impacto y probabilidades.

La determinación de la probabilidad de que una amenaza afecte los activos seleccionados se hizo con los criterios de valoración presentados en la tabla 14:

Probabilidad de ocurrencia en un (1) años	Valor Cualitativo	Valor Asignado
Una vez cada año	Raro	1
Una vez cada seis (6) meses	Baja (Improbable)	2
Una vez cada tres (3) meses	Media (Posible)	3
Una vez cada mes	Alta (Probable)	4
Más de una vez al mes	Muy Alta	5

Tabla 14 Probabilidad de ocurrencia.

Se usaron los criterios de valoración de la tabla 14 para obtener la valoración del impacto tabla 15.

Impacto	Impacto cuantitativo (Porcentaje sobre	Impacto Cualitativo (Uno o más factores)	Valor
Insignificante	Genera pérdidas financieras pequeñas no significativas. (Perdida Menor o igual a 0.25%)	• No afecta la seguridad de la información de la entidad. • No afecta la imagen de la entidad ante las partes interesadas. • Genera reprocesos insignificantes. • La información se puede recuperar rápidamente con la misma calidad.	1
Menor	Genera pérdidas financieras menores no significativas. (Perdida Mayor a 0.25% y menor o igual a 5%)	• No afecta la seguridad de la información de la entidad. • Afecta en menor grado la imagen de la entidad ante las partes interesadas. • Genera reprocesos menores. • La información se puede recuperar en un tiempo moderado con la misma calidad.	2
Moderado	Genera pérdidas financieras moderadas. (Mayor a 5% y menor o igual a 20%)	• Afecta en menor grado la seguridad de la información de la entidad. • Afecta medianamente la imagen de la entidad ante las partes interesadas. • Genera reprocesos moderados. • La información se puede recuperar pero no con la misma calidad	3
Mayor	Genera pérdidas financieras mayores. (Perdida mayor o igual a 20% y menor a 50%)	• Afecta en mayor grado la seguridad de la información de la entidad. • Afecta altamente la imagen de la entidad ante las partes interesadas. • Genera reprocesos mayores. • Es difícil recuperar la información	4
Catastrófico	Genera pérdidas financieras críticas. (Perdidas Mayores a 50%)	• Afectar seriamente la seguridad de la información de la entidad. • Afecta gravemente la imagen de la empresa ante las partes interesadas • Puede generar pérdida masiva de clientes. • Genera alto nivel de reprocesos. • Es difícil y costoso recuperar la información. • Afecta la continuidad del negocio	5

Tabla 15 Valoración del impacto.

La clasificación del riesgo residual varía de acuerdo a su nivel de riesgo, se empleó la clasificación de valoración para determinar el tipo de riesgo tabla 16:

Riesgo Extremo	Nivel Riesgo mayor o igual a 15 puntos	Requiere acciones inmediatas que permitan reducir y compartir el riesgo, transferirlo o incluso evitarlo
Riesgo Alto	Nivel Riesgo mayor o igual a 10 y menor a 15 puntos	Requieren atención urgente e implementar medidas para reducir el nivel del riesgo
Riesgo Medio	Nivel Riesgo mayor o igual a 5 y menor a 10 puntos	Requiere de medidas prontas y adecuadas que permitan disminuir el riesgo a nivel bajo o inusual
Riesgo Bajo	Nivel Riesgo mayor o igual a 3 y menor a 5 puntos	El riesgo se mitiga con actividades propias y por medio de algunas medidas preventivas para reducir el riesgo
Riesgo Inusual	Nivel Riesgo Menor a 3 puntos	Se puede aceptar el riesgo sin necesidad de tomar otras medidas de control diferentes a las existentes.

Tabla 16 Valoración del riesgo.

Como resultado de la valoración del riesgo residual para las amenazas de los activos de información seleccionados en el ejercicio se pueden observar los resultados en la tabla 17.

ID DEL RIESGO	RIESGOS	VALORACION IMPACTO			PROBABILIDAD	ESTIMACION DE RIESGOS			NIVEL DE RIESGO
		D	I	C		D	I	C	
R1	Ataques Externos /internos (hacking)	Mayor		Mayor	Alta	Riesgo extremo		Riesgo extremo	Riesgo extremo
R2	Acceso no aurorizado		Mayor	Catastrofico	Alta		Riesgo extremo	Riesgo extremo	Riesgo extremo
R3	Cambio de privilegios sin autorizacion	Moderado	Moderado	Moderado	Alta	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Alto
R4	Desastres Naturales	Mayor			Raro	Riesgo Bajo			Riesgo Bajo
R5	Error de administrador	Moderado			Alta	Riesgo Alto			Riesgo Alto
R6	Interceptacion no autorizada de informacion en transito		Mayor	Mayor	Alta		Riesgo extremo	Riesgo extremo	Riesgo extremo
R7	Interrupcion en los servicios	Moderado			Media	Riesgo Medio			Riesgo Medio
R8	Modificacion sis autorizacion		Moderado		Media		Riesgo Medio		Riesgo Medio
R9	Robo de informacion	Mayor		Mayor	Media	Riesgo Alto		Riesgo Alto	Riesgo Alto
R10	Suplantacion de identidad de usuarios			Moderado	Baja			Riesgo Medio	Riesgo Medio
R11	Uso inadecuado de sistemas para generar fraudes			Mayor				Riesgo Medio	Riesgo Medio
R12	Uso inadecuado de sistemas que generan interrupcion	Mayor			Baja	Riesgo Medio			Riesgo Medio

Tabla 17 Valoración de riesgo inherente.

ID DEL RIESGO	Riesgo	Activos	Probabilidad	Impacto	Nivel de riesgo probabilidad por impacto	
R1	Ataques Externos /internos (hacking)	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	4. Alta	4. Mayor	16	**Riesgo extremo**
R2	Acceso no autorizado	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	4. Alta	5. Catastrófico	20	**Riesgo extremo**
R6	Interceptación no autorizada de información en transito	Plataforma de correo	4. Alta	4. Mayor	16	**Riesgo extremo**
R3	Cambio de privilegios sin autorización	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	4. Alta	3. Moderado	12	Riesgo Alto

R11	Uso inadecuado de sistemas para generar fraudes	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	2. Baja	4. Mayor	8	Riesgo Medio
R12	Uso inadecuado de sistemas que generan interrupción	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	2. Baja	0. No afecta	8	Riesgo Medio
R13	Suplantación de identidad de usuarios	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	2. Baja	3. Moderado	6	Riesgo Medio
R4	Desastres Naturales	Central principal de proceso	1. Raro	0. No afecta	4	Riesgo Bajo
R5	Error de administración	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	4. Alta	0. No afecta	12	Riesgo Alto
R9	Robo de información	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	3. Media	4. Mayor	12	Riesgo Alto
R7	Interrupción en los servicios	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	3.Media	0. No afecta	9	Riesgo Medio
R8	Modificación sin autorización	Central principal de proceso, Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	3. Media	0. No afecta	9	Riesgo Medio
R11	Uso inadecuado de sistemas para generar fraudes	Servidores de aplicación, Servidores de bases de datos, Plataforma de correo electrónico	2. Baja	4. Mayor	8	Riesgo Medio

Tabla 18 Riesgo inherente por tipo de riesgo.

14. MAPA DE CALOR

Con el se puede analizar de manera gráfica por áreas donde se posicionan los riesgos, dependiendo de su probabilidad y su impacto. las áreas dentro del mapa de calor establecen un tipo de riesgo, el cual muestra las acciones que se deben efectuar para el tratamiento del riesgo.

Por medio de este se establecen los activos a tratar, lo que le permite a la mesa directiva realizar una correcta toma de decisiones y de esta forma implementar la mejor solución para la alcaldía.

Se detallan los activos que presenten mayores riesgos, con el fin de que estos sean mitigados o trasladados para con esto generar un resultado positivo en la solución planteada inicialmente, por otro lado, debemos tener en cuenta que el riego puede bajar su impacto, pero en ocasiones no desaparece.

Por otro lado, la realizar la clasificación de dichos riesgos se hace más fácil la toma de decisiones con respecto a la vulnerabilidad de activos, los que permite a la meda directiva establecer un panorama de tablero de control para realizar un tratamiento óptimo de los ítems surgidos después del inventario.

Al tener elaborado dicho cuadro, permite una explicación cruzada de prioridades para la ejecución y balance financiero de priorizar el costo beneficio de los mismos.

MAPA DE CALOR

IMPACTO	Riesgo Inusual	Riesgo Bajo	Riesgo Medio	Riesgo Alto	Riesgo Extremo
5	Zona de Riesgo Medio 5 puntos Reduir el Riesgo a niveles mas bajos	Zona de Riesgo Alto 10 puntos Evitar-Gestionar el Riesgo	Zona de Riesgo Extermo 15 punto Evitar-Gestionar Riesgo Requiere acción inmediata	Zona de Riesgo Extermo 20 punto Evitar-Gestionar Riesgo Requiere acción inmediata	Zona de Riesgo Extermo 25 punto Evitar-Gestionar Riesgo Requiere acción inmediata
4	Zona de Riesgo Bajo 4 puntos Administrar el Riesgos	Zona de Riesgo Medio 8 puntos Reduir el Riesgo a niveles mas bajos	Zona de Riesgo Alto 12 puntos Evitar-Gestionar el Riesgo	Zona de Riesgo Extermo 16 punto Evitar-Gestionar Riesgo Requiere acción inmediata	Zona de Riesgo Extermo 20 punto Evitar-Gestionar Riesgo Requiere acción inmediata
3	Zona de Riesgo Bajo 3 puntos Administrar el Riesgo	Zona de Riesgo Medio 6 puntos Reduir el Riesgo a niveles mas bajos	Zona de Riesgo Medio 9 puntos Reduir el Riesgo a niveles mas bajos	Zona de Riesgo Alto 12 puntos Evitar-Gestionar el Riesgo	Zona de Riesgo Extermo 15 punto Evitar-Gestionar Riesgo Requiere acción inmediata
2	Zona de Riesgo Inusual 2 puntos Asumir el Riesgo	Zona de Riesgo Bajo 4 puntos Administrar el Riesgo	Zona de Riesgo Medio 6 puntos Reduir el Riesgo a niveles mas bajos	Zona de Riesgo Medio 8 puntos Reduir el Riesgo a niveles mas bajos	Zona de Riesgo Alto 10 puntos Evitar-Gestionar el Riesgo
1	Zona de Riesgo Inusual 1 punto Asumir el Riesgo	Zona de Riesgo Inusual 2 puntos Asumir el Riesgo	Zona de Riesgo Bajo 3 puntos Administrar el Riesgo	Zona de Riesgo Bajo 4 puntos Administrar el Riesgo	Zona de Riesgo Medio 5 puntos Reduir el Riesgo a niveles mas bajos
	1	2	3	4	5

PROBABILIDAD

Tabla 19 Mapa de calor a usar.

15. Mapa de riesgo inherente

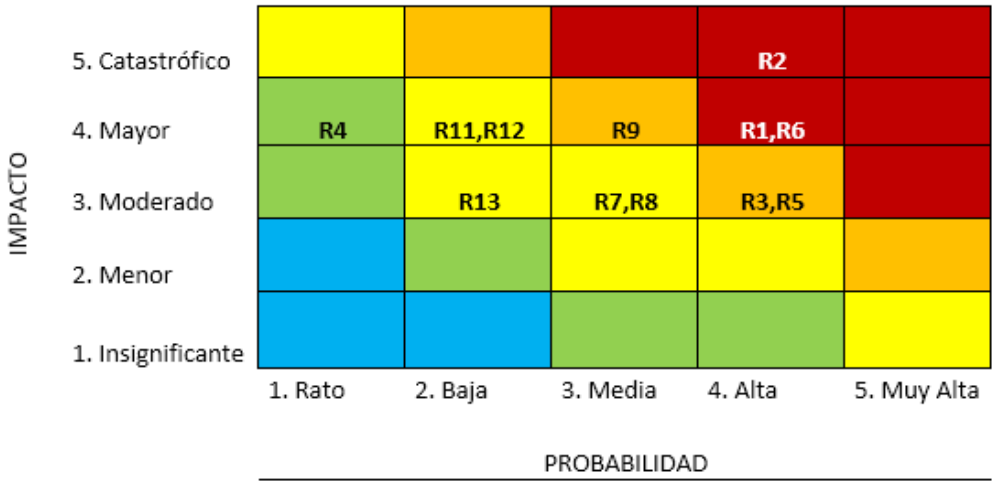


Figura 3. Mapa de riesgo inherente.

Ilustración 3 Mapa de riesgo inherente.

16. CONTROLES

ANALISIS DE CONTROLES						INHERENTE		
Riesgo	**Descripción del Control I**	**Descripción del Control II**	**Descripción del Control III**	**Tipo de Control**	**Como opera el Control**	**Impacto**	**Probabilidad**	**Nivel del Riesgo**
Ataques Externos /internos (hacking)	**C1** Establecer desde el directorio activo, prolíficas de roles que permitan la autenticación segmentada para el rastreo de posibles intrusiones sobre la plataforma tecnológica de la entidad.	**C2** Implementar herramientas como, Web Security Appliance, SSL Secure Site, escáner de seguridad, encriptación, entre otras que permitan la detección de intrusiones dentro de los servicios de la entidad.	**C3** Realizar un entrenamiento a todo el personal sobre el uso de USB, PC, Laptos, y conexiones externas de ingeniería social que permitan la integración con el SGSI de la entidad	Probabilidad / Impacto	Automático	MEDIO	MEDIO	RIESGO MEDIO

Acceso no autorizado	**C4** Establecer un sistema de control de acceso físico para el ingreso del visitante al recinto y funcionarios	**C5** Realizar la entrega de tarjetas de registro fotográfico adhesivas	**C6** Entrenamiento al personal de seguridad física perimetral para el manejo de situaciones de ingreso	Probabilidad / Impacto	Automático /manual	MEDIO	MUY BAJO	RIESGO BAJO
Interceptación no autorizada de información en transito	**C7** implementación de un firewall y routers o appliance que permitan a un servidos de FTP, una evolución de paquetes en la red.	**C8** Establecer niveles de acceso desde la política del directorio activo.	**C9** Entrenamiento mensual al personal sobre el manejo de información dentro de la red.	Probabilidad / Impacto	Automático	MEDIO	MUY BAJO	RIESGO BAJO
Cambio de privilegios sin autorización	**C10** Realizar una configuración y actualización de datos del personal activo dentro de la entidad	**C11** Definir políticas de acceso a nivel de Firewalls	**C12** Actualizar las configuraciones de Firewalls.	Probabilidad	Automático	MEDIO	MEDIO	RIESGO MEDIO

Error de administrador TI	**C13** Realizar una actualización de manuales y entrenamiento IT a los administradores de red	**C14** Definir procedimientos de Planes de Contingencias.	**C15** Establecer un plan de pruebas para la operabilidad del sistema	Probabilidad / Impacto	Automático /manual	MEDIO	MEDIO	RIESGO MEDIO
Robo de información	**C16** Mantener un control de inventario de activos asociado a controles lógicos del sistema.	**C17** Revisar periódicamente al acceso y controles de dispositivos conectados a la red	**C18** Entrenamiento constante para detectar el uso de ingeniería social dentro de las instalaciones	Probabilidad / Impacto	Automático /manual	MEDIO	MEDIO	RIESGO MEDIO

Tabla 20 Controles y riesgo inherente.

17. CONCLUSIONES

17.1.1 De acuerdo con el diagnóstico realizado dentro de la entidad alcaida de Puerto Asís se puede pudo evidenciar que tiene muchas falencias en seguridad y privacidad de la información, las cuales pueden llegar a perjudicar a la entidad en cualquier momento de no continuar con el desarrollo de la metodología planteada para establecer controles para todos sus activos de información.

17.1.2 Una buena identificación de activos de información me permite el desarrollo de un plan de seguridad y privacidad de la información robusto que me proporciona confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad y de esta manera poder tener la información con un tratamiento adecuado y poder reducir al mínimo los riesgos para la dentro de la entidad.

17.1.3 Los planes y políticas de seguridad de la información dentro de una entidad deben estar en constante revisión y actualización además de que se debe establecer un plan de socialización para los empleados.

17.1.4 El mantener un buen plan de SGSI se pueden estandarizar procesos y de este modo tener la mejor toma de decisiones en la alta gobernabilidad.

17.1.5 La seguridad de la información es un instrumento clave para brindar confianza en la elaboración de procesos gobernativos los cuales acreditan un orden en el establecimiento publico

17.1.6 EL actuar efectivamente por medio de modelos como es descrito en este documento, permite reorganizar y garantizar la información de la vía gubernativa.

17.1.7 Anticiparse antes de que hechos lamentables con el manejo de información y recursos públicos debe ser una misión constante.

17.1.8 Al realizar los procedimientos expuestos en este trabajo, se permite llevar a estándares congruentes para el manejo de la información.

17.1.9 Al mantener dichos lineamientos se pretende ser modelo para otras alcaldías y desarrollar las mejores practicas que se vean reflejadas en el trabajo cooperativo para el manejo de la información.

17.1.10 Al implementar el proceso mencionado, las herramientas permiten la integración y recolección de información para el desarrollo de tareas de actualización y estandarización de servicios de información.

17.1.11 Basados en el enfoque de riesgo gubernamental, se hace fundamental generar alertas constantes sobre el incentivas los respectivos planes de mejora y mitigación o traslados de riesgos asociados a los activos evaluados.

18. Lista de referencias

REFERENCIA. (20 de ENERO de 2010). Obtenido de WWW.REFERENCIA.COM

Adminstracion Publica Nacional. (2015). Obtenido de http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

Estrategia gobierno en linea. (2016). Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

Alcaldia de Puerto Asis. (2016). Recuperado el Noviembre de Marzo de 2018, de http://puertoasis-putumayo.gov.co/Paginas/default.aspx

Alta consejeria distrital de TIC. (2016). Obtenido de hhttp://ticbogota.gov.co/

Repostorio UNAD. (2016). Obtenido de http://repository.unad.edu.co/bitstream/10596/6327/1/35250225.pdf

Banco de la republica. (s.f.). Obtenido de http://www.banrep.gov.co/es/politicas-de-seguridad-de-la-informacion

19. Anexos

- ANEXO 1: Herramienta de diagnóstico MINTIC ISO 27001: 2013 aplicado a la Alcaldía de Puerto Asís.