PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020 - 2023

RIONEGRO
juntos avanzamos más

Secretaría de Gestión Humana y Desarrollo Organizacional
Subsecretaría de TIC

Carolina Tejada Marín
Secretaria de Gestión Humana y Desarrollo Organizacional

Héctor Fabio Orjuela Pérez
Subsecretario de TIC

Wilson Libardo López
Profesional Universitario

Deivis Carrillo Castillo
Profesional Universitario

Juan Sebastian Abril
Profesional Universitario

David Machado Montoya
Profesional Universitario

Colaboradores contratistas
Bladimir Villada, Dairo Ayala, Fabián Arbeláez, Jonathan Muñoz, Juan Pablo Martínez, Jurani Marín.

Texto elaborado por:

Juan Abril, Deivis Carrillo
Héctor Fabio Orjuela Pérez

CONTENIDO

1. INTRODUCCIÓN 5
2. GLOSARIO 6
3. OBJETIVOS 8
   3.1. Objetivo General 8
   3.2. Objetivos específicos 8
4. ALCANCE 9
5. PLAN DE TRATAMIENTO DE RIESGOS 10
   5.1. ORGANIZACIÓN DE ROLES Y RESPONSABILIDADES 10
      5.1.1. Comité Institucional de Gestión y Desempeño 10
      5.1.2. Subsecretaría de TIC 10
      5.1.3. Grupo de Gestión de TI 10
      5.1.4. Otros grupos o responsables 10
6. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS 12
   6.1. Riesgos Internos 12
   6.2. Riesgos Externos 13
7. ANÁLISIS Y CLASIFICACIÓN DE LOS RIESGOS 15
8. APLICACIÓN DE CONTROLES 17
9. ACTIVIDADES DEL PLAN SEGÚN EL RIESGO 21
   9.1. R1 - Pérdida de la confidencialidad, disponibilidad o integridad de información almacenada en aplicativos críticos 21
      9.1.1. Gestión del riesgo residual 21
      9.1.2. Procedimiento de respuesta tras la materialización del riesgo: 21
   9.2. R2 - Indisponibilidad de aplicativo crítico 22
      9.2.1. Gestión del riesgo residual 22
      9.2.2. Procedimiento de respuesta tras la materialización del riesgo: 22
   9.3. R3 - Falla técnica en servidor virtual 23
      9.3.1. Gestión del riesgo residual 23
      9.3.2. Procedimiento de respuesta tras la materialización del riesgo: 23
   9.4. R4 - Falla técnica en servidor físico 24
      9.4.1. Gestión del riesgo residual 24

9.4.2. Procedimiento de respuesta tras la materialización del riesgo: 24
9.5. R5 - Falla técnica en un equipo de comunicaciones de la entidad..... 25
9.5.1. Gestión del riesgo residual 25
9.5.2. Procedimiento de respuesta tras la materialización del riesgo: 25
9.6. R6 - Falla de base de datos 26
9.6.1. Gestión del riesgo residual 26
9.6.2. Procedimiento de respuesta tras la materialización del riesgo: 26
9.7. R8 - Ausencia de personal del Grupo de Gestión de TIC durante la materialización del riesgo. 27
9.7.1. Gestión del riesgo residual 27
9.7.2. Procedimiento de respuesta tras la materialización del riesgo: 27
9.8. R9 - Documentación de la infraestructura de TI incompleta..... 28
9.8.1. Gestión del riesgo residual 28
9.8.2. Procedimiento de respuesta tras la materialización del riesgo: 28
9.9. R10 - Interrupción del suministro eléctrico por más de 15 minutos..... 28
9.9.1. Gestión del riesgo residual 29
9.9.2. Procedimiento de respuesta tras la materialización del riesgo: 29
9.10. R12 - Indisponibilidad del servicio telefónico 29
9.10.1. Gestión del riesgo residual..... 29
9.10.2. Procedimiento de respuesta tras la materialización del riesgo:..... 30
9.11. R13 - Interrupción del servicio por ataque informático..... 30
9.11.1. Gestión del riesgo residual..... 30
9.11.2. Procedimiento de respuesta tras la materialización del riesgo:..... 31
9.12. R14 - Interrupción de servicios por sismo o incendio..... 31
9.12.1. Gestión del riesgo residual..... 32
9.12.2. Procedimiento de respuesta tras la materialización del riesgo:..... 32
9.13. 15 - Resolución DNS inadecuada 33
9.13.1. Gestión del riesgo residual..... 33
9.13.2. Procedimiento de respuesta tras la materialización del riesgo:..... 33
10. PLAN DE PRUEBAS..... 35
11. REVISIÓN, MANTENIMIENTO Y ACTUALIZACIÓN DE ESTE PLAN..... 36
12. CONTROL DE CAMBIOS..... 36

1. INTRODUCCIÓN

El Municipio de Rionegro reconoce la información como un activo valioso y a medida que los sistemas de información apoyan cada vez más sus procesos misionales, se hace necesaria la ejecución de planes, programas y proyectos que garanticen la integridad, confidencialidad y disponibilidad de la misma.

Debido a que la infraestructura de TI continuamente se encuentra expuesta a diferentes tipos de riesgos que podrían ocasionar pérdida o indisponibilidad de los sistemas de información, la Subsecretaría de TIC de la Alcaldía de Rionegro se encuentra comprometida con este plan, con el fin de definir estrategias para responder de forma adecuada ante un evento, previniendo la materialización de riesgos, recuperando y/o restaurando los servicios informáticos en el menor tiempo posible reduciendo el impacto sobre los procesos críticos de la Administración Municipal.

El plan de tratamiento de riesgos de seguridad y privacidad de la información que se presenta a continuación incluye una guía no restrictiva del uso de recursos físicos y humanos para responder de manera eficaz y eficiente ante la materialización de un riesgo en la infraestructura de TI y tiene como propósito garantizar la continuidad de la prestación de los servicios informáticos, minimizando las pérdidas consecuentes del evento.

2. GLOSARIO

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados. (ISO 27001)

Contingencia: Es algo probable que ocurra en un sistema de información o en un servicio tecnológico, aunque no se tiene una certeza al respecto.

Disponibilidad: Es asegurar que la infraestructura, los procesos, las herramientas y las funciones de TI estén adecuados para cumplir con los objetivos del negocio y los niveles de servicio propuestos.

Evento: Es un suceso detectable e importante que ocurre en la infraestructura tecnológica y que puede afectar la prestación del servicio en la organización.

Frecuencia del evento: puede ser (nunca, aleatoria, periódico y continuo).

Impacto: Es la afectación a nivel organizacional (número de usuarios afectados, áreas que no pueden operar, proceso de negocio afectados, etc) después de ocurrido un evento. Puede ser (leve, moderado, grave y muy severo).

Integridad: propiedad de exactitud y completitud. (ISO 27000)

Plan de continuidad: Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Riesgo: es la identificación, evaluación, medición y reporte de amenazas y oportunidades que afectan la continuidad del negocio. Existen distintos tipos de riesgo:

> **Riesgos naturales:** Es la probabilidad que ocurra un evento natural como una inundación, un terremoto, lluvias, derrumbes, etc.
>
> **Riesgos sociales:** Es la posibilidad de que ocurra un ataque terrorista, un desorden público, etc.
>
> **Riesgos tecnológicos:** Es la probabilidad de que ocurra un daño o una pérdida debido a eventos asociados con el almacenamiento, producción, transformación o transporte de sustancias y/o residuos químicos peligrosos, radiactivos, biológicos, líquidos inflamables, materiales combustibles, electricidad y/o hidrocarburos, así como con las actividades que operen altas presiones, altas temperaturas o con posibilidades de impacto mecánico.

MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable: Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

RPO (Recovery Point Objective) o Punto de Recuperación Objetivo: Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.

RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo: Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

WRT (Work Recovery Time) o Tiempo del Trabajo de Recuperación: Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo.

Seguridad de la información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Sistemas críticos: Son sistemas de información en donde un fallo puede ocasionar pérdidas económicas significativas los cuales soportan los procesos misionales de la entidad.

Troncal SIP: Canal de comunicaciones telefónicas que se establece entre la entidad y el proveedor a través del canal de fibra óptica que también provee internet.

UTM (*Unified Threat Management*): Sistema unificado de gestión de riesgos en la red de computadores.

VM (Virtual Machine) o Máquina Virtual: Software que permite emular el funcionamiento de servidores utilizando los recursos de un servidor físico.

3. OBJETIVOS

3.1. Objetivo General

Identificar y establecer un plan para el tratamiento de riesgos de seguridad y privacidad de la información con el fin de prevenir la materialización de riesgos y reestablecer de forma eficiente y eficaz la prestación de servicios de TI en el Municipio de Rionegro tras la ocurrencia de eventos que puedan alterar el normal funcionamiento de los sistemas críticos de información.

3.2. Objetivos específicos

- Identificar, analizar y valorar los riesgos a los que están expuestos los sistemas de información críticos.
- Planear acciones de mitigación de riesgos.
- Establecer roles y responsabilidades del personal interno y externo para intervenir en los planes de recuperación de los sistemas de información.
- Preparar los recursos necesarios para el restablecimiento de servicios de TI.
- Reestablecer los servicios de TI en el Municipio de Rionegro en el menor tiempo posible a partir de la materialización de un riesgo.
- Minimizar las pérdidas financieras y operativas derivadas de la ocurrencia de un fallo en la infraestructura de TI, previendo procedimientos efectivos y eficientes de recuperación.

4. ALCANCE

En este plan se identifican los riegos potenciales a los que están expuestos los sistemas de información críticos del Municipio de Rionegro y se indican las funciones, procedimientos y recursos necesarios para reanudar y restaurar las funcionalidades y los servicios tras la materialización de un riesgo.

Para garantizar la seguridad de la información se deben tener en cuenta el hardware y el software que soportan la operación de la entidad. Los procedimientos propuestos contemplan cada uno de esos aspectos de manera separada para brindar una recuperación efectiva y eficiente de la operación de los sistemas de información críticos de la organización.

Una vez realizadas las pruebas propuestas en este plan de continuidad, se establecerá el tiempo Máximo de Inactividad Tolerable RPO y el Tiempo de Recuperación Objetivo RTO para cada uno de los riesgos planteados.

5. PLAN DE TRATAMIENTO DE RIESGOS

5.1. ORGANIZACIÓN DE ROLES Y RESPONSABILIDADES

5.1.1. Comité Institucional de Gestión y Desempeño

El Comité Institucional de Gestión y Desempeño creado por la Resolución Municipal 561 del 12 de julio de 2018, será el responsable de orientar la implementación de la política de Seguridad Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión (MIPG).

5.1.2. Subsecretaría de TIC

Según el artículo 2.2.9.1.3.4.del decreto 1008 de 2018, el Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, de la respectiva entidad, tendrá la responsabilidad de liderar la implementación de la Política de Gobierno Digital. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

La Subsecretaría de TIC es la dependencia encargada directamente de la gestión de las tecnologías de la información de la Alcaldía de Rionegro y por lo tanto establece el presente plan de continuidad con el ánimo de definir lineamientos claros para preparar el personal, recursos y procedimientos necesarios para responder a las contingencias que puedan presentarse en los activos críticos de información de la organización.

5.1.3. Grupo de Gestión de TI

Está conformado por el subsecretario de TIC, quien hará las veces de coordinador de ejecución de los planes de continuidad y por el personal de la subsecretaría que está responsabilizado de la administración y mantenimiento de los sistemas de información.

5.1.4. Otros grupos o responsables

Los contratistas, proveedores de bienes y servicios de TI de la Alcaldía de Rionegro, actuarán como colaboradores cuando se materialicen riesgos en los activos de su competencia. Las empresas que actualmente prestan sus servicio son:

Cio Digital

Como proveedor administrador del DNS, es el encargado de mantener los nombres de dominio y el direccionamiento de los subdominios de la entidad.

Como proveedor de servicios de hosting de algunos subdominios de la Alcaldía de Rionegro y entidades descentralizadas, la empresa Cio Digital también debe ser

contactada en caso de presentarse una contingencia en los dominios alojados en sus servidores.

Think IT

Proveedor de servicios de administración de las bases de datos críticas de la organización, debe ser contactado cuando se requiera realizar pruebas, cambios u otras actividades relacionadas con el backup o la administración de las bases de datos.

Tigo-Une

El proveedor de servicios de internet debe ser contactado en caso de que se materialicen riesgos relacionados con la conectividad a internet, el servicio de telefonía o el sistema de aire acondicionado de precisión del Data Center.

Saimyr

Proveedor de servicios de soporte para el sistema ERP de la entidad, debe ser contactada en caso de requerir su intervención para activar una contingencia o realizar tareas administrativas en el aplicativo.

Los demás proveedores de servicios de TI que sean contratados por la entidad tras la aprobación de este plan.

B2B TIC S.A.S.

Proveedor del servicio de mesa de ayuda. Encargados del soporte a las herramientas de hardware y software de los funcionarios de la Alcaldía del Municipio de Rionegro, donde dichas solicitudes serán elaboradas a través de una herramienta (Help people) que asignara las actividades y se validarán a través de tickets que medirán la gestión del servicio.

Otros proveedores

Los datos de contacto de los proveedores de servicios citados en esta sección y otros pueden ser consultados en el inventario de activos de información.

6. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

6.1. Riesgos Internos

6.1.1. Pérdida de la confidencialidad, disponibilidad o integridad de información almacenada en aplicativos críticos (R1)

Consiste en la eliminación, alteración o copia no autorizada de información que es considerada confidencial o clasificada como reservada. La causa de la materialización es la falta de ética de la persona que aprovecha las deficiencias en las políticas de seguridad, vulnerabilidades del software o problemas de configuración de los sistemas de información o la ejecución de un virus en los equipos internos de la entidad. Al materializarse puede ocasionar pérdidas económicas, demandas y sanciones a la entidad y mala imagen institucional.

6.1.2. Indisponibilidad de aplicativo crítico (R2)

Puede deberse a un error de configuración y/o en el código fuente del aplicativo, la falla de un componente de hardware o software del servidor anfitrión, a la falta de recursos del servidor o a la falla de uno de los equipos de red de los que depende. Puede ocasionar que el servicio quede total o parcialmente inoperante o inestable.

6.1.3. Falla técnica en servidor virtual (R3)

Corresponde a la falla de una máquina virtual dentro de un servidor físico, donde operan una o varias aplicaciones, puede ocurrir por errores en la configuración o por agotamiento de recursos del sistema. Puede ocasionar que el servicio quede inoperante o inestable.

6.1.4. Falla técnica en servidor físico (R4)

Corresponde a la falla de un componente de hardware o de software, incluyendo el sistema operativo anfitrión. Puede afectar varios servicios, dejándolos inoperantes o inestables.

6.1.5. Falla técnica en un equipo de comunicaciones de la entidad (R5)

Corresponde a la falla de un componente de hardware o software de un switch o un router propiedad de la administración municipal. Se puede presentar por una descarga eléctrica, interrupción del suministro eléctrico o un error en la configuración, afectando la comunicación de los usuarios y los sistemas de información.

6.1.6. Falla de base de datos de aplicativo crítico (R6)

Corresponde a la falla en el software o configuración de una base de datos, afectando la operación de los sistemas de información.

6.1.7. Calentamiento del centro de cómputo (R7)

La principal causa es una falla en el sistema de aire acondicionado del centro de cómputo y tiene como posibles consecuencias el recalentamiento de los servidores y equipos de red, dejándolos finalmente inoperativos.

6.1.8. Ausencia de personal del Grupo de Gestión de TIC (R8)

La ausencia del personal puede deberse a las vacaciones programadas, días compensatorios o incapacidades, entre otras y puede afectar negativamente el tiempo y la calidad de la respuesta ante un incidente y una contingencia en la infraestructura de TI.

6.1.9. Documentación de la infraestructura de TI incompleta (R9)

Consiste en la falta de documentación del inventario, de la topología y de las configuraciones de los sistemas de información, sus relaciones y los proveedores de servicios de soporte y/o administración, disminuyendo la efectividad, eficiencia y oportunidad en la solución de los incidentes y en la activación de una contingencia.

6.2. Riesgos Externos

6.2.1. Interrupción del suministro eléctrico por más de 15 minutos (R10)

Consiste en la interrupción del suministro eléctrico debido a una falla en las redes externas. Puede dejar inoperativos los sistemas críticos de la entidad (servidores y comunicaciones).

6.2.2. Indisponibilidad del canal de internet (R11)

Consiste en la falla general de la conectividad a internet del Palacio Municipal y puede deberse a un fallo físico o lógico en la red MPLS de UNE. Este fallo puede afectar la conectividad de los sistemas críticos con otras sedes y redes externas y puede implicar la caída de la troncal SIP de telecomunicaciones.

6.2.3. Indisponibilidad del servicio telefónico (R12)

Consiste en la imposibilidad del personal para realizar llamadas entre sedes o para realizar llamadas a líneas fijas y celulares, puede deberse a problemas con la planta telefónica o inoperancia de la troncal SIP con UNE.

6.2.4. Interrupción del servicio por ataque informático (R13)

Puede presentarse por ataque informático realizado desde equipos externos a la entidad, implicando la caída del canal de internet o la inoperancia de los servicios publicados.

6.2.5. Interrupción de servicios por sismo o incendio (R14)

En caso de presentarse un sismo o incendio que afecte la infraestructura de los sistemas de información críticos de la entidad, puede presentarse suspensión total o parcial en la prestación de los servicios de TI, inoperancia de los sistemas o inestabilidad de los mismos.

6.2.6. Resolución DNS inadecuada (R15)

Consiste en la redirección de las conexiones entrantes al portal www.rionegro.gov.co u otro subdominio de la organización hacia otras páginas. Puede deberse a la pérdida de configuración del servidor o a la alteración de los registros por un ataque informático a los sitios web hospedados en servidores vulnerables. Sus consecuencias pueden ser leves o mayores, de acuerdo con las intenciones y conocimientos del atacante.

6.2.7. Falla técnica en un equipo de comunicaciones (R16)

Corresponde a la falla de un componente de hardware o software de un switch o un router propiedad de. Se puede presentar por una descarga eléctrica, interrupción del suministro eléctrico o un error en la configuración, afectando la comunicación de los usuarios y los sistemas de información.

7. ANÁLISIS Y CLASIFICACIÓN DE LOS RIESGOS

El análisis de los riesgos identificados se realiza de acuerdo a la Guía para la administración del riesgo del Departamento Administrativo de la Función Pública.

No.	Riesgo	Probabilidad	Impacto	Calificación
1	Pérdida de la confidencialidad, disponibilidad o integridad de información almacenada en aplicativos críticos	5	MAYOR	EXTREMA
2	Indisponibilidad de aplicativo crítico	4	MODERADO	ALTA
3	Falla técnica en servidor virtual	3	MODERADO	ALTA
4	Falla técnica en servidor físico	4	MAYOR	EXTREMA
5	Falla técnica en un equipo de comunicaciones de la entidad	4	MODERADO	ALTA
6	Falla de base de datos de aplicativo crítico	3	MAYOR	ALTA
7	Calentamiento del centro de cómputo	4	INSIGNIFICANTE	MODERADA
8	Ausencia de personal del Grupo de Gestión de TIC	4	MODERADO	ALTA
9	Documentación de la infraestructura de TI incompleta	4	MODERADO	ALTA
10	Interrupción del suministro eléctrico por más de 15 minutos	4	MODERADO	ALTA

No.	Riesgo	Probabilidad	Impacto	Calificación
11	Indisponibilidad del canal de internet	4	MODERADO	ALTA
12	Indisponibilidad del servicio telefónico	4	MODERADO	ALTA
13	Interrupción del servicio por ataque informático	4	MAYOR	EXTREMA
14	Interrupción de servicios por sismo o incendio	1	MODERADO	MODERADA
15	Resolución DNS inadecuada	4	MAYOR	EXTREMA
16	Falla técnica en un equipo de comunicaciones de UNE	1	MODERADO	MODERADA

8. APLICACIÓN DE CONTROLES

Una vez definidos y valorados los riesgos a los que se encuentra expuesta la entidad, se efectúa un análisis de los controles preventivos o correctivos con los que cuenta la Subsecretaría de TIC.

Dependiendo si el control afecta la Probabilidad o el Impacto se debe desplazar en la matriz de evaluación del riesgo así: la probabilidad avanza hacia abajo y el impacto avanza hacia la izquierda el número de cuadrantes indicado.

Puntaje	Cuadrantes a disminuir
Entre 0 y 50	0
Entre 51 y 75	1
Entre 76 y 100	2

No.	Riesgo	Control	Puntaje
1	Pérdida de la confidencialidad, disponibilidad o integridad de información almacenada en aplicativos críticos	✓ Seguridad Endpoints ✓ Firewall red cableada ✓ Plan de Backups ✓ Sistema de monitoreo	30
2	Indisponibilidad de aplicativo	✓ Sistema de monitoreo de páginas	45
3	Falla técnica en servidor virtual	✓ Sistema de monitoreo por ping	35
4	Falla técnica en servidor físico	✓ Sistema de monitoreo por ping	35
5	Falla técnica en un equipo de comunicaciones de la entidad	Ninguno aplicado	0
6	Falla de base de datos de aplicativo crítico	Ninguno aplicado	0
7	Calentamiento del centro de cómputo	✓ Aire acondicionado de precisión ✓ Sistema de monitoreo en línea	75

No.	Riesgo	Control	Puntaje
8	Ausencia de personal del Grupo de Gestión de TIC durante la materialización del riesgo.	Ninguno aplicado	0
9	Documentación de la infraestructura de TI incompleta	Ninguno aplicado	0
10	Interrupción del suministro eléctrico por más de 15 minutos	✓ UPS ✓ Apagado manual y controlado de servidores. ✓ Planta eléctrica inoperante	15
11	Indisponibilidad del canal de internet	✓ SLA contrato UNE ✓ Monitoreo de conexión a internet	75
12	Indisponibilidad del servicio telefónico	✓ SLA contrato UNE	15
13	Interrupción del servicio por ataque informático	✓ Firewall ✓ Restricciones de tráfico entre redes ✓ Seguridad Endpoints	20
14	Interrupción de servicios por sismo o incendio	Ninguno aplicado	0
15	Resolución DNS inadecuada	Ninguno aplicado	0
16	Falla técnica en un equipo de comunicaciones de UNE	✓ Sistema de monitoreo de UNE ✓ Documentación de la infraestructura de red MPLS	75

De acuerdo con el análisis, los controles que implementa la Subsecretaría de TIC actualmente afectan la probabilidad de materialización de los riegos analizados como se refleja en la siguiente tabla.

No	Riesgo	Antes del control			Después del control		
		Prob	Impacto	Calif	Prob	Impacto	Calif
1	Pérdida de la confidencialidad,	5	MAYOR	EXT	5	MAYOR	EXT

No	Riesgo	Antes del control			Después del control		
		Prob	Impacto	Calif	Prob	Impacto	Calif
	disponibilidad o integridad de información almacenada en aplicativos críticos						
2	Indisponibilidad de aplicativo crítico	4	MOD	ALTA	4	MOD	ALTA
3	Falla técnica en servidor virtual	3	MOD	ALTA	3	MOD	ALTA
4	Falla técnica en servidor físico	4	MAYOR	EXT	4	MAYOR	EXT
5	Falla técnica en un equipo de comunicaciones de la entidad	4	MOD	ALTA	4	MOD	ALTA
6	Falla de base de datos de aplicativo crítico	3	MAYOR	ALTA	3	MAYOR	ALTA
7	Calentamiento del centro de cómputo	4	INSIG	MOD	3	INSIG	BAJA
8	Ausencia de personal del Grupo de Gestión de TIC durante la materialización del riesgo.	4	MOD	ALTA	4	MOD	ALTA
9	Documentación de la infraestructura de TI incompleta	4	MOD	ALTA	4	MOD	ALTA
10	Interrupción del suministro eléctrico en más de 15 minutos	4	MOD	ALTA	4	MOD	ALTA
11	Indisponibilidad del canal de internet	4	MOD	ALTA	3	MENOR	MOD

No	Riesgo	Antes del control			Después del control		
		Prob	Impacto	Calif	Prob	Impacto	Calif
12	Indisponibilidad del servicio telefónico	4	MOD	ALTA	4	MOD	ALTA
13	Interrupción del servicio por ataque informático	4	MAYOR	EXTR	4	MAYOR	EXTR
14	Interrupción de servicios por sismo o incendio	1	MOD	MOD	1	MOD	MOD
15	Resolución DNS inadecuada	4	MAYOR	EXTR	4	MAYOR	EXTR
16	Falla técnica en un equipo de comunicaciones de UNE	1	MOD	MOD	1	MENOR	BAJA

Tras el análisis de los controles existentes, se plantearán las acciones de respuesta ante la materialización de los riesgos que se encuentren en categoría extrema, alta y moderada.

9. ACTIVIDADES DEL PLAN SEGÚN EL RIESGO

9.1. R1 - Pérdida de la confidencialidad, disponibilidad o integridad de información almacenada en aplicativos críticos

Consiste en la eliminación, alteración o copia no autorizada de información almacenada en los aplicativos Saimyr, Document, BPMS y el repositorio de información One Drive, considerada confidencial o clasificada como reservada. Se clasifica como riesgo interno cuando las acciones son realizadas desde redes internas por un funcionario o contratista de la entidad.

9.1.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel EXTREMO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de este riesgo tendrá periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la probabilidad de materialización:

- Actualización y ejecución del plan de copias de respaldo.
- Adición de cláusula de confidencialidad e integridad de la información en contratos de personal.
- Implementación de firewall para las redes inalámbricas.
- Definir plan de transición a IPv6.
- Instalación, actualización y monitoreo de antivirus en servidores.
- Implementación de autenticación de doble factor en Saimyr.
- Auditoría periódica de contraseñas.
- Cambio periódico de contraseñas de servidores y sistemas de backup.
- Cambio periódico de contraseña de administrador local.
- Restringir el acceso remoto a servidores.
- Restringir y registrar el acceso de personal a los Datacenter.
- Consultar periódicamente la existencia de vulnerabilidades en el software de los activos de información en el sitio us-cert.gov.
- Definición de roles y funciones específicos para la administración de la infraestructura técnica y de seguridad de la entidad.
- Implementación de firma digital para documentos.

9.1.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

1. El usuario al que le ocurrió el incidente debe reportar la pérdida de información a la Mesa de Ayuda, identificando la aplicación, módulo y tipo de información afectada.
2. El personal del Grupo de Gestión de TIC valida la información reportada por el usuario y realiza un informe técnico de la situación analizada.
3. Se contacta al proveedor de servicios administrativos de base de datos para realizar la restauración de la información que se vio comprometida.
4. Apoyar al usuario en la restauración de la información hasta que pueda seguir con su función normal.

Después de la materialización:

1. Se contacta al proveedor de los sistemas de información para corregir las posibles brechas de seguridad detectadas tras el evento.
2. Se realiza ajuste a las políticas de seguridad de la información en caso de ser necesario.
3. Se capacita al usuario en los procedimientos y usos de los recursos.

9.2. R2 - Indisponibilidad de aplicativo crítico

Puede deberse a un error de configuración y/o en el código fuente del aplicativo, la falla de un componente de hardware o software del servidor anfitrión, a la falta de recursos del servidor o a la falla de uno de los equipos de red de los que depende. Puede ocasionar que el servicio quede total o parcialmente inoperante o inestable.

9.2.1. Gestión del riesgo residual

Debido a que este riesgo está catalogado en nivel ALTO se deben establecer acciones de control preventivas que permitan reducir probabilidad de ocurrencia del riesgo. La administración de estos riesgos tendrá periodicidad bimestral.

Se propone la implementación de las siguientes medidas con el fin de reducir la probabilidad de materialización:

- Actualización y ejecución del plan de copias de respaldo
- Implementación de sistema de monitoreo de páginas y aplicaciones.
- Implementación y mantenimiento de la CMDB.
- Actualizar la documentación técnica y de soporte de los aplicativos Document, módulos de Saimyr, BPMS y el repositorio de información One Drive.
- Actualización de la infraestructura técnica y sistemas operativos.

9.2.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la contingencia:

1. Realizar el reporte del incidente en la herramienta HelpPeople para llevar la documentación del caso.

2. El personal del Grupo de Gestión de TI realiza un diagnóstico del servidor para determinar la causa de la interrupción en el servicio.
3. Si el problema obedece a una falla física del servidor host, realizar el diagnóstico específico del componente que presenta problemas y solicitarlo a través del servicio de mesa de ayuda.
4. En caso de requerirlo, se debe contactar al proveedor de soporte del aplicativo o el administrador de bases de datos para retornar el aplicativo a producción.
5. Informar al grupo de usuarios sobre el estado de la contingencia a través de correo electrónico, teléfono o según se proceda.

Después de la contingencia:

1. Se contacta al proveedor del sistema de información para solucionar los bugs o problemas detectados ocasionados por el evento.
2. Documentar y cerrar el caso en HelpPeople.
3. Se realiza ajuste a las políticas de seguridad de la información en caso de ser necesario.
4. Se capacita al usuario en los procedimientos y usos de los recursos.

9.3. R3 - Falla técnica en servidor virtual

Corresponde a la falla de una máquina virtual dentro de un servidor físico, donde operan una o varias aplicaciones, puede ocurrir por errores en la configuración o por agotamiento de recursos del sistema. Puede ocasionar que el servicio quede inoperante o inestable.

9.3.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel ALTO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos será con periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la probabilidad de materialización:

- Actualización y ejecución del plan de copias de respaldo de VM
- Implementación de sistema de monitoreo de recursos de servidores
- Implementación y mantenimiento de la CMDB.
- Actualizar la documentación de la infraestructura tecnológica.
- Análisis y actualización de la capacidad de la infraestructura tecnológica.

9.3.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la contingencia:

1. Realizar el reporte del incidente en la herramienta HelpPeople para llevar la documentación del caso.
2. El personal de la Grupo de Gestión de TIC realiza un diagnóstico del servidor para determinar la causa de la interrupción en el servicio.
3. Si el problema obedece a la falla de un aplicativo, realizar el diagnóstico específico del módulo o componente que presenta problemas y solicitar soporte técnico al proveedor.
4. Informar al grupo de usuarios sobre el estado de la contingencia a través de correo electrónico, teléfono o según se proceda.

Después de la contingencia:

1. Documentar y cerrar el caso en HelpPeople.
2. Se realiza ajuste a las políticas de seguridad de la información en caso de ser necesario.
3. Se capacita al usuario en los procedimientos y usos de los recursos.

9.4. R4 - Falla técnica en servidor físico

Corresponde a la falla de un componente de hardware o de software, incluyendo el sistema operativo anfitrión. Puede afectar varios servicios, dejándolos inoperantes o inestables.

9.4.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel EXTREMO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos será con periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la probabilidad de materialización:

- Actualización y ejecución del plan de copias de respaldo
- Implementación de sistema de monitoreo de recursos de servidores
- Implementación y mantenimiento de la CMDB.
- Actualizar la documentación de la infraestructura tecnológica.
- Stock de partes de repuesto para servidores críticos
- Restringir y registrar el acceso de personal a los Datacenter.

9.4.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la contingencia:

1. Realizar el reporte del incidente en la herramienta Help People para llevar la documentación del caso.

2. El personal de la Grupo de Gestión de TIC realiza un diagnóstico del servidor para determinar la causa de la falla.
3. Si el problema obedece a una falla física, realizar el diagnóstico específico del componente que presenta problemas y solicitarlo a través del contrato de mesa de ayuda.
4. Si el problema obedece a la falla de un componente de software, realizar el diagnóstico específico del módulo o componente que presenta problemas y solicitar soporte técnico al proveedor.
5. Informar al grupo de usuarios sobre el estado de la contingencia a través de correo electrónico, teléfono o según se proceda.

Después de la contingencia:

1. Documentar y cerrar el caso en HelpPeople.
2. Se realiza ajuste a las políticas de seguridad de la información en caso de ser necesario.
3. Se capacita al grupo de usuarios en los procedimientos y usos de los recursos.

9.5. R5 - Falla técnica en un equipo de comunicaciones de la entidad

Corresponde a la falla de un componente de hardware o software de un switche o un router propiedad de la administración municipal. Se puede presentar por una descarga eléctrica, interrupción del suministro eléctrico o un error en la configuración, afectando la comunicación de los usuarios y los sistemas de información.

9.5.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel ALTO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos tendrá periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización:

- Actualización y ejecución del plan de copias de respaldo de configuración.
- Implementación de sistema de monitoreo de recursos de dispositivos de red.
- Implementación y mantenimiento de la CMDB.
- Actualizar la documentación de la infraestructura tecnológica.
- Restringir y registrar el acceso de personal a los Datacenter.
- Registro de cambios en conexiones de dispositivos.
- Stock de switches para reposición.

9.5.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la contingencia:

1. Realizar el reporte del incidente en la herramienta HelpPeople para llevar la documentación del caso.
2. El personal de la Grupo de Gestión de TIC realiza un diagnóstico del dispositivo para determinar la causa de la falla.
3. Si el problema obedece a una falla física, realizar el diagnóstico específico del componente que presenta problemas y solicitarlo a través del contrato de mesa de ayuda.
4. Si el problema obedece a la falla de un componente de software o configuración, realizar el diagnóstico específico para realizar la corrección o solicitar soporte técnico al proveedor.
5. Informar al grupo de usuarios sobre el estado de la contingencia a través de correo electrónico o teléfono según proceda.

Después de la contingencia:

1. Documentar y cerrar el caso en HelpPeople.
2. Se realiza ajuste a las políticas de seguridad de la información en caso de ser necesario.
3. Se capacita al grupo de usuarios en los procedimientos y usos de los recursos.

9.6. R6 - Falla de base de datos

Corresponde a la falla en el software o configuración de una base de datos, afectando la operación de los sistemas de información.

9.6.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel ALTO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos tendrá periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización:

- Actualización y ejecución del plan de copias de respaldo.
- Implementación de sistema de monitoreo de recursos de motores de bases de datos.
- Actualizar la documentación técnica y de soporte de la base de datos.
- Implementación y mantenimiento de la CMDB.

9.6.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

1. Aplicar el check list para identificar el problema en la base de datos por parte del Grupo de Gestión de TI.

2. Llamar al proveedor en caso de ser necesario.
3. Realizar los cambios respectivos.

Después de la materialización:

4. Actualizar la documentación de la infraestructura tecnológica y de soporte de la base de datos.
5. Capacitar al personal del Grupo de Gestión de TI.
6. Ajustar el sistema de monitoreo para asegurar la detección temprana de este tipo de fallas.

9.7. R8 - Ausencia de personal del Grupo de Gestión de TIC durante la materialización del riesgo.

La ausencia del personal puede deberse a las vacaciones programadas, días compensatorios o incapacidades y puede afectar negativamente el tiempo y la calidad de la respuesta ante un incidente y una contingencia en la infraestructura de TI.

9.7.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel MODERADO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos tendrá periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización:

- Responsable y suplente de personal idóneo por componente de infraestructura técnica.
- Actualizar la documentación técnica y de soporte de los componentes de infraestructura críticos.
- Implementación y mantenimiento de la CMDB.

9.7.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

1. Consultar, analizar y guiarse con la documentación existente.
2. Contactar al proveedor en caso de ser necesario.
3. Solicitar soporte en sitio de personal especializado en caso de ser necesario.

Después de la materialización:

1. Actualizar la documentación técnica y de soporte de los componentes de infraestructura críticos.
2. Capacitar al personal del Grupo de Gestión de TI

9.8. R9 - Documentación de la infraestructura de TI incompleta

Consiste en la falta de documentación del inventario, la topología y las configuraciones de los sistemas de información, sus relaciones y los proveedores de servicios de soporte y/o administración, lo que puede disminuir la efectividad, eficiencia y oportunidad en la solución de los incidentes y en la activación de contingencias.

9.8.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel ALTO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos será con periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización:

- Revisión de marco legal y elaboración de documentación faltante.
- Mantenimiento de los Inventarios de TI.
- Implementación y monitoreo de la apropiación de políticas.
- Creación y almacenamiento adecuado de manuales.
- Implementación de cronogramas de tareas del área de TI.
- Implementación y mantenimiento de la CMDB.
- Actualizar la documentación técnica y de soporte de los componentes de infraestructura críticos.

9.8.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

1. Consultar, analizar y guiarse con la documentación existente.
2. Contactar al proveedor en caso de ser necesario.
3. Solicitar soporte en sitio de personal especializado en caso de ser necesario.

Después de la materialización:

1. Actualizar la documentación técnica y de soporte de los componentes de infraestructura críticos.
2. Actualizar la CMDB.
3. Capacitar al personal del Grupo de Gestión de TI

9.9. R10 - Interrupción del suministro eléctrico por más de 15 minutos

En caso de presentarse una interrupción en el suministro eléctrico debida a un fallo en las redes externas a la entidad y si éste se prolonga más de quince minutos, las consecuencias pueden ser graves para la entidad debido a que los servidores deben ser apagados, entorpeciendo las labores de los procesos misionales de la entidad.

9.9.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel ALTO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos tendrá periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización:

- Ampliación de la capacidad de las UPS
- Implementación de un sistema de monitoreo en línea de las UPS
- Reparación y definición de plan de pruebas periódicas de la planta eléctrica del Palacio Municipal
- Actualizar la documentación técnica y de soporte de los componentes.
- Actualizar la CMDB.

9.9.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

1. Controlar el tiempo de interrupción del servicio eléctrico y contactar a EPM sobre la indisponibilidad presentada.
2. Transcurridos 10 minutos del evento, se procede a realizar un apagado controlado de los componentes de infraestructura en el centro de cómputo.

Después de la materialización:

1. Cinco minutos después del restablecimiento del servicio eléctrico y comprobar con el proveedor que no se va a tener más intermitencia se procede a realizar un encendido controlado de los componentes de infraestructura en el centro de cómputo.
2. Verificar la adecuada carga y restablecimiento de la UPS.
3. Realizar un monitoreo y confirmar con los usuarios el restablecimiento de los servicios.
4. Actualizar la documentación técnica y de soporte de los componentes.
5. Actualizar la CMDB.

9.10. R12 - Indisponibilidad del servicio telefónico

El servicio de llamadas a líneas físicas nacionales e internacionales y teléfonos celulares para el Municipio de Rionegro es prestado por UNE a través de una troncal SIP. Este servicio depende del canal de datos a través de la MPLS. En caso de que presente indisponibilidad, la medida correctiva está en manos del proveedor.

9.10.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel ALTO se deben establecer acciones de control preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos tendrá periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización:

- Implementación, configuración y monitoreo de sistema de monitoreo del servicio telefónico
- Restringir y registrar el acceso de personal a los Datacenter
- Registro de cambios en conexiones de dispositivos.

9.10.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

1. Controlar el tiempo de interrupción del servicio y contactar a Tigo-Une vía celular sobre la indisponibilidad presentada.
2. Escribir al grupo general Alcaldía para informar sobre la situación y avances en la reparación.
3. Transcurridos diez minutos se realiza una nueva prueba de llamada y seguimiento al caso con Tigo-Une

Después de la materialización:

1. Realizar un monitoreo y confirmar con los usuarios el restablecimiento de los servicios.
2. Actualizar la documentación técnica y de soporte de los componentes.

9.11. R13 - Interrupción del servicio por ataque informático

En un ataque informático pueden verse comprometidos distintos recursos internos y externos de la entidad, tras la materialización de este riesgo deben identificarse los componentes de la infraestructura de TI que resultaron afectados para dar respuesta a cada situación según el presente plan.

9.11.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel ALTO se deben establecer acciones de control correctivas y preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos será con periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización:

- Auditoria periódica de contraseñas de usuarios de Document, Saimyr, BPMS y directorio activo

- Capacitación en seguridad informática a usuarios.
- Implementación de certificado SSL para todos los subdominios web.
- Implementación de sistema de seguridad para los portales web contra DDoS tipo Cloud Flare.
- Implementación obligatoria de conexión VPN para proveer o consumir servicios web.
- Análisis mensual de logs de la consola de seguridad endpoint y definición de tareas prioritarias.
- Análisis mensual de logs de la UTM y definición de tareas prioritarias.
- Implementación y mantenimiento de la CMDB.

9.11.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

1. El grupo de Gestión de TI identifica los sistemas de información afectados por el ataque.
2. Sacar de producción los sistemas de información afectados.
3. Identificar la información que se vio comprometida durante el ataque.
4. Identificar la fuente del ataque, el tipo de ataque y vulnerabilidades explotadas.
5. Reportar el caso a Colcert.
6. Contactar los proveedores relacionados para reestablecer las copias de seguridad necesarias.
7. Actualizar las versiones vulnerables de los sistemas de información afectados.
8. Retornar los sistemas de información a producción.

Después de la materialización:

1. Se contacta al proveedor de los sistemas de información para corregir las posibles brechas de seguridad detectadas tras el evento.
2. Se realiza ajuste a las políticas de seguridad de la información en caso de ser necesario.
3. Cerrar el caso en Colcert.
4. Realizar monitoreo diario de los sistemas de información afectados para detectar posibles ataques.

9.12. R14 - Interrupción de servicios por sismo o incendio

En caso de presentarse un sismo o incendio que afecte la infraestructura de los sistemas de información críticos de la entidad, puede presentarse suspensión total o parcial del funcionamiento o de la prestación de los servicios de TI, inoperancia de los sistemas o inestabilidad de estos.

La entidad cuenta con un programa de seguridad y salud en el trabajo que asegura la disponibilidad de extintores suficientes y adecuados además del personal capacitado para la extinción de contactos en caso de presentarse.

Por otro lado, el respaldo de la información crítica del BPMS en la nube brindará un soporte de la información en caso de que un sismo deje inoperante la infraestructura de TI de la entidad.

Debido a que la materialización de este riesgo puede comprometer distintos recursos internos y externos de la entidad, deben identificarse los componentes de la infraestructura de TI que resultaron afectados para dar respuesta a cada uno según el presente plan.

9.12.1. Gestión del riesgo residual

Debido a que este riesgo está catalogado en nivel MODERADO se deben establecer acciones de control preventivas que permitan reducir la materialización del riesgo. La administración de estos riesgos será con periodicidad bimestral.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización:

- Respaldo de información crítica en la nube.
- Implementación de sistema automático de detección y extinción de incendios en el Datacenter.
-

9.12.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

El personal debe proceder de acuerdo con los planes de emergencia definidos por la oficina de seguridad y salud en el trabajo

Después de la materialización:

1. Documentar y reportar los problemas físicos sufridos en la infraestructura de TI incluyendo las paredes, piso y puerta del Datacenter, UPS y equipo de aire acondicionado
2. Contactar al proveedor de soporte de los sistemas de información para corregir las posibles consecuencias del evento.
3. En caso de sismo, comprobar con el proveedor del servicio eléctrico y conectividad a internet que no se va a tener intermitencia.
4. En caso de determinar que es seguro reestablecer las operaciones, retornar a producción los sistemas de información y verificar su funcionamiento con los usuarios internos y externos.
5. Verificar la adecuada carga y restablecimiento de la UPS.

6. Monitorear constantemente los sistemas de información para detectar posibles problemas no detectados durante el diagnóstico inicial.
7. Actualizar la documentación técnica y de soporte de los componentes.
8. Actualizar la CMDB.

9.13. 15 - Resolución DNS inadecuada

Consiste en la redirección de las conexiones entrantes al portal www.rionegro.gov.co u otro subdominio de la organización hacia otras páginas. Puede deberse a la pérdida de configuración del servidor o a la alteración de los registros por un ataque informático a los sitios web hospedados en servidores vulnerables. Sus consecuencias pueden ser leves o mayores, de acuerdo con las intenciones y conocimientos del atacante.

9.13.1. Gestión del riesgo residual

Debido a que el riesgo está catalogado en nivel EXTREMO se deben establecer acciones de control correctivas y preventivas que permitan evitar la materialización del riesgo. La administración de estos riesgos será con periodicidad mensual.

Se propone la implementación de las siguientes medidas con el fin de reducir la posibilidad de materialización

- Traslado de la configuración del sistema DNS.
- Realizar copia de seguridad de la configuración de DNS de la entidad.

9.13.2. Procedimiento de respuesta tras la materialización del riesgo:

Durante la materialización:

1. El grupo de Gestión de TI identifica los dominios o subdominios afectados por el ataque.
2. Sacar de producción los sistemas de información afectados
3. Reportar el problema al proveedor de servicios de registro de dominios para realizar el restablecimiento de los registros afectados.
4. Identificar la fuente del ataque, el tipo de ataque y vulnerabilidades explotadas.
5. Reportar el caso a Colcert aportando la documentación requerida.
6. Retornar los sistemas de información a producción.

Después de la materialización:

1. Se contacta al proveedor de los sistemas de información para corregir las posibles brechas de seguridad detectadas tras el evento.
2. Cerrar el caso en Colcert.

3. Realizar monitoreo diario de los sistemas de información afectados para detectar posibles ataques.

10. PLAN DE PRUEBAS

El plan de pruebas tiene como objetivo principal capacitar al personal del Grupo de Gestión de TI y a los funcionarios que hacen uso de los sistemas de información críticos, para identificar y usar los recursos, realizar los procedimientos y contactar al personal adecuado tras la materialización de un riesgo.

Otro de los objetivos es determinar los tiempos de atención y solución en cada uno de los escenarios para documentarlos y mejorar continuamente los acuerdos de nivel de servicio con la entidad.

Este plan de pruebas debe tener por lo menos una prueba semestral de cada uno de los planes de acción ante la materialización de un riesgo. Las pruebas deben realizarse en horarios que minimicen el impacto sobre el negocio.

Las pruebas deben incluir, por lo menos las siguientes actividades:

- Restauración de copias de respaldo de bases de datos de aplicativos críticos.
- Lectura de logs de software que soporte los aplicativos críticos de la entidad.
- Restauración de copias de respaldo de máquinas virtuales.
- Diagnóstico de componentes de servidores físicos.
- Carga de configuración en un router y en un switch administrable y traslado de puntos de red.
- Atención de incidente por personal no titular.
- Revisión de la documentación disponible para la atención del problema durante la prueba.
- Funcionamiento de las UPS ante cortes de energía.
- Lectura de logs de sistemas de seguridad como firewall y end point.
- Contacto a proveedores.

El personal de Grupo de Gestión de TI debe documentar toda la información relacionada con la atención del problema como el tiempo de respuesta, recursos usados, proveedores contactados y otra información que se considere relevante para mejorar este plan.

11. REVISIÓN, MANTENIMIENTO Y ACTUALIZACIÓN DE ESTE PLAN

El Grupo de Gestión de TI debe revisar y actualizar este plan semestralmente, cada vez que sea usado para dar respuesta a la materialización de un riesgo o cuando se presente uno de los siguientes eventos:

- Pruebas.
- Adquisición de nueva infraestructura tecnológica.
- Materialización de riesgos no identificados en el plan.
- Cambios en la identificación o análisis de riesgos.

Los objetivos de la revisión y actualización de este plan son:

- Identificar y registrar nuevos riesgos y su respectiva valoración.
- Revisar la adecuación a requisitos legales
- Agregar aspectos no considerados dentro del plan
- Actualizar controles implementados y la valoración del efecto de cada uno.
- Actualizar el listado de proveedores, usuarios y administradores funcionales de los aplicativos en el directorio.

12. CONTROL DE CAMBIOS

FECHA	VER.	PROYECTÓ	REVISÓ	APROBÓ	DESCRIPCIÓN
24/01/2019	1.0	Oscar Franco Catalina Martínez	Héctor Fabio Orjuela	Comité Institucional de Gestión y Desempeño	Versión inicial
06/09/2019	2.0	Oscar Franco	Héctor Fabio Orjuela	Comité Institucional de Gestión y Desempeño	Actualización con manual de Riesgos V2
03/02/2022	3.0	Juan Abril	Héctor Fabio Orjuela	Comité Institucional de Gestión y Desempeño	Actualización Proveedor mesa de ayuda