INSTITUTO MUNICIPAL PARA LA RECREACION Y DEPORTE (IMRD)

MUNICIPIO SAN JOSÉ DE CUCUTA
NORTE DE SANTANDER - COLOMBIA
2022

INTRODUCCION

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan todo el ciclo de vida del servicio. Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad del negocio o institución. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en La Instituto Municipal Para la Recreación y Deporte. Antes de iniciar con este plan de gestión se ha revisado el documento con el diagnóstico del sistema actual del Instituto, donde se conoce la situación actual de la organización y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información. El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos para tener como reducir la ocurrencia de un evento no deseado (**probabilidad**) y sus consecuencias (**impacto**).

Contenido

1. Objetivos 5
1.1 Objetivo General 5
1.2 Objetivos Específicos 5
2. ALCANCES Y LIMITACIONES 6
2.1 ALCANCES 6
2.2 LIMITACIONES 7
3. GESTIÓN DE RIESGOS 7
3.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS 7
3.2 DEFINICION GESTIÓN DEL RIESGO DE SEGURIDAD EN LA INFORMACIÓN 8
3.4 IDENTIFICACIÓN DEL RIESGO 10
3.4.1. Riesgo Estratégico: 10
3.4.2. Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte 10
3.4.3. Riesgos Operativos: 10
3.4.2. Riesgos Financieros: 10
3.4.5. Riesgos de Cumplimiento: 10
3.4.6. Riesgos de Tecnología: 10
3.5 SITUACION NO DESEADA 11
4. ORIGEN DEL PLAN DE GESTION 11
4.1 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN 12
4.2 IDENTIFICACIÓN DEL RIESGO 12
5. ANALISIS DE VULNERABILIDADES 13
5.1 DESCRIPCIÓN DE VULNERABILIDADES 13
5.2 MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO 16

6. PROPUESTA DE SEGURIDAD 20

6.1 PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD 20

6.2 PLAN DE CONTINUIDAD DEL NEGOCIO 21

6.3 IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN 22

6.4 PLAN DE CAPACITACIÓN 22

1. Objetivos

1.1 Objetivo General

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en el IMRD

1.2 Objetivos Específicos

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos a proteger en el IMRD.
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

- Lograr el compromiso del IMRD para emprender la implementación del plan de gestión del riesgo en la seguridad de la información para que logremos detectar y responder de forma eficaz las brechas e intrusiones de seguridad informática, los ataques de malware, los ataques de phishing y el robo de datos, tanto dentro como fuera de la red.

- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

- Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

2.2 LIMITACIONES

- Falta de presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en el IMRD.

3. GESTIÓN DE RIESGOS

3.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo. EL IMRD, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015. Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información. Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad. Considerando la situación actual del IMRD reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

La norma ISO 27005:2011 es un estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información. Contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera. Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo mediante el plan de tratamiento de riesgos. El no contar con una buena gestión de la seguridad de la información, para el IMRD puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

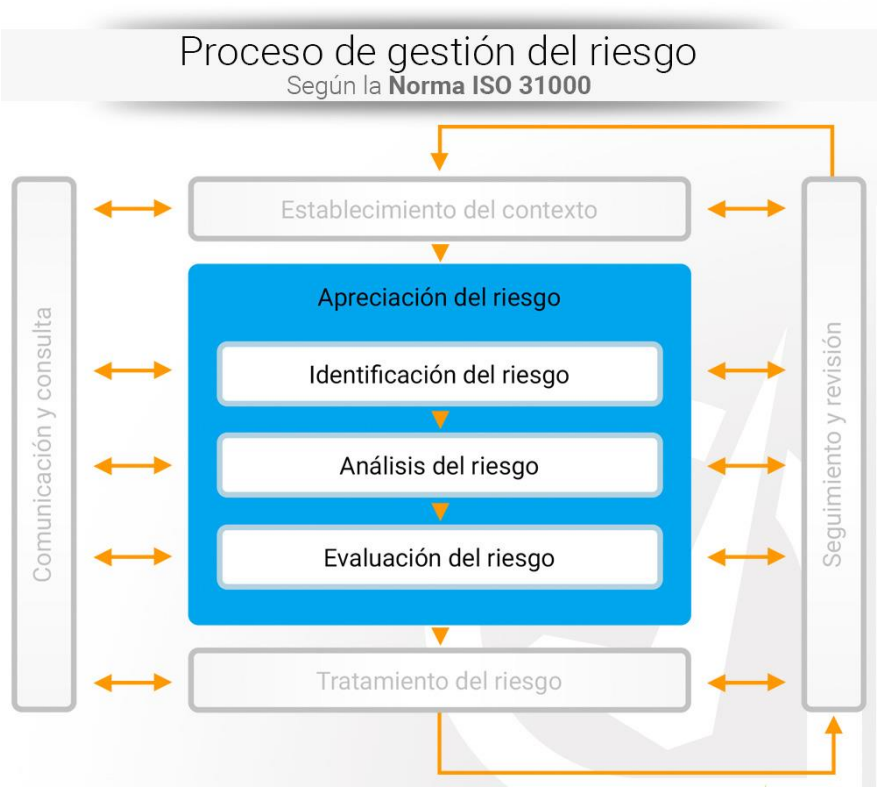
3.2 DEFINICION GESTIÓN DEL RIESGO DE SEGURIDAD EN LA INFORMACIÓN

La gestión de riesgos de seguridad de la información es el proceso de identificar, comprender, evaluar y mitigar los riesgos –y sus vulnerabilidades subyacentes– y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones. Además de identificar los riesgos y las medidas de mitigación de riesgos y las medidas de mitigación del riesgo, un método y proceso de gestión del riesgo ayudará

- Identificar los activos críticos de información. Un programa de gestión de riesgos puede ampliarse para identificar también a personas críticas, procesos de negocio y tecnología.
- Comprender por qué los activos críticos escogidos son necesarios para las operaciones, la realización de la misión y la continuidad de las operaciones.

Para cumplir con la gestión de riesgos como componente de preparación para la ciberseguridad, una organización debe crear un sólido programa de evaluación y gestión del riesgo de la seguridad de la información. Si ya existe un programa de gestión del riesgo empresarial (ERM), un programa de gestión de riesgos de seguridad de la información puede soportar el proceso de ERM.

3.3 VISION GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN



Controlar el riesgo.- Fortalecer los controles existentes y/o agregar nuevos controles.

.

3.4 IDENTIFICACIÓN DEL RIESGO

3.4.1. Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

3.4.2. Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

3.4.3. Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

3.4.2. Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

3.4.5. Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

3.4.6. Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

3.5 SITUACION NO DESEADA

- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales.
- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de internet.
- Daño de equipos y de información.
- Atrasos en la entrega de información.
- Atrasos en asistencia técnica
- Fuga de información
- Manipulación indebida de información**.**
- Fallas en la red.

4. ORIGEN DEL PLAN DE GESTION

Debido a que el IMRD no tiene un área de sistemas conformada y se evidenció que no existen procesos asignados a dicha área entre otras vulnerabilidades nos encontramos en el nivel 1 de MPSI, es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad la información.

La situación actual del sistema de seguridad de la información en la entidad se encuentra planteado en el Diagnostico de seguridad y privacidad de la Información con fecha de Diciembre de 2018. El Gobierno Nacional y el Ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las alcaldías y

entidades públicas en el país. Es por ello necesario que el IMRD cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población.

4.1 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

4.2 IDENTIFICACIÓN DEL RIESGO

Proceso → Objetivo del Proceso → Identificación de Activos → Riesgo

↓

Causas (Amenazas y Vulnerabilidades).

↓

Descripción del Riesgo.

↓

Efectos de la materialización del Riesgo.

5.

ANALISIS DE VULNERABILIDADES

5.1 DESCRIPCIÓN DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en el IMRD se encontraron otras amenazas e impactos como los siguientes:

1. La red de internet implementada no es la más adecuada teniendo en cuenta que la mayor parte del IMRD tiene conexión WiFi. Debido a que la infraestructura física es amplia, compleja y la señal debe atravesar paredes por ello conlleva la perdida de señal afecta de forma directa los tiempos de producción laboral y desempeño de las funciones.

2. Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.

3. Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas

básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

- En algunas oficinas del IMRD no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.

- No existe Datacenter de la entidad por lo cual se requiere de algunas características importantes para cumplir con las normas de funcionamiento (alimentación eléctrica estabilizada e ininterrumpida, sistemas contra incendios, control de acceso, extintores, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad, piso falso entre otros).

- No existen cuentas de usuario y claves para el acceso de los recursos informáticos, en equipos compartidos.

- La información es llevada en memorias o discos duros portátiles personales, por ende la información sale de la entidad.

- No hay control para el uso de memorias portátiles en los equipos del IMRD, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

- Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en el IMRD.

- No existe un Firewall para la red inalámbrica del IMRD.

- El sistema ofimático Microsoft Office que se utiliza en el IMRD no cuenta con algunas licencias de funcionamiento. en este caso la entidad está incumpliendo la Ley 603 de 2000.

- No existe un área de sistemas con personal encargado de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad de la información para el IMRD.

- No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la entidad.

- Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

- No existen procesos de copias de seguridad establecidos. Ésta solución no es óptima, ya que existe riesgo de pérdida total de información en caso de ocurrir desastres naturales, incendios u otros que afecten las copias de respaldo almacenadas ubicado dentro de la misma entidad.

- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones del IMRD. (en caso de incendio o desastre natural existen altas probabilidades de perder la información)

- No se cuentan con los tipos de extintores adecuados para cada emergencia.

5.2 MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO

				ANALISIS		VALORACION		VIGENCIA DE CUMPLIMIENTO
VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACION	CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	
*Fallas eléctricas	Las conexiones no son suficientes, no cumplen con las exigencias el tamaño de la red de equipos de cómputo (cables sueltos, inadecuada estructura y adecuación)	Inadecuada conexión de cableado eléctrico	Posible pérdida de información	*Riesgo tecnológico *Riesgo físico *Riesgo humano	40	Riesgo moderado	Plantear un nuevo diseño de la red eléctrica	Vigencia 2022
*Afectación de activos de información y activos informáticos.	Desconocimiento de las políticas y normas de seguridad de la información.	No socialización No capacitación de las políticas y normas de seguridad.	Acciones no adecuadas en el tratamiento de los activos de información e informáticos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información * Riesgo en personal	60	Riesgo Alto	Socializar e implementar el Manual de políticas y normas de seguridad de la información en la alcaldía municipal.	Vigencia 2022
*Pérdida de información *Pérdida de tiempo productivo en funciones laborales.	La red implementada no es la más adecuada para la estructura física de la alcaldía y la cantidad de equipos informáticos. Las fallas en la señal de internet son constantes.	Señal inalámbrica	Señal débil en las oficinas. Retraso en tiempos de producción para los funcionarios.	*Riesgo Tecnológico *Riesgo en Servicio *Riesgo de información	40	Riesgo Importante	Implantar un modelo de red basado en cableado estructurado.	Vigencia 2022

				ANALISIS		VALORACION		VIGENCIA DE CUMPLIMIENTO
VULNERABILIDAD	**DESCRIPCIÓN**	**CAUSA**	**EFECTO**	**CLASIFICACION**	**CALIFICACION**	**EVALUACION**	**MITIGACION DEL RIESGO**	
Incumplimiento de las actividades de seguridad de la información.	El personal encargado de los sistemas no es suficiente. No se están siguiendo protocolos y normas para garantizar la seguridad de la información en la entidad.	No existe personal encargado del proceso de aseguramiento de la información	Ausencia de transferencia de conocimiento y falta de capacitación	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	60	Riesgo Alto	Encargar a personal capacitado para el aseguramiento de la información. Capacitar al personal de la alcaldía municipal para el cumplimiento de procesos y actividades de seguridad de la información	Vigencia 2022
Confidencialidad e Integridad de la información	En la entidad se trabaja en la campaña cero papel, sin embargo se han encontrado dentro del papel reutilizable información personal de algunos pobladores del municipio beneficiarios de programas sociales.	Exposición de datos personales en papel reutilizable.	incumplimiento de confidencialidad e integridad de la información	*riesgo de Información	60	Riesgo Alto	Socializar con los funcionarios de la entidad acerca de las políticas de seguridad y confidencialidad de la información.	Vigencia 2022
Pérdida total de Información	No se cuentan con los tipos de extintores adecuados para cada necesidad.	No se cuentan con los tipos de extintores adecuados para cada necesidad.	*No hay extintores	*Riesgo de información. *Riesgo tecnológico	60	Riesgo Alto	Adquirir los extintores necesarios.	Vigencia 2022

			ANALISIS		VALORACION		VIGENCIA DE CUMPLIMIENTO
VULNERABILIDAD	**CAUSA**	**EFECTO**	**CLASIFICACION**	**CALIFICACION**	**EVALUACION**	**MITIGACION DEL RIESGO**	
*Pérdida de Información	No se hace el debido resguardo de copias de seguridad . No existen cuentas de usuario. No hay control de uso	Posible pérdida de información Infección por Virus	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	40	Riesgo Importante	*Crear un instructivo de copias de seguridad *Capacitar al personal IMRD para el dominio de este tema. *Adquirir un servidor para almacenar las copias de seguridad e información. *Adquisición de una nube para almacenamiento de información. *Crear cuentas de usuario con claves.	Vigencia 2022
*Perdida de información	Incendios, ingreso de personal no autorizado, posible robo de equipos, Daño discos solidos.	Perdida de información por catástrofe o riesgo en manos	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	40	Riesgo Moderado	Adecuación del Datacenter del IMRD, cumpliendo con las características exigidas por normas y estándares en Colombia. (Piso falso, cámara de seguridad, extintores adecuados, entre otros)	Vigencia 2022

			ANALISIS		VALORACION		VIGENCIA DE CUMPLIMIENTO
VULNERABILIDAD	**CAUSA**	**EFECTO**	**CLASIFICACION**	**CALIFICACION**	**EVALUACION**	**MITIGACION DEL RIESGO**	
*Pérdida de información y/o deterioro físico	No se ha iniciado el manejo adecuado de los documentos físicos están siendo archivados en sitios no adecuados para ello.	Daño de documentos y Digitalización de la información.	Riesgo de la información con el deterioro del papel.	40	Riesgo importante	Iniciar la ejecución de la digitalización y Almacenamiento de la información contenida en papel.	Vigencia 2022
No hay respaldo de información en sistemas de información	No hay procesos de copias de seguridad establecidos	Perdida de información	*Riesgo Tecnológico *Riesgo de información	60	Riesgo Importante	*Crear procesos de copias de seguridad. *Invertir en un software o sistema de información para el almacenamiento y consulta de la documentación física existente en el IMRD	Vigencia 2022

6. PROPUESTA DE SEGURIDAD

- Se debe cambiar la red inalámbrica actual por cableado estructurado, para minimizar el problema de conexiones demoradas y caídas de señal.
- Implementar un firewall para la red que se utiliza en el IMRD.
- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Replantear y Socializar las políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- Revisar las políticas existentes proyectadas para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.
- Socializar las políticas de seguridad y privacidad de la información con el personal del IMRD.
- Creación de cuentas de usuario y claves para tratar de mitigar los riesgos de pérdida de información en manos de otro funcionario que use el equipo compartido.
- El personal de sistemas puede crear las cuentas y claves, socializando al personal del IMRD a la creación de claves en forma correcta.
- Crear un rubro del presupuesto para la adquisición de la licencia del sistema ofimático Office para los equipos del IMRD.
- En caso de usar Software libre como Libreoffice se debe capacitar al personal en el manejo del sistema ofimático
- Implementar el sistema de documentación digital en el IMRD para reducir riesgos de pérdida de información física.

6.1 PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

- Adquirir un servidor con características específicas para el almacenamiento de copias de seguridad de la información local manejada en las diferentes dependencias.

- Obtener una nube dedicada para la información del IMRD con el fin de tener un respaldo.

- Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves. Nunca se debe olvidar que la realidad es que el Instituto puede sufrir un incidente que afecte su continuidad y, dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Una de las principales características que debe poseer la entidad es buscar cómo establecer un Sistema de seguridad

enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

6.2 PLAN DE CONTINUIDAD DEL NEGOCIO

- Diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar la auditorías periódicas al con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.

- Socializar con los directivos y depemdemcias o la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.

- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

  1) Detectar el riesgo

  2) Plantear controles y efectuar las implementaciones respectivas.

  3) Mitigar el riesgo.

- Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:

  1) Política de copia de seguridad de datos

  2) Procedimientos de almacenamiento fuera de la alcaldía

  3) Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones

6.3 IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permitió identificar que se desconocen y poco se cumplen las políticas de seguridad; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

- Socialización y capacitación de temas de seguridad.
- Ambiente con la seguridad física adecuada.
- Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

6.4 PLAN DE CAPACITACIÓN

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

1) Detectar los requerimientos tecnológicos.

2) Determinar objetivos de capacitación para personal.

3) Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.

4) Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.

5) Evaluar los resultados de cada actividad.