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

2024

ALCALDIA DEL MUNICIPIO DE LA APARTADA

DEPARTAMENTO DE CORDOBA

OSCAR MIGUEL CALAO LÓPEZ

Alcalde

ENERO, 2024

TABLA DE CONTENIDO

Contenido

1. INTRODUCCION 4
2. OBJETIVOS 5
2.1. Objetivo general 5
2.2. Objetivos específicos 5
3. ALCANCE 5
4. DEFINICIONES 6
5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACION DEL RIESGO 10
6. POLITICA DE ADMINISTRACION DEL RIESGO 11
7. ETAPAS PARA LA ADMINISTRACION DEL RIESGO 12
8. DIMENSIONES DE SEGURIDAD 13
9. ANALISIS DE AMENAZAS 14
10. AMENAZAS 16
11. IMPACTO POTENCIAL 17
12. EVALUACION DEL RIESGO 17
13. VALORACION DE LOS RIESGOS 17
14. IDENTIFICACION DE CONTROLES 18
15. MANEJO DE RIESGOS 19
15.1. Controles de clase técnica 19
15.2. Controles de clase documental 19
15.3. Implementar programas de capacitación y sensibilización 19
15.4. Implementación de procedimiento de manejo de incidentes de seguridad 19
16. SEGUIMIENTO DE RIESGO 21
17. EQUIPO DE TRABAJO 22
17.1. UNIDAD PLANEACIÓN INFORMÁTICA 23
17.2. UNIDAD GESTIÓN INFORMÁTICA 23

Palacio municipal - Carrera 7 No. 20-21
Barrio Daniel Alfonso Paz
alcaldia@laapartada-cordoba.gov.co
Teléfono - 604 - 810 4319

17.3. UNIDAD INGENIERÍA Y TECNOLOGÍA INFORMÁTICA 23
17.4 UNIDAD OPERACIONES INFORMÁTICA 24
18. PENSAMIENTO ESTRATÉGICO 24
18.1. ESTRATEGIA 24
19. OPORTUNIDAD DE MEJORA 25
20. RECURSOS 25
21. PRESUPUESTO 25

1. INTRODUCCION

Los riesgos presentes en los sistemas de información son una amenaza permanente en el mundo físico y el entorno digital, donde estamos expuestos día a día a perdida de confidencialidad, integridad y disponibilidad de cada uno de los activos dispuestos.

Por lo anteriormente expuesto, dado que para el cumplimiento de las funciones del equipo de trabajo de la Alcaldía de La Apartada, está expuesto a riesgos, se hace necesario establecer una estructura y metodología en conjunto con lo dictaminado por el Ministerio de las TIC, para identificar las causas y consecuencias evitando la materialización de los eventos detectados, teniendo como fin la seguridad de la información bajo los principios de Integridad, Disponibilidad y Confidencialidad de la información.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos del estándar ISO 27001:2013, alineado con ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el Departamento Administrativo de la Función Pública y aquellas que la Alcaldía defina.

2. OBJETIVOS

2.1. Objetivo general

Dotar a la Alcaldía de la Apartada de una herramienta que le facilite identificar, evaluar, controlar y valorar los riesgos de los proyectos de tecnología de información que emprenda la administración, mejorando la gestión y mitigar la materialización de los riesgos de seguridad de la información en la Alcaldía La Apartada, con el fin de disminuir el impacto de la tecnología en los costos, recursos y tiempo, protegiendo y preservando la integridad, confidencialidad y disponibilidad y de la información.

2.2. Objetivos específicos

- Identificar, definir y documentar la metodología de evaluación y valoración de los riesgos asociados a los proyectos de tecnología de Información.
- Fomentar el uso y apropiación de la Política de Seguridad vigente en los funcionarios y contratistas, con mecanismos de control de riesgos para los proyectos de tecnologías de información de la Alcaldía Municipal La Apartada.
- Involucrar y comprometer a todos los funcionarios y contratistas en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos acordes a los requerimientos legales y reglamentarios pertinentes a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital alineado al plan de desarrollo Municipal.

3. ALCANCE

Definir y documentar la metodología de análisis y valoración de riesgos en proyectos de la tecnología de la información de una manera estructurada y modular, por fases

o etapas que permita identificar, evaluar, controlar y valorar los riesgos en el área de Gobierno Digital.

Con el propósito de realizar una eficiente gestión de riesgos de Seguridad Digital en la Alcaldía La Apartada, esta actividad se debe realizar integrando los procesos de la entidad con este plan, mediante el uso de buenas prácticas y lineamientos nacionales, y locales, con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

A partir de lo anterior definir los lineamientos mediante una guía para la gestión de riesgos de Seguridad Digital y tratamiento de los riesgos asociados a la información que es soportada por compontes tecnológicos en el entorno digital.

4. DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro de la Alcaldìa.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Ambiente Informativo: es la integración de tres componentes básicos: aplicación, tecnología y personas.

Aplicación: Conjunto de programas que soportan un proceso en la organización.

Aplicación crítica: Es aquella que, por ser esencial, requiere ser procesada para darle continuidad al negocio.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Contingencia Informática: Es un suceso fortuito que afecta el procesamiento automatizado de la información y suspende las actividades normales del negocio.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Costo: estos son tanto directos como indirectos, involucran un impacto positivo o negativo, esto se refiere a dinero, tiempo, trabajo, desorganización, renombre, políticas y pérdidas intangibles como imagen, confianza, credibilidad

Control: Medida que modifica el riesgo.

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.

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.

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

Frecuencia/Probabilidad: Es una medida sobre el porcentaje de ocurrencia de un evento expresado en número de ocurrencias o veces que se da un evento, también se define como el numero de veces que una amenaza deja de serlo para convertirse en realidad.

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.

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.

Información: Es el conjunto de datos que procesados e interpretados arrojan un resultado y con base en él se toman decisiones.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Infraestructura Tecnológica: son los componentes de hardware (servidores, computadores, cables de red entre otros. Software (básico, específico, corporativo o departamental). Bases de datos y aplicaciones que en forma conjunta e integrada procesan datos y producen resultados que generan información y con base en ella se toman decisiones.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

MSPI: Modelo de Seguridad y privacidad

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proyecto: Un proyecto puede concebirse como un conjunto de actividades

interdependientes, para viabilizar y poder materializar los objetivos de una organización en forma eficiente, una acción no repetitiva ni rutinaria orientada hacia

el logro de un objetivo específico y que se ejecuta con metas preestablecidas de calidad, costo y tiempo.

Proyecto de Tecnología de Información: Lo componen un conjunto de actividades interdependientes que se realizan en forma planeada, coordinada y controlada, donde se integran las personas, los procesos y la tecnología con el fin de dar una solución automatizada que a través de un sistema de información resuelvan una necesidad planteada por el usuario informático o la organización.

Prevenir Riesgos: Estrategia en la administración de riesgos consistente en actuar sobre las acciones y/o las condiciones inseguras, para disminuir la frecuencia de los siniestros.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Riesgo Informático: Es un suceso incierto que puede llegar a presentarse en un futuro con la probabilidad de Generar Consecuencias NEGATIVAS que afecten el ambiente informático o la información.

Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Siniestro: Todo evento accidental, súbito e imprevisto (repentino, no planeado), que normalmente genera consecuencias negativas sobre un sistema.

Seguro: Es un contrato en virtud del cual, un ASEGURADOR se compromete mediante el pago de una prima a pagar aun asegurado o beneficiario una indemnización, en caso de ocurrir un siniestro

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Severidad/Impacto: Es la evaluación del efecto y consecuencia del riesgo. Generalmente, la exposición riesgo se mide en aspectos económicos imagen de las personas o empresas, disminución de capacidad de respuesta y competitividad, interrupción de operaciones.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Transferir Riesgos: Estrategia en la administración de riesgos consistente en controlar las consecuencias económicas de los siniestros, mediante la transferencia parcial o total de las mismas a un tercero.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Tecnología de Información: Se define como el conjunto de procesos informáticos, gente especializada e infraestructura tecnológica necesaria y con un amplio grado de integración de sus componentes que maximizan la prestación de los servicios para satisfacer los requerimientos de la entidad.

Usuario Informático: persona que utiliza la infraestructura informática para acceder a la información y con base en ella tomar decisiones.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACION DEL RIESGO

Evaluar y reportar la evolución de las acciones y el riesgo, Ayudando en la definición de las acciones a tomar frente al riesgo del que son responsables cada uno de los miembros de la Alcaldía, (alcalde, secretarias, control interno, consultores, proveedores y Gobierno Digital).

Palacio municipal - Carrera 7 No. 20-21
Barrio Daniel Alfonso Paz
alcaldia@laapartada-cordoba.gov.co
Teléfono - 604 - 810 4319

Proveer los recursos necesarios para poder implementar las acciones dentro del proceso de gestión de riesgos.

Definir los criterios a nivel de los objetivos ayudando a evaluar los riesgos y las acciones planificadas al respecto.

Definir los diferentes roles en la gestión de riesgos y asignarlos a las personas implicadas, asumiendo responsabilidades en la ejecución y dirección de los recursos y presupuesto asignados a la gestión de riesgos.

ROL	RESPONSABLES
Elaboración	Consultores y Gobierno Digital
Revisión	Secretarias, Control Interno y Planeación
Aprobación	Alcalde
Divulgación y Ejecución	Gobierno Digital

6. POLITICA DE ADMINISTRACION DEL RIESGO

La Alcaldía Municipal de la Apartada, en su compromiso con la protección de datos, adoptará la política de seguridad y privacidad de la información, permitiendo que los servidores públicos de la entidad cumplan con los controles, procedimientos y directrices para la protección de los activos de información pertenecientes a la entidad.

Evitar el Riesgo: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo del activo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de archivos se retiran los permisos de acceso.

Prevenir el riesgo: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.

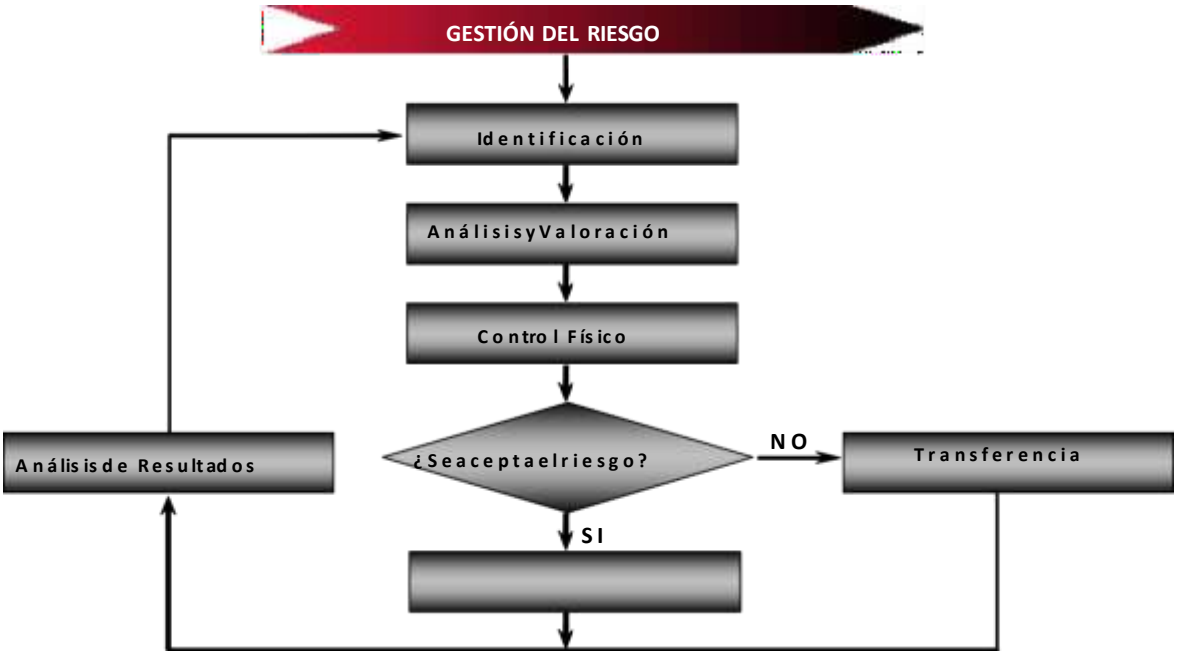
Reducir o mitigar el Riesgo: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo.

Dispersar el riesgo: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola

Palacio municipal - Carrera 7 No. 20-21
Barrio Daniel Alfonso Paz
alcaldia@laapartada-cordoba.gov.co
Teléfono - 604 - 810 4319

responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos.

Compartir el riesgo: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.



Procesos Vs. Tecnología de Información: el equipo de trabajo analizara cada recurso de la tecnología informática, evaluando el hardware, software, aplicaciones, comunicaciones, red, instalaciones físicas donde se encuentra ubicado o vaya a funcionar el proyecto a implantar.

7. ETAPAS PARA LA ADMINISTRACION DEL RIESGO

Se hace énfasis en las diferentes etapas a realizar de la gestión de riesgo.

Identificación: consiste en determinar las causas y efecto qué pueden tener impacto en los tipos de riesgos más probables, que afecten al proyecto de tecnología de información y las características de cada uno de los objetivos estratégicos, de proceso y/o áreas afectadas.

Análisis: se establecen los niveles de probabilidad e impacto del riesgo permitiendo la ubicación del mismo, (calificación, evaluación y respuesta). En los proyectos a realizar con la debida gestión de cada área del equipo de trabajo y gobierno digital.

Valoración: se hace la realización de asignación de controles y asignación del plan de contingencia.

Manejo: definir las acciones que serán aplicadas y los indicadores que permitirán medir el cumplimiento para tomar medidas correctivas cuando sea necesario en los proyectos de la Alcaldía.

Monitoreo: asegure que se lleven a cabo las acciones necesarias para evitar que el riesgo se materialice o impacte en el menor grado a la organización en caso de hacerse realidad.

8. DIMENSIONES DE SEGURIDAD

La Alcaldía la Apartada es responsable de la protección de la información que gestionan ante las amenazas de este entorno y deben, por todos los medios disponibles, garantizar su confidencialidad, integridad y disponibilidad, los riesgos que surgen relacionados con tecnologías y procesos, requieren sistemas, soluciones y servicios emergentes mediante las siguientes dimensiones.

Disponibilidad: asegurar que los usuarios autorizados tienen acceso cuando lo requieran en los tiempos adecuados.

Integridad: garantía de la exactitud y de que la información sea completa, así como los métodos de su procesamiento.

Confidencialidad: asegurar que la información es sólo accesible para aquellos autorizados.

Autenticidad de los usuarios del servicio: asegurar la identidad de los usuarios que manejan o acceden al activo.

Autenticidad del origen de los datos: asegurar la identidad u origen de los datos.

Trazabilidad del servicio: asegurar que en todo momento se podrá determinar quién hizo qué y en qué momento.

Trazabilidad de los datos: asegurar que en todo momento se podrá determinar quién ha accedido a los datos.

9. ANALISIS DE AMENAZAS

Para poder hacer el análisis y la valoración del riesgo es necesario elaborar las escalas de probabilidad y gravedad en que se pueden presentar las amenazas, de forma Natural, Social y Técnico en la Alcaldía la Apartada.

Las fases de la metodología a utilizar son las siguientes:

Definir alcance, Identificar los activos, Identificar amenazas, Identificar vulnerabilidades y salvaguardas, Evaluar el riesgo, Tratar el riesgo.

Definiendo la frecuencia o posibilidad de ocurrencia, en cuanto a la consecuencia o gravedad si se llegara a materializar la amenaza.

VALOR	PROBABILIDAD	DEFINICION
1	Improbable	Se presenta bajo circunstancias extremas de orden público en el país, de catástrofe o bajo situaciones excepcionales fuera del Alcance de la Alcaldía o del proyecto. Como paros, huelgas, sabotajes o amenazas de terrorismo.
2	Remoto	Se presenta por situaciones atribuibles a las personas, y pueden ser causadas por hechos internos de la organización hacia el proyecto como suspenderlo, no apoyarlo, abortarlo, entre otra.
3	Ocasional	El evento se clasifica como no rutinario y no es inherente a la tecnología, su frecuencia se asocia con variables externas a la tecnología, los procesos o componentes del proyecto.
4	Moderado	Se presenta por situaciones atribuibles al descuido o error humano que afectan la ejecución del proyecto.
5	Frecuente	Se presenta con cierta regularidad, y su causa es atribuible a los recursos mínimos del proyecto (Personas, presupuesto, tiempo, Tecnología) los cuales son necesarios para su ejecución.
6	Constante	Se presenta en el día a día, su origen es atribuible a situaciones normales del proyecto como interrupciones menores de los procesos, los servicios de la tecnología, la desviación de los Recursos y otros similares.

Para determinar los límites de cada una, de la aceptabilidad se utilizan los siguientes criterios de valoración.

Criterio	Valor
Crítico	= 5
Alto	= 3 y < 5
Medio	= 1 y < 3
Bajo	= 0 y < 1

10. AMENAZAS

Factor externo de riesgo, sistema expuesto vulnerable, representado por la potencial ocurrencia de un suceso de origen natural o generada por la actividad humana, que puede manifestarse en un sitio especifico y con una duración determinada, suficiente para producir efectos adversos en las personas, infraestructura, bienes Y servicios de la entidad clasificadas así:

Infraestructura: lugares donde se alberguen los sistemas de información y comunicaciones, en precarias condiciones afectando a los equipos, servidores y otros.

Hardware: soportes de ejecución de las aplicaciones informáticas, donde se generen daños, fugas o alteración de información, equipos portátiles o de escritorios, celulares, dispositivos, servidor de correo, bases de datos, aplicaciones, servidor Backup.

Software: gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios, se puede generar alteración, eliminación o divulgación de programas de producción de datos, manejo documental, programas de administración contable, sistemas operativos, aplicaciones ofimáticas, correos electrónicos, llamadas y fugas de información.

Redes: Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro, que pueden sufrir daños o alteración el servidor, router, switch, página web y equipos.

Organización: funciones alternadas o eliminadas a nivel jurídico, financieros, contables, archivos contractuales y de gestión, licencias, permisos y proyectos.

Personal: Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores, sean negligentes por falta de capacitación y tengan acceso no autorizado a sistemas de información y mal manejo de equipos.

11. IMPACTO POTENCIAL

En este sentido, es de suma importancia que el grupo de expertos analice, identifique y exponga las principales lecciones aprendidas utilizando el análisis de información, entrevistas u otras herramientas utilizando los siguientes factores.

Probabilidad: Raro, Improbable, posible, probable, casi seguro

Impacto: Insignificante, menor, moderado, mayor, Catastrófico.

12. EVALUACION DEL RIESGO

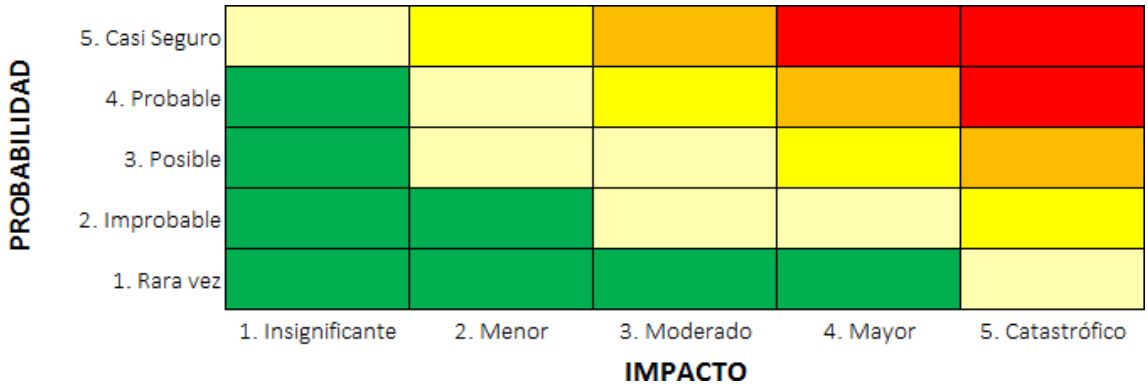
Una vez que los riesgos han sido identificados y evaluados, los pasos subsiguientes para prevenir que ellos ocurran, protegerse contra ellos o mitigar sus consecuencias son mucho más programáticos.

Una vez analizada la probabilidad, impacto, y efecto de todos los riesgos conocidos que pueden afectar el proyecto, como también las acciones correctivas que deben llevarse a cabo en caso que el riesgo llegara efectivamente a ocurrir.

DESCRIPCION	CRITERIO DE ACEPTABILIDAD
Aceptable	25%
Tolerable	0%
Inaceptable	25%
Inadmisible	50%

13. VALORACION DE LOS RIESGOS

Se considera la probabilidad de que la amenaza identificada explote la vulnerabilidad y el impacto resultante sobre el activo evaluado, determina el Riesgo Total interpretado en las siguientes zonas de riesgo de acuerdo con el siguiente Mapa de Calor.



14. IDENTIFICACION DE CONTROLES

Esta fase consiste en identificar y analizar las soluciones disponibles para tratar los riesgos estudiados en las etapas anteriores, con el fin de reducir la frecuencia y severidad de las pérdidas, en caso de que los riesgos identificados se materialicen. y documentar las características de cada uno de los objetivos estratégicos, de proceso y/o áreas afectadas.

Las más importantes herramientas usadas en la identificación de riesgos incluyen: registros internos de la organización, listas de chequeo. Cuestionarios de análisis de riesgos, flujos de procesos, análisis financiero, inspecciones, entrevistas, tormenta de ideas, entre otras.

Aproximación de combinación, todas las herramientas de identificación de riesgos están hechas para tolerar problemas. Cada herramienta puede resolver una parte del problema. Por ejemplo: las entrevistas y los cuestionarios y hacer análisis cruzados de ambos instrumentos, con el fin de disminuir la subjetividad en el análisis.

La gestión de Riesgos es una responsabilidad de todos los integrantes del Proyecto.

El análisis y gestión de los riesgos del Proyecto es una acción continua y dinámica.

15. MANEJO DE RIESGOS

Plan de acción propuesto por el grupo de trabajo, cuya evaluación beneficio costo resulta positivo y es aprobado por el alcalde.

15.1. Controles de clase técnica

Nos permite gestionar y asegurar operativamente, los accesos, manipulación a los sistemas operativos software, hardware, manejo de la información, accesos a la plataforma, implementación del sistema de gestión y mitigación del riesgo.

15.2. Controles de clase documental

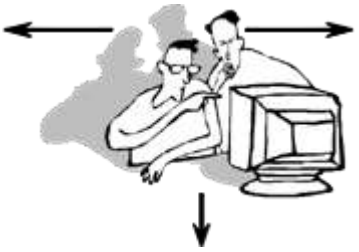
Los controles nos contribuyen un funcionamiento con instructivos y reglamentos, si no se aplican correctamente, generamos fallas en el sistema de gestión de seguridad.

15.3. Implementar programas de capacitación y sensibilización

Realizar adecuadamente las respectivas capacitaciones y sensibilizaciones, depende en gran parte el éxito de la implementación del sistema. Al aplicar algunos controles se deberá realizar el debido seguimiento para verificar y cuantificar la funcionalidad del mismo, sin embargo, esto no aplica para todos los controles.

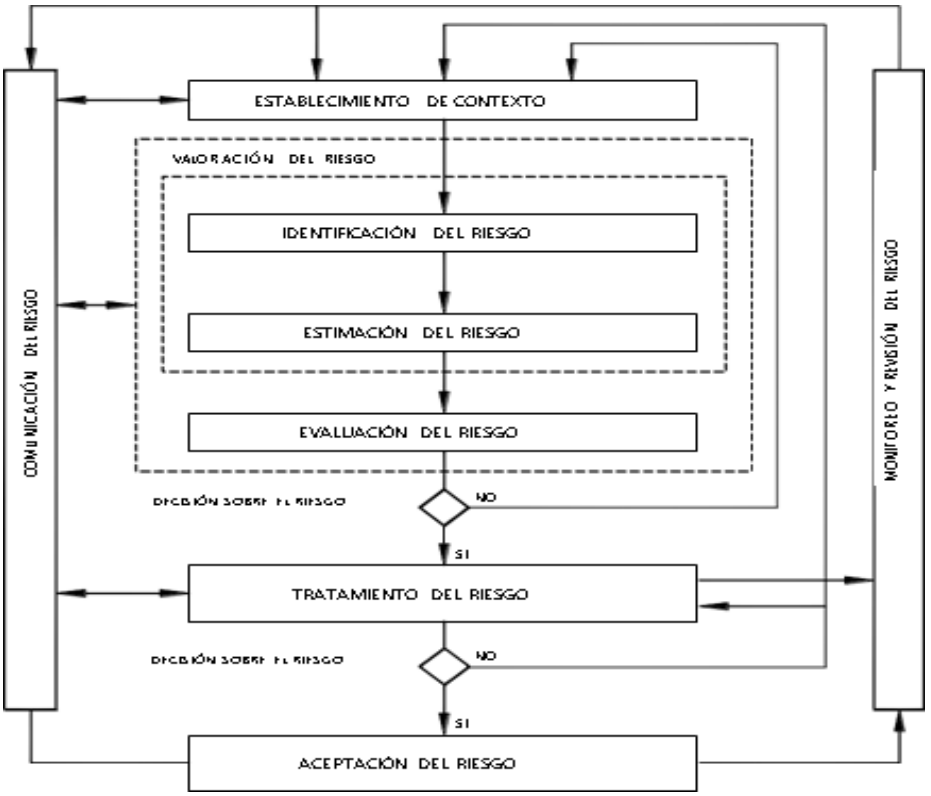
15.4. Implementación de procedimiento de manejo de incidentes de seguridad

Este suceso puede ser llevado a cabo a voluntad o accidental. Dependiendo de la gravedad de la situación este puede afectar el funcionamiento normal de la organización. Por lo general el manejo del incidente implica que este se debe solucionar en el menor tiempo posible para evitar una afectación mayor y se debe buscar documentar.



Identificar las características generales de las personas involucradas en el proyecto, así como las percepciones, motivaciones y sugerencias que tiene frente a la administración de los riesgos.

DESARROLLO METODOLOGICO



16. SEGUIMIENTO DE RIESGO

La Alcaldía Municipal la Apartada “evaluará el desempeño del modelo del plan de tratamiento de riegos de seguridad y privacidad de la información”, por medio de un monitoreo esencial para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

17. EQUIPO DE TRABAJO

Para realizar este tipo de proyectos es necesario conformar un equipo de trabajo interdisciplinario entre la Dirección de Informática y las secretarias con el apoyo puntual de las áreas que se requieran y deban participar en el análisis y valoración de riesgos, utilizando mecanismos de integración, comunicación y coordinación teniendo en cuenta lo siguiente.

Conformar el equipo de trabajo con roles y responsabilidades definidas.

Conformar el Comité directivo del proyecto con roles y responsabilidades definidas que ayuden a dirimir conflictos, a tomar decisiones y a apoyar el proyecto.

Divulgar la metodología utilizada para hacer el análisis y valoración de riesgos en proyectos de tecnología de información a los participantes por parte de la Dirección de Informática.

Analizar los ajustes y mejoras requeridas en la metodología de acuerdo con los cambios que hayan surgido en los sistemas de información y los ambientes tecnológicos.

Recolectar la información necesaria relacionada con las actividades de la metodología teniendo en cuenta los controles que se implementan y buscan mejorar el escenario del riesgo y disminuir su impacto.

Aplicar la metodología teniendo en cuenta los ajustes y mejoras que hayan sido requeridas y que fueron el resultado del análisis de la misma.

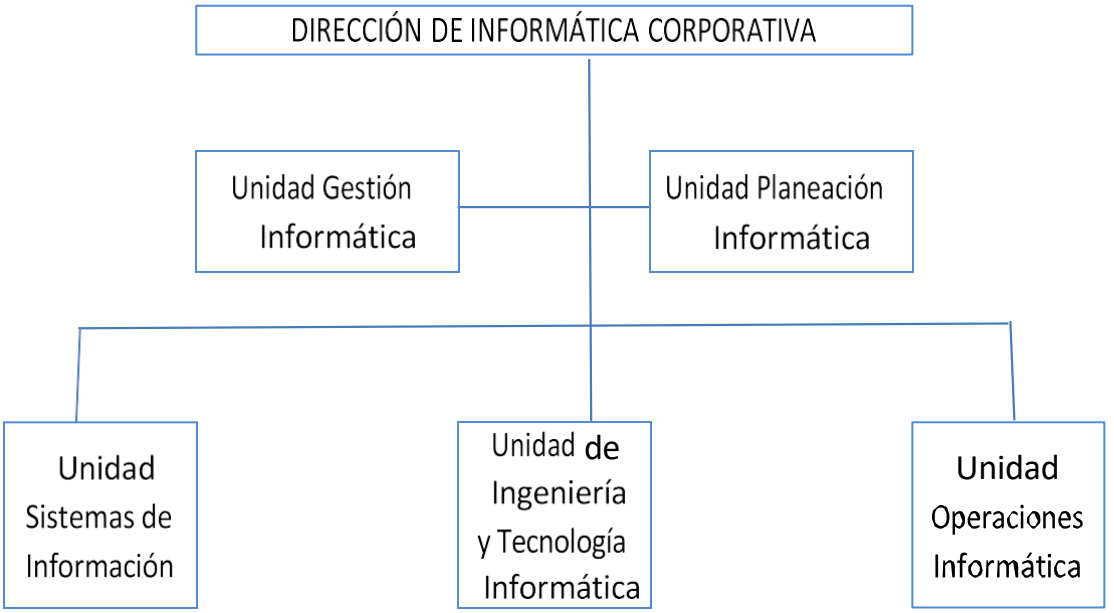
Efectuar reuniones periódicas con los diferentes miembros del equipo de trabajo, para conocer el estado de avance del análisis y valoración.

Analizar la información y validar los resultados obtenidos de acuerdo con la metodología aplicada.

Estructurar el informe final del análisis y valoración de los riegos.

GOBIERNO DIGITAL

Es el área encargada de promover y liderar la planeación y el desarrollo coherente e integrado de la informática en la Alcaldía la Apartada para garantizar una estrategia informática alineada con la visión corporativa.



17.1. UNIDAD PLANEACIÓN INFORMÁTICA

Su función es elaborar y mantener actualizada la estrategia informática, en cuanto a aplicaciones, tecnologías y organización con sus correspondientes planes estratégicos y tácticos, para garantizar un desarrollo integrado de la información en la entidad.

17.2. UNIDAD GESTIÓN INFORMÁTICA

Su función es asesorar y trabajar en equipo con las unidades de la Dirección Informática y con las demás secretarias, en la ejecución y el mejoramiento de sus planes, para garantizarla coherencia de la gestión informática de todas las unidades, ofrece apoyo ofrece apoyo en lo referente al mejoramiento de los productos y servicios, medición de la calidad del servicio, asesoría y adquisición de infraestructura informática.

17.3. UNIDAD INGENIERÍA Y TECNOLOGÍA INFORMÁTICA

Su función es coordinar la planeación informática, las necesidades de ingeniería, tecnología y la infraestructura informática para proveer asesoría especializada a toda la organización.

Presta soporte especializado en los temas de seguridad informática, viabilidad técnica para adquisición de tecnología y compatibilidad con la infraestructura que posee y requiere la Metodología para el Análisis y Valoración de Riesgos en Proyectos.

17.4 UNIDAD OPERACIONES INFORMÁTICA

Su función es coordinar la instalación, soporte, operación y mantenimiento de todos los equipos informáticos, servidores, redes y aplicaciones para garantizarle a la corporación la disponibilidad de la infraestructura tecnológica.

18. PENSAMIENTO ESTRATÉGICO

Para entender la Dirección Informática Corporativa en lo relacionado con la infraestructura de TI.

18.1. ESTRATEGIA

Retener y Potenciar el liderazgo en servicios de TI en la Administración Municipal.

Ser los líderes de la planeación, la evolución y el soporte de los paquetes corporativos

Obtener sinergias en TI entre la Alcaldía la Apartada y sus Proveedores.

ACTIVIDADES A DESARROLLAR

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
Establecer un plan de actualización de hardware y software.	Realizar diagnóstico de la Situación actual del Hardware y Software y establecer un cronograma de cambio para no permitir la obsolescencia en un alto grado.	Dirección de Sistemas
Establecer mecanismos robustos para las copias de seguridad.	Establecer mecanismos claros y tallados de las copias de seguridad, que permitan una realización más eficiente y segura de estas	Dirección de Sistemas
Implementar planta de energía y energía regulada	Implementar planta de energía en la entidad y energía regulada en cada una de las estaciones de trabajo.	Dirección de Sistemas
Establecer políticas de seguridad y privacidad de la información	Implementar lineamientos claros en materia de seguridad y privacidad de la información para todos los empleados, contratistas, proveedores y todos los que tienen algún vínculo con la entidad.	Dirección de Sistemas
Implementar plan de Recuperación ante Desastres (DRP)	Implementar plan de recuperación ante desastres o DRP el cual contenga de manera detallada para proceder ante una eventualidad.	Dirección de Sistemas

19. OPORTUNIDAD DE MEJORA

La Alcaldía la Apartada, no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

20. RECURSOS

La Alcaldía la Apartada, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital, dispone de los siguientes recursos.

RECURSOS	VARIABLES
Humanos	La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI) , ISO 27005, Magerit
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos para los controles producto de la gestión de riesgos

21. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento, como la gestión de sus recursos dentro de la planificación de los mismos.