**CBN-1107**

**PLAN DE CONTINGENCIA INSTITUCIONAL**

**UNIDAD ADMINISTRATIVA ESPECIAL**

**DE REHABILITACIÓN Y MANTENIMIENTO VIAL**

**TABLA DE CONTENIDO**

Contenido

[1. INTRODUCCIÓN 4](#_Toc32412030)

[2. OBJETIVO 5](#_Toc32412031)

[3. ACLARACIONES 6](#_Toc32412032)

[4. GESTION DE RIESGOS 7](#_Toc32412033)

[5. POSIBLES ESCENARIOS DE CONTINGENCIA 13](#_Toc32412034)

[6. SISTEMAS DE INFORMACIÓN 16](#_Toc32412035)

[7. INFRAESTRUCTURA 23](#_Toc32412036)

[8. CENTRO DE DATOS 26](#_Toc32412037)

[9. ARQUITECTURA CLOUD 28](#_Toc32412038)

[10. POLÍTICAS DE SEGURIDAD 30](#_Toc32412039)

[10.1 PROPÓSITO 30](#_Toc32412040)

[10.2 POLÍTICAS ESPECIFICAS. 30](#_Toc32412041)

[11. ROLES Y RESPONSABILIDADES 31](#_Toc32412042)

[12. CONTROL DE ACCESO 32](#_Toc32412043)

[13. CANALES DE COMUNICACIÓN 33](#_Toc32412044)

[14. COPIAS DE RESPALDO. 35](#_Toc32412045)

[15. SISTEMAS DE SEGURIDAD PERIMETRAL 36](#_Toc32412046)

[16. INVENTARIOS DE INFRAESTRUCTURA TI 37](#_Toc32412047)

[17. MONITOREO 38](#_Toc32412048)

[18. SISTEMAS WEB 39](#_Toc32412049)

[19. SISTEMA DE RESPALDO ELÉCTRICO 40](#_Toc32412050)

[20. SISTEMA INTEGRADO DE SEGURIDAD ELECTRÓNICA (CCTV) 41](#_Toc32412051)

[21. PRUEBAS 42](#_Toc32412052)

[22. RIESGOS DE SALUD OCUPACIONAL Y/O SISTEMAS DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO 43](#_Toc32412053)

[23. RIESGOS DE GESTIÓN AMBIENTAL 43](#_Toc32412054)

[24. ANÁLISIS DE RIESGO Y VULNERABILIDAD 44](#_Toc32412055)

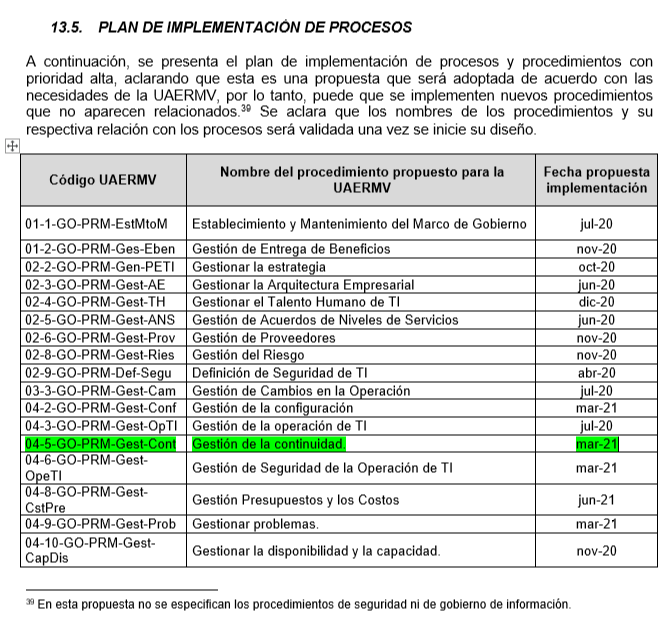
[OBJETIVOS ESPECÍFICOS 44](#_Toc32412056)

# INTRODUCCIÓN

En el cumplimiento de sus actividades Misionales la UMV ha venido evolucionando sus planes operativos hacia una entidad Digital. Esto conlleva a que la plataforma tecnológica de la UMV haya tenido un avance significativo en los últimos años.

El siguiente documento reúne un compendio de actividades, roles y responsabilidades en alto nivel, encaminadas a garantizar la operación de la UMV en caso de presentarse un evento imprevisto bien sea de características naturales, antrópicos, humanos, salud ocupacional y técnicos, que atenten con la infraestructura critica de la entidad.

Para cumplir con este plan es necesario tener en cuenta las etapas de Evaluación del estado actual, elaboración de planes de mitigación, pruebas de viabilidad y ejecución de estas.



# OBJETIVO

Presentar las diferentes acciones ejecutadas por la UAERMV para dar continuidad a la operación de la entidad desde el dominio de la plataforma tecnológica de la entidad, el funcionamiento de los sistemas de información misionales y operativos de la UMV en caso de presentarse un evento de desastre natural o físico o una interrupción mayor causada por ataques tecnológicos, así como el plan de emergencias implementado por la Entidad.

# ACLARACIONES

La Unidad de Mantenimiento Vial actualmente tiene elementos, planes, estrategias y documentos a ser considerados en el Plan de Continuidad del Negocio para que la operación de esta pueda continuar con sus actividades misionales en un espacio diferente a la sede principal.

Dado que no se cuenta con todos los artefactos que conforman un Plan de Continuidad normalizado si es posible gracias a sus estrategias y planes mitigar las posibles causas de un evento evitable que ocasione una interrupción en su operación.

Las siguientes son los elementos que conforman el plan de recuperación tecnológico de la UMV.

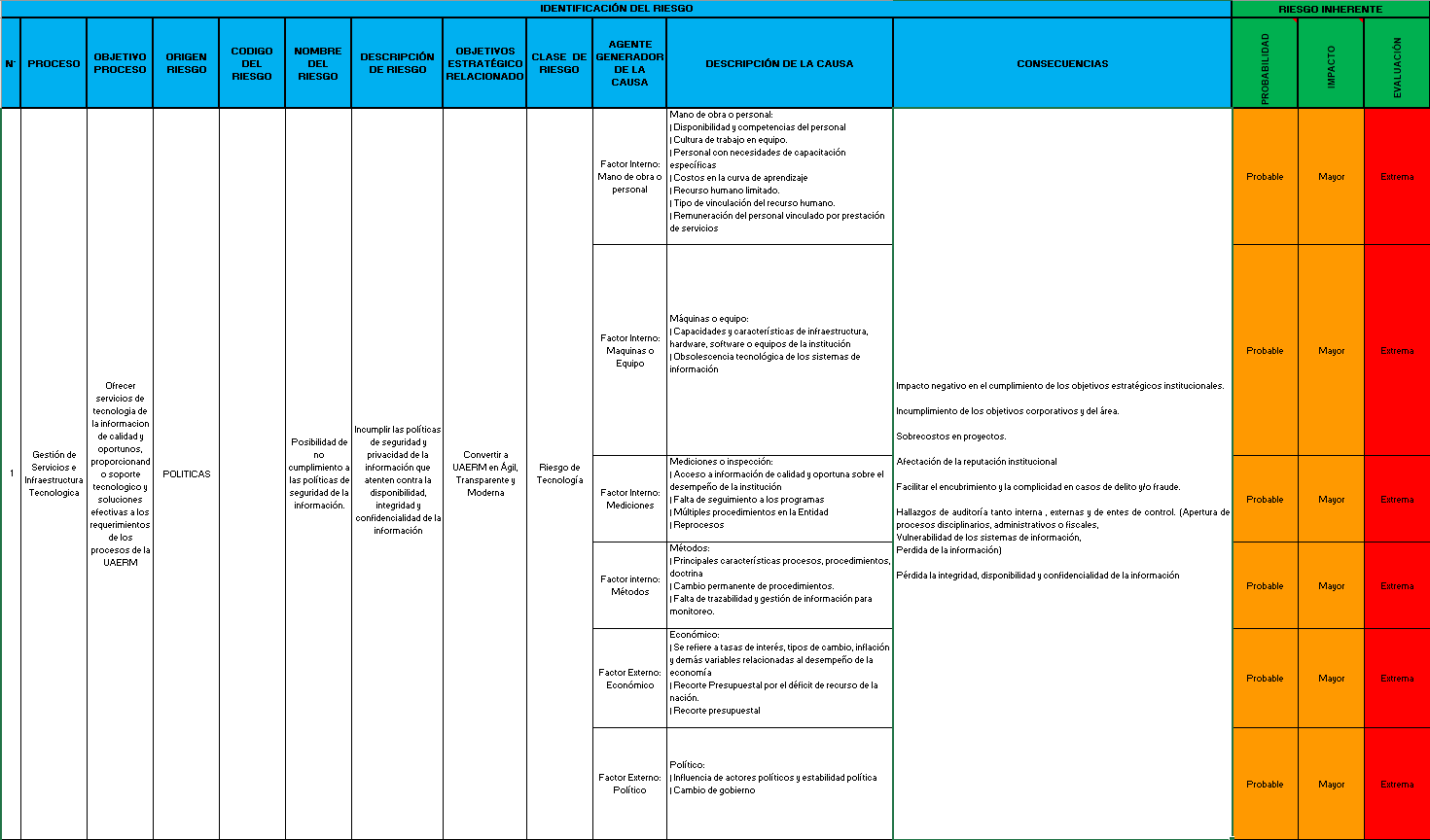
Los servicios Misionales y de gran impacto se encuentran bajo una Arquitectura de Nube contratada en Oracle Cloud Infrastructure.

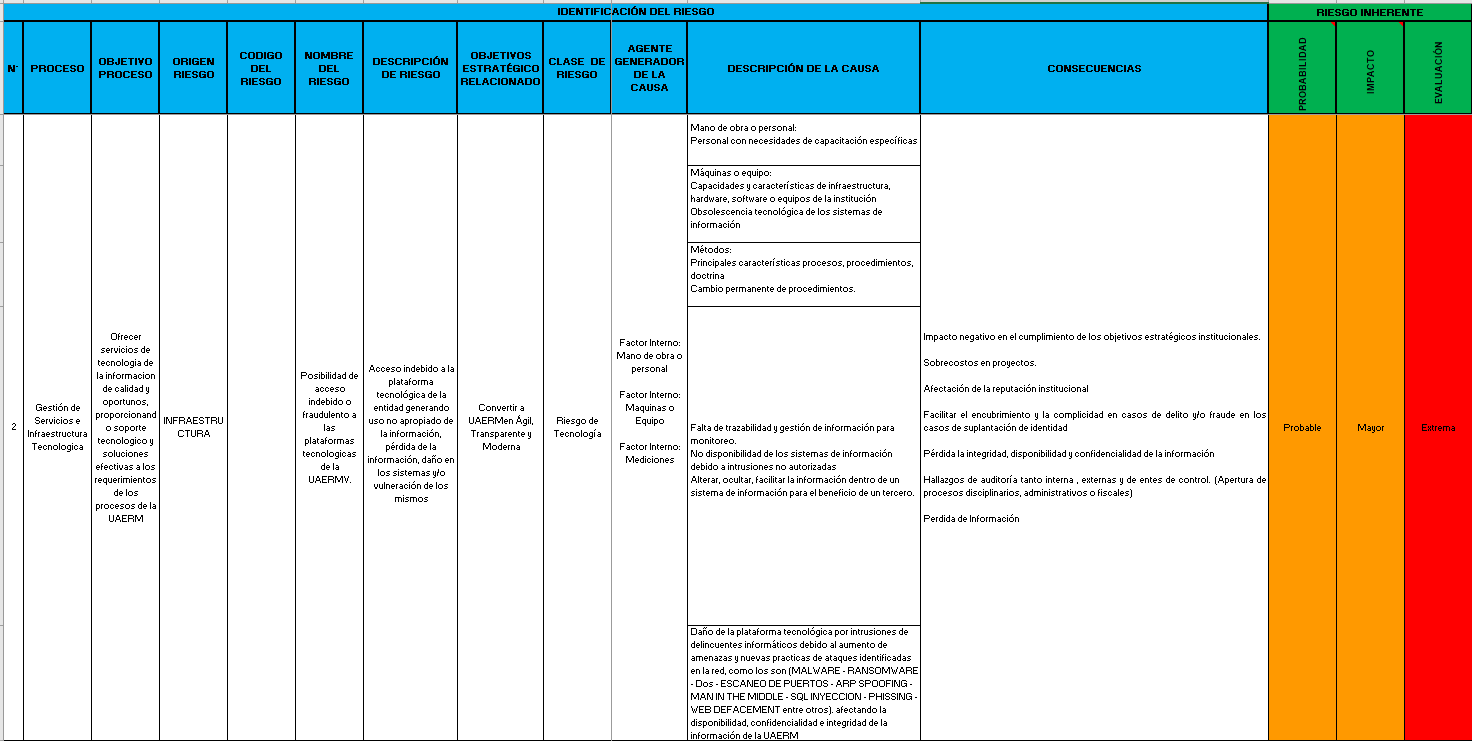
* El centro de Cómputo principal no cuenta con las características de un centro de datos Tier. [[1]](#footnote-2)No se cumplen con todas las disposiciones de la TIA 942[[2]](#footnote-3).
* Actualmente la entidad no tiene contratado un Centro de Cómputo Alterno, que cuente con infraestructura idéntica el centro de cómputo principal ni con respaldo de equipos servidores que estén replicados a los de la arquitectura Cloud.
* Los servidores que se encuentran en el centro de cómputo principal tienen Arquitecturas Físicas y virtualizadas. Sin embargo, estos equipos sufren de obsolescencia tecnológica y la licencia de virtualización es libre.
* Se debe realizar un dimensionamiento tanto de espacio en discos como en características de los equipos tanto los que se tienen en el centro de cómputo principal como los que están en la Nube de Oracle para dimensionar un centro de datos alterno.
* Para las aplicaciones misionales se deben crear ambientes de preproducción, pruebas y producción para la continuidad.
* La infraestructura tecnológica debe contar con equipos en Alta disponibilidad y redundancia tanto en discos como en fuentes de energía.
* Los canales de comunicación deben ser de alta disponibilidad y cada sede debe contar con acceso a la Nube de Oracle OCI.

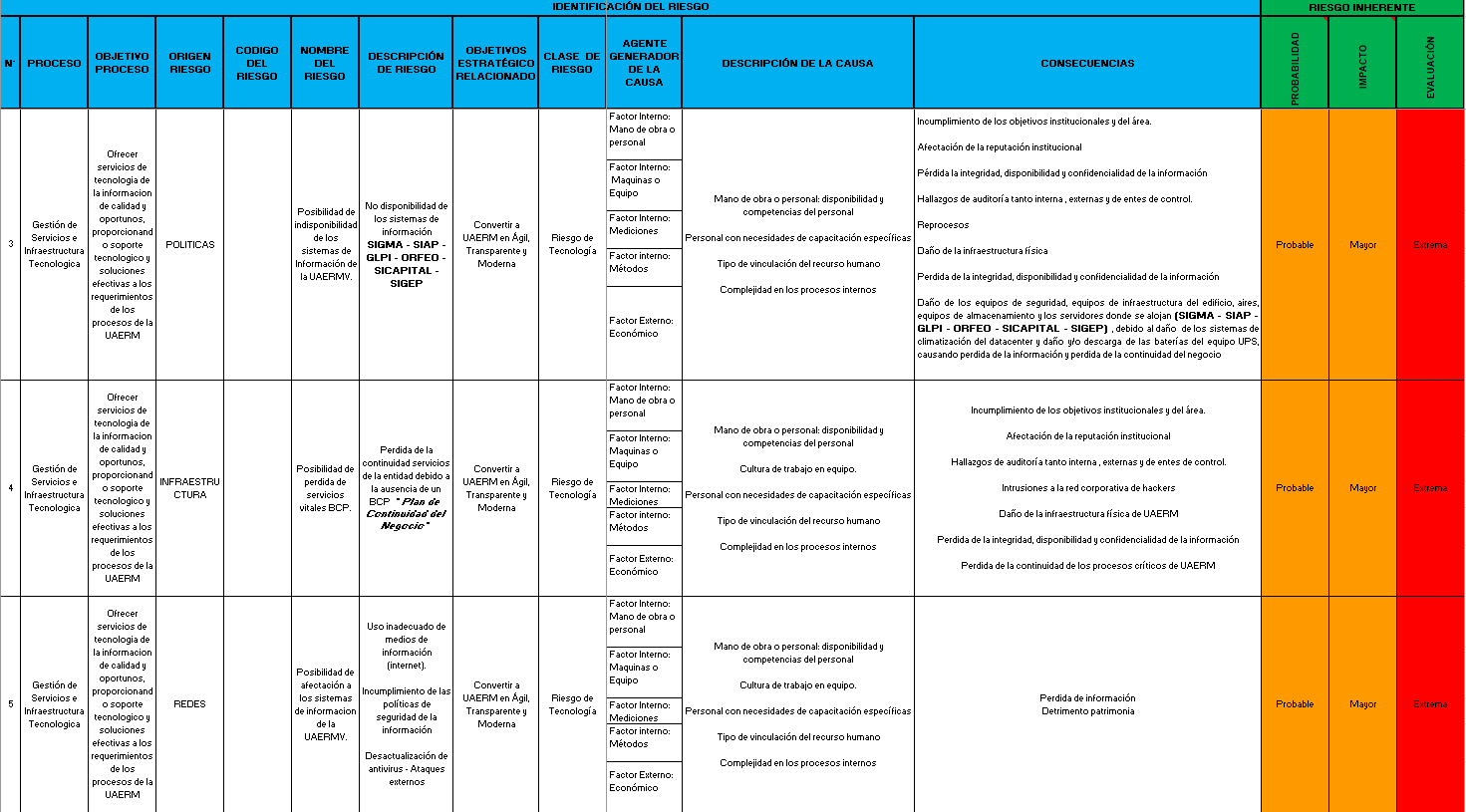
Además, la entidad cuenta con tres sedes que dan una ventaja hablando de temas de contingencia ya que en una de las se puede pensar en tener implementado un Centro de Operaciones Alterna para operar en caso de una emergencia en cualquiera de sus otras sedes.

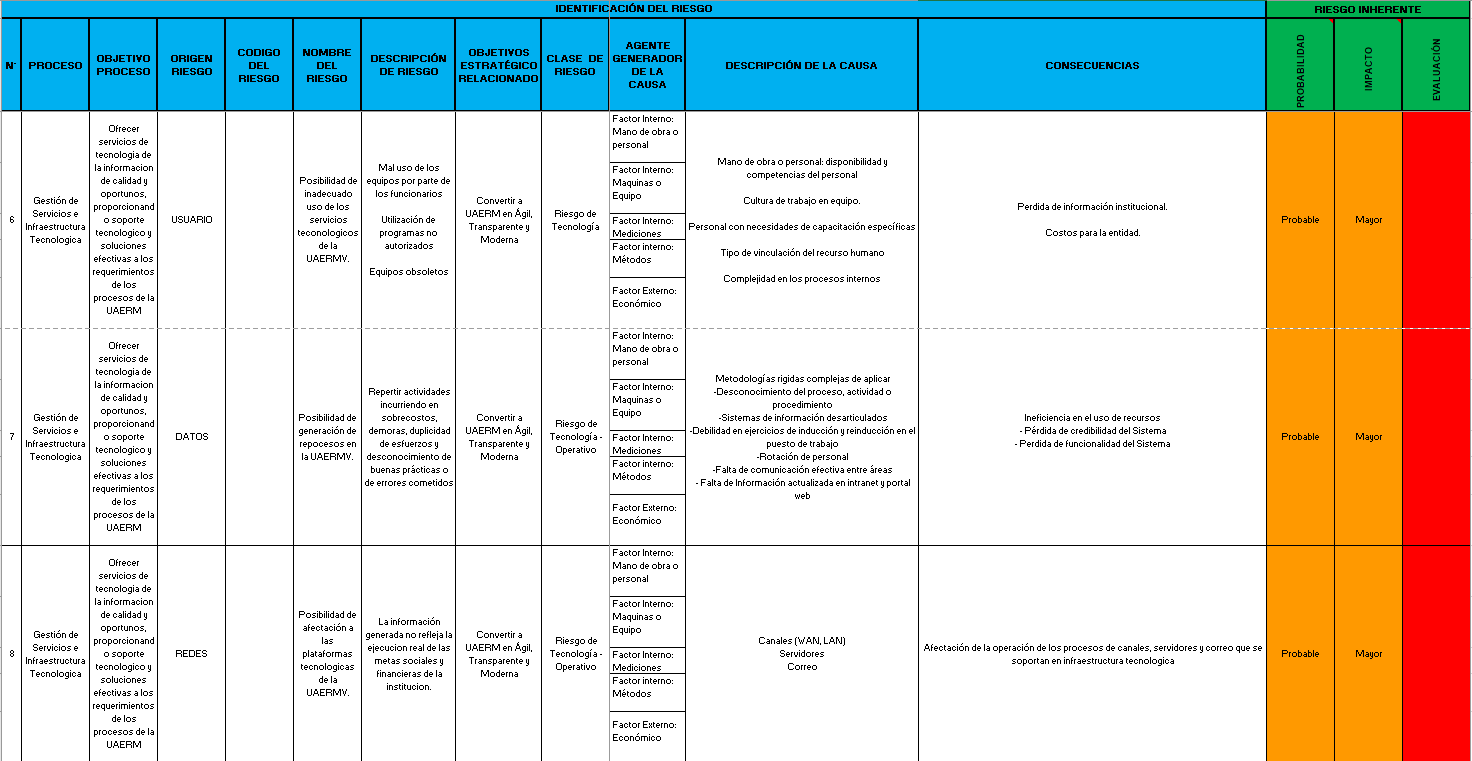
# GESTION DE RIESGOS

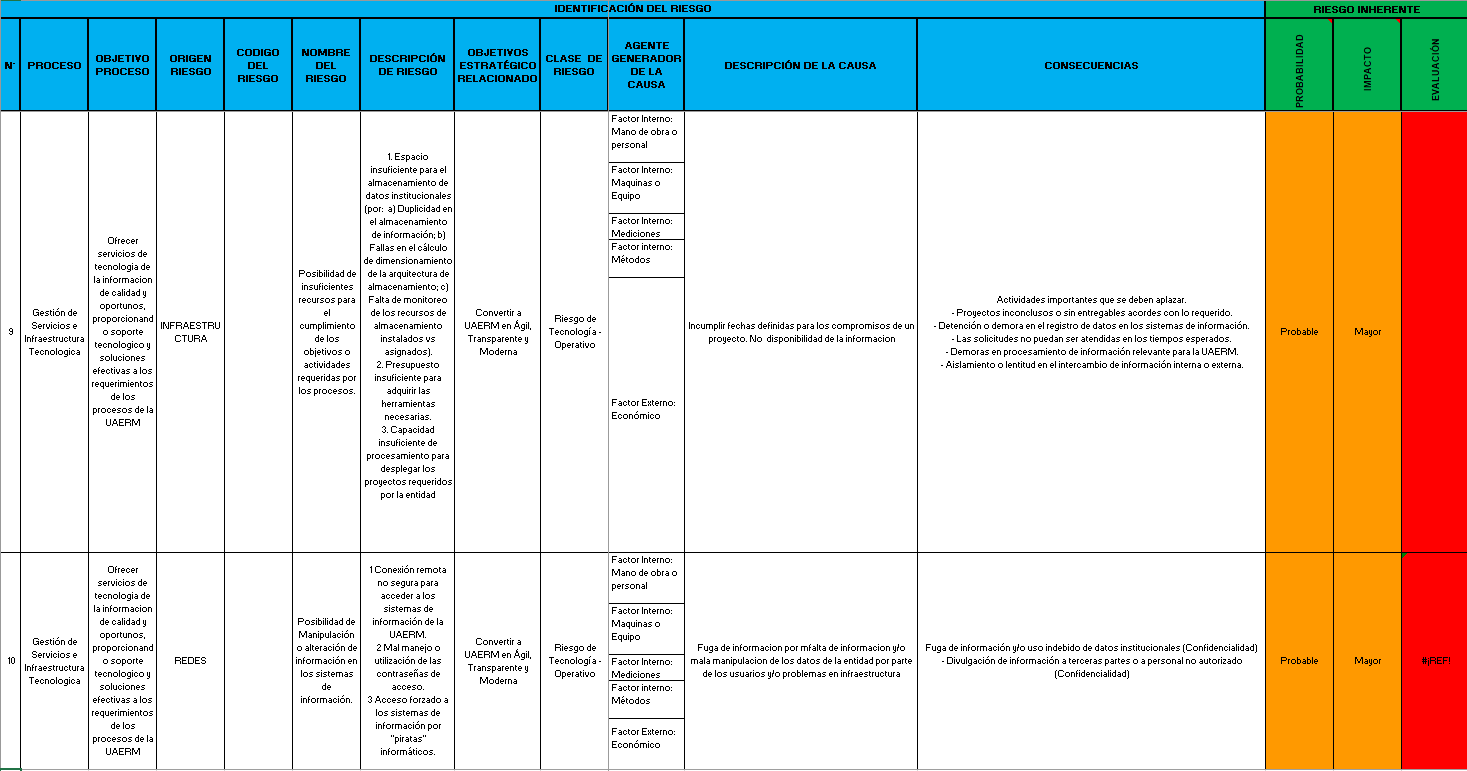
Los riesgos de seguridad y/o ciberseguridad deben formar parte de la estrategia general de la entidad por su indudable impacto en la sostenibilidad de la organización. Por consiguiente, el análisis de riesgos de seguridad y/o ciberseguridad debe alzarse hasta la alta dirección. Resulta esencial evaluar de forma detallada los riesgos por área: Tesorería, Tecnología etc., así como los objetivos que se pretenden alcanzar para tomar las decisiones sobre qué, dónde, y en qué medida destinar los recursos para su mitigación, lo que implica la identificación y secuenciamiento de las actividades, la asignación de recursos humanos, el empleo de recursos materiales, las necesarias asignaciones económicas y los métodos de control del progreso de las actividades. La planificación se realiza suponiendo que todo va a suceder de acuerdo con lo que se ha pensado y valorado desde el punto de vista tecnológico.











# POSIBLES ESCENARIOS DE CONTINGENCIA

* 1. Imposibilidad de Acceso a la Infraestructura.

Puede presentarse problemas de acceso a las instalaciones de la sede administrativa ubicadas en el Edificio Colciencias por temas de Orden Público, Catástrofes Naturales, Terrorismo y por incidentes en el edificio como incendios, inundaciones u otros por determinar.

Contingencia: Ante estos acontecimientos los funcionarios que manejan procesos críticos deben asistir a la sede de operaciones ubicada en la elvira para dar continuidad a sus actividades y permitid así la continuidad de las Operaciones de la entidad.

* 1. Imposibilidad de Acceso a los recursos informáticos.

Ya que la entidad cuenta con varios recursos informáticos, como medida de contingencia se planeó desde un principio manejar diferentes esquemas que permiten tener redundancia en los servicios misionales de la entidad.

Contingencia: En caso de presentarse se tienen servicios de acceso a la red de manera On premise y acceso a la arquitectura Cloud. Esto permite contar con opciones alternas para acceder a diferentes servicios.

Los servicios de Correo se pueden acceder desde cualquier lugar con acceso a internet mediante validación de credenciales del portal de Microsoft.

* 1. Acceso no autorizado a las instalaciones.

Acceso de personal ajeno a la entidad que ponga en riesgo la infraestructura.

Contingencia: Para el acceso a las instalaciones en la sede administrativa la entidad cuenta con servicios de vigilancia en un doble anillo. Por parte de la Administración del edificio existe contratado un servicio de vigilancia quien no permite el acceso a los ascensores del edifico sin haberse registrada en el área de Recepción. Además, la UMV tiene un contrato de vigilancia y un sistema de control de acceso en sus dos pisos. Esto garantiza en gran parte que el acceso a nuestras instalaciones está controlado.

En cuanto a las otras dos sedes de la entidad se tiene contrato vigente con empresa de Vigilancia que se encarga de registrar a los visitantes y a los colaboradores para el ingreso a sus instalaciones.

* 1. Acceso no autorizado a los sistemas de Información.

Ataques informáticos.

Contingencia: Los sistemas de información están protegidos por sistemas perimetrales de seguridad tanto a nivel de arquitectura On Premise como la Arquitectura Cloud. Además de esta protección se tiene un sistema de validación de credenciales para los usuarios que pueden ingresar a estas aplicaciones Misionales, con el fin de salvaguardar su operación y la información que se maneja.

* 1. Desastres Naturales

Terremoto, Inundaciones.

Contingencia: Ante un desastre Natural de grandes proporciones la entidad está en la capacidad de dar continuidad con los servicios de correo, información, SIGMA, Orfeo, SIGEP, Si-Capital y ecosistemas Web, ya que estos servicios se encuentran en arquitectura cloud.

La entidad no cuenta con un COA (Centro de Operaciones Alterno) y este debería ser implementado a más de 42 Kms en línea recta según las normas de las mejores prácticas.

* 1. Fallos de Personal Clave.

Renuncia de Personal.

Contingencia: La entidad en el área de Tecnología cuenta solo con 3 persona de planta, lo que evidencia un riesgo en la operación. Las personas claves de la operación son contratistas y aunque es un grupo interdisciplinario y multifuncional si es un riesgo que se debería mitigar con contrataciones directas o por encargo.

Una de las opciones que se maneja para este riesgo es la documentación de los procesos que se manejan en el repositorio documental con el que cuenta la entidad. Es importante aclarar que este repositorio está construido en una herramienta de Microsoft que tiene sus servidores en centros de datos de la más alta tecnología, que permiten un porcentaje alto de disponibilidad y de contingencia.

* 1. Fallos de Hardware.

Daño de equipos tipo servidor, equipos activos, equipos de almacenamiento y/o equipos de seguridad perimetral.

Contingencia: Ante los fallos de Hardware critico en el caso de Networking los switch Core de las sedes son propiedad del arrendador de las instalaciones. La obligación ante un fallo de estos equipos debe ser asumido por el arrendador.

Para el tema de servidores se está realizando un plan de cambio y modernización de infraestructura en la cual se adquieren equipos tipo servidor con sistemas internos redundantes en lo relacionado a sistemas eléctricos y de almacenamiento. Al igual se piden con garantía a 3 años 7X24X365 con atención en sitio en las primeras 4 horas después de reportar un daño físico.

También se realizó un plan de mantenimiento que cubre la infraestructura critica propia de la entidad para prevenir daños por mal funcionamiento que ocasionen tiempos muertos de operación.

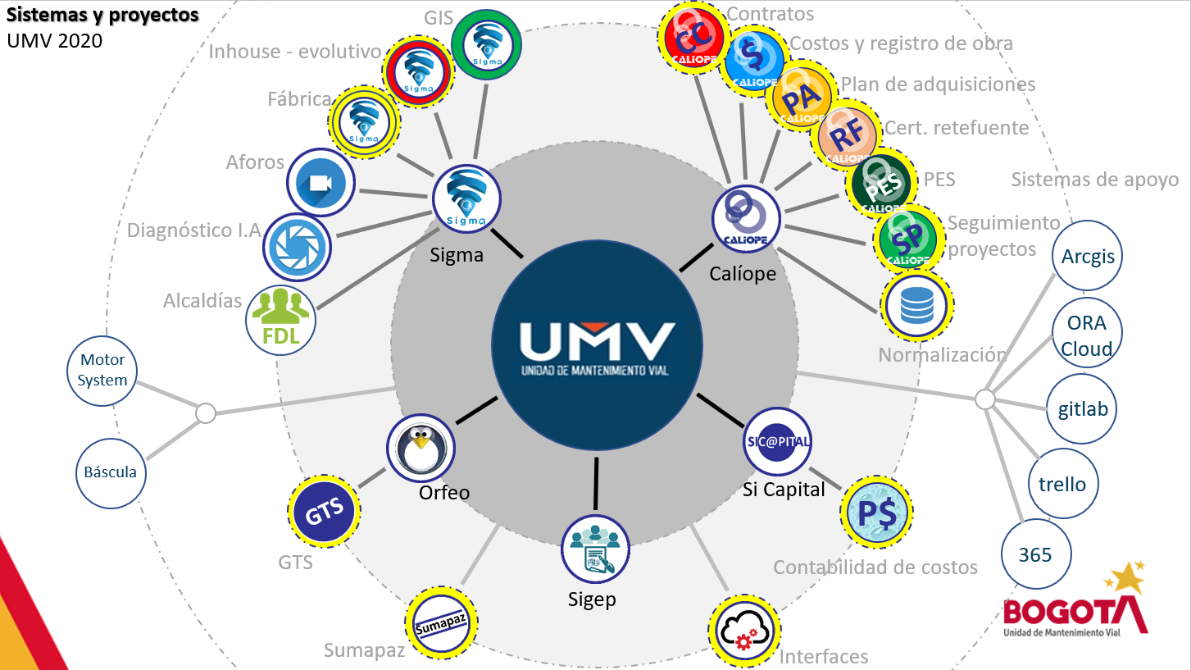
# SISTEMAS DE INFORMACIÓN

Las actividades más determinantes de la UMV están soportadas en la infraestructura tecnológica y en sus sistemas de información. Sistemas que por su importancia en la operación se han vuelto misionales y han permitido a la entidad dar un salto hacia la Transformación Digital.

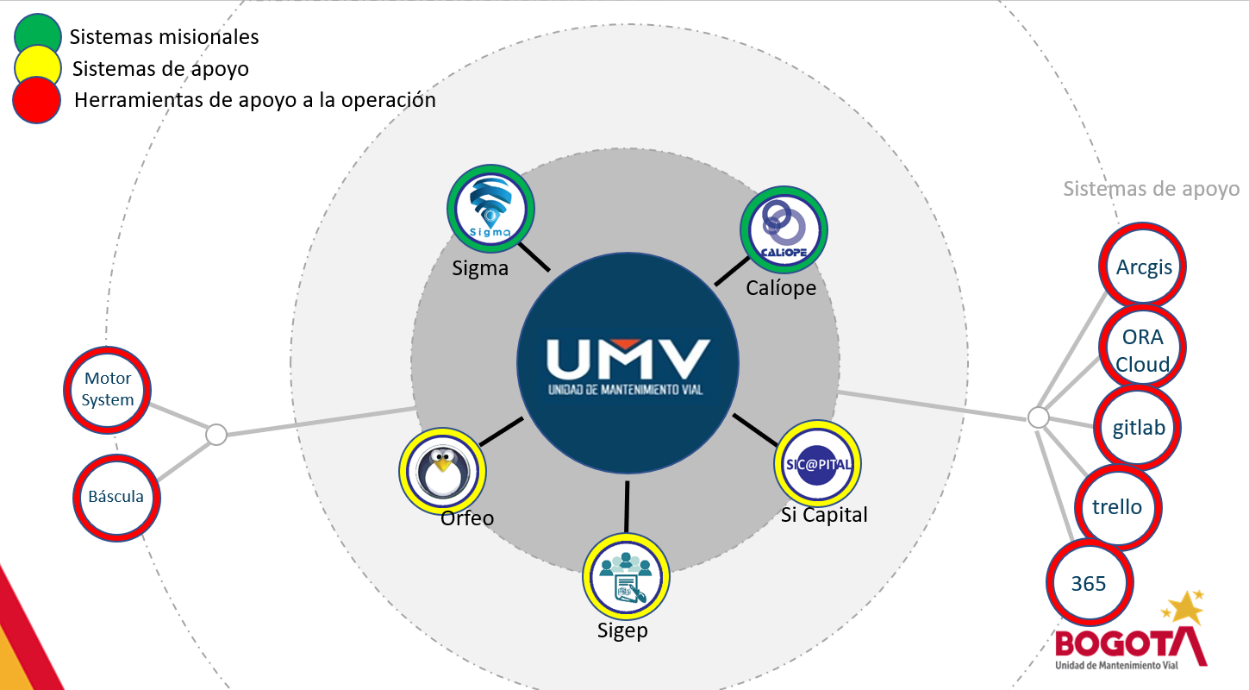
A continuación, un resumen de la Aplicación SIGMA catalogada como la más importante a nivel operativo de la entidad.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **INCIDENTE** | **TIPO** | **PROBABILIDAD** | **IMPACTO** | **DESCRIPCIÓN** | **CONTINGENCIA** | **AFECTA DISPONIBILIDAD DEL SERVICIO** | **TIEMPO ESTIMADO DE RESPUESTA** |
| 1 | Pérdida de códigos fuente | Fuente | Media | Alto | Pérdida de una funcionalidad parcial, o de la totalidad del código de la aplicación por daño en los repositorios o en una máquina de desarrollo | Al estar almacenado y versionado tanto en un repositorio, como en las máquinas de desarrolladores, se puede recuperar desde cualquier máquina de desarrollo y ejecutar el procedimiento de “Merge” de Gitlab | No | 4 horas |
| 2 | Pérdida de la base de datos | Datos | Baja | Alto | Caída de la base de datos | Se hacen backups diarios en nube y semanales en otro servidor. Se puede recuperar el último backup con pérdida de transacciones inferior a 8 horas. | Si | 4 horas |
| **ID** | **INCIDENTE** | **TIPO** | **PROBABILIDAD** | **IMPACTO** | **DESCRIPCIÓN** | **CONTINGENCIA** | **AFECTA DISPONIBILIDAD DEL SERVICIO** | **TIEMPO ESTIMADO DE RESPUESTA** |
| 3 | Daño en servicio de base de datos Oracle | Servicios o Infraestructura (nube) | Baja | Alto | Daño en el servicio de base de datos e la nube que proporciona Oracle | Hay una licencia local. Se puede montar la última copia de base de datos en local y apuntar las aplicaciones a esta base de datos, aunque afectaría velocidad. | Si | 8 horas |
| 4 | Daño en servidor front o back | Servicios o Infraestructura (nube) | Baja | Alto | Daño en la máquina virtual de los servidores, incluyendo un servicio o una aplicación de dichas máquinas. | Restablecer la máquina y los servicios en una nueva máquina virtual, subir nueva versión de la aplicación | Si | 4 horas |
| 5 | Caída de servicios geográficos de la Entidad | Servicios o Infraestructura (nube) | Baja | Alto | Daño en el servidor de Arcgis | Recuperación de backup, montaje en servidor de pruebas y apuntar las aplicaciones al servidor de pruebas | Si | 2 horas |
| 6 | Caída de servicios geográficos de IDU | Datos | Alta | Alto | Indisponibilidad de los servicios proporcionados por IDU | Aunque se está solicitando mesa de trabajo con IDU, no hay contingencia automatizada para este incidente. El tiempo de respuesta de IDU es inferior a 8 horas. Ya que los datos no son propiedad de la UMV, tampoco es posible manipularlos sin su autorización. | Parcial | 8 horas |

Los sistemas de información se grafican en el siguiente Diagrama



Y son considerados sistemas críticos que pueden afectar la operación de



6.1 SIGMA

Sistema de información misional de la Entidad, que centraliza e integra la información requerida para la adecuada gestión de pavimentos, relacionada con:

* + Formulación
  + Planeación
  + Programación
  + Ejecución
  + Seguimiento de la conservación de la malla vial local.
* Incluye artefactos para toma oportuna de decisiones sobre gestión de la conservación de las vías locales.
* Automatiza la coordinación entre las áreas que participan en la conservación de la malla vial local.
* Intercambia y publica información geográfica con otros actores del Distrito como el IDU y la Secretaría de Movilidad

BENEFICIOS

* Ahorrar costos en papelería
* Disminuir los tiempos de respuesta en cada flujo misional de la entidad
* Disponer información oportuna para toda la entidad (en tiempo real)
* Mejorar la calidad de los productos de cara a la ciudadanía
* Facilitar el trabajo de los funcionarios de la UMV

6.2 CALIOPE

Sistema de información que permite modelar flujos y captura propios de la misionalidad. Permite Integrar los flujos con Sigma, o los sistemas de apoyo.

* Pretende automatizar flujos de captura sin intervención del equipo de ingeniería.
* Permite generar reportes, informes o planillas a partir de plantillas en Word o Excel.
* Está diseñado para gestionar plantillas en los formatos oficiales de calidad de la UMV.
* Permite interfaz con el sistema Geográfico de la UMV (mapas y tableros de control).

BENEFICIOS

* Ahorrar costos en papelería
* Disminuir los tiempos de respuesta en cada flujo misional de la entidad.
* Disponer información oportuna para toda la entidad (en tiempo real).
* Integrar los demás sistemas de información con tecnología de punta.
* Centralizar los desarrollos de la entidad en una única herramienta.

6.3 SI-CAPITAL

El ERP Si-Capital es el sistema de soporte a los procesos financieros de la Entidad.

Este sistema es una adaptación del sistema de la Secretaría de Hacienda Si-Capital, ajustado a las necesidades de la UMV.

BENEFICIOS

* Ahorrar costos y tiempos a los usuarios
* Mantener a la Entidad al día en normas financieras vigentes
* Mejorar la calidad y confiabilidad de la información financiera

6.3 ORFEO

Soporta el proceso documental de la Entidad. En un futuro cercano soportará la gestión electrónica de documentos.

El sistema Orfeo permite realizar flujos documentales, borradores, radicaciones de entrada y salida, tanto para la ventanilla de radicación como para los funcionarios y colaboradores de la Entidad.

BENEFICIOS

* Ahorrar costos en papelería
* Disminuir los tiempos de respuesta al cliente interno
* Mejorar la calidad del proceso de PQRS
* Facilitar el trabajo de los funcionarios de la UMV

6.4 SIGEP

El sistema Sigep es un sistema diseñado para el Departamento Administrativo de la Función Pública DAFP, adoptado por la UMV para la liquidación del cálculo de la nómina y almacenamiento de históricos relacionados.

Actualmente es soportado por la empresa Heinsohn

BENEFICIOS

* Mejorar la calidad y confiabilidad de la información interna y externa
* Preservar los históricos de la entidad
* Disponer de herramientas tecnológicas de vanguardia para evitar la obsolescencia tecnológica
* Al estructurar los datos de los costos y gastos asociados a la nómina de la Entidad, se podrá realizar proyecciones y estudios de inversión en el personal

# INFRAESTRUCTURA

La UAERMV es una entidad distrital de Bogotá, encargada de implementar y mantener la malla vial local, la cual cuenta con tres (3) instalaciones ubicadas en la ciudad de Bogotá:

* Sede administrativa, ubicada en la Av. Cl. 26 No. 57- 41
* Sede Operativa, ubicada en la Cl. 22d No. 120-40 Fontibón
* Sede Producción, Ubicada en el parque minero industrial el “Mochuelo”

LA UAERMV cuenta con 410 usuarios que usan la red entre las diferentes sedes, accediendo desde equipos de escritorio, portátiles y dispositivos móviles a través de conexiones cableadas e inalámbricas, a servicios como navegación en internet, telefonía IP, servicios de impresión, aplicaciones locales y aplicaciones en la nube.

La infraestructura critica en los centros de datos de la entidad es la Siguiente:

Centro de Datos Piso 8 Sede Administrativa

* Servidor IBM xSeries 3550 M2.
* Servidor Thermaltake AD.
* Switch Core Xtreme.
* Switch de Borde Enterays y Cisco.
* Router Ztek ISP Internet.
* Equipo de Seguridad Perimetral Fortinet 100E.
* Tape Vault LTO IBM.
* Encloser IBM.
* Sistemas de UPS.
* Sistemas de AA.
* Equipo NVR.
* Encloser IBM.
* Sistemas de UPS.
* Sistemas de AA.
* Pantalla Monitoreo SISTEMA INTEGRADO DE SEGURIDAD ELECTRÓNICA Cámaras Análogas.

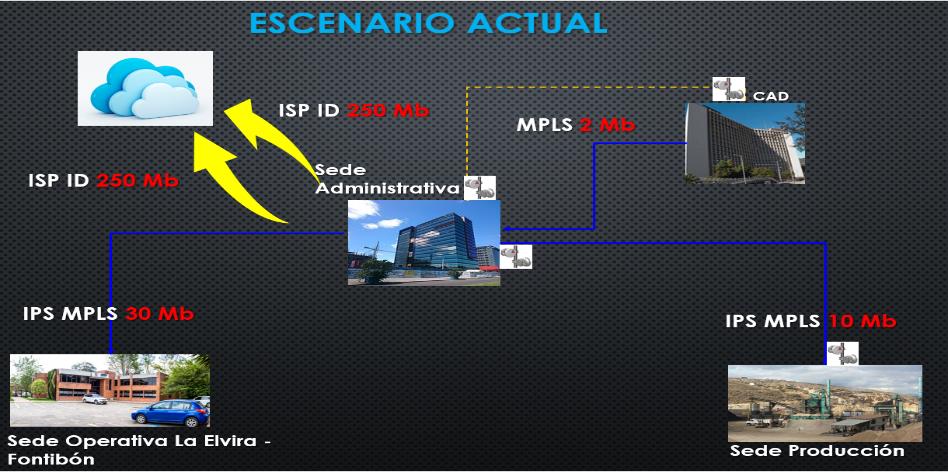
Centro de Datos Piso 7 Sede Administrativa

* Switch de Borde Enterays
* Switch de Borde Xtreme
* Sistema de UPS
* Sistema de AA
* Equipo NVR

Centro de Datos Sede Operativa

* Switch Core Xtreme
* Switch de Borde Cisco
* Switch de Borde 3com
* Sistema de UPS
* Sistema de AA
* Equipo NVR
* Servidor AD

Los canales de comunicaciones están centralizados en su sede principal, sin embargo, para atender una contingencia que ocurra en dicha sede se tiene planeado implementar canales pasivos de Internet en las sedes de producción y operación.



**CONTINGENCIA DE INFRAESTRUCTURA**

Dentro del plan de contingencia de la UMV se contempla que ante una eventualidad en su sede Administrativa se utilice un espacio físico en la sede de operaciones a modo de COA (Centro de Operaciones Alterno). Para esto es necesario contar con un canal a Internet desde esta sede. Este Canal será Pasivo – Activo y debe hacer el bypass en el momento que no se tenga conectividad con el canal principal MPLS que comunica las dos sedes.

Este COA también se puede utilizar para la sede de Producción ya que el esquema que se manejará será el mismo.

COA preparado para atender hasta 10 colaboradores designados previamente por la entidad para encargarse de las actividades que pueden afectar la continuidad de las operaciones.

# CENTRO DE DATOS

En la actualidad la entidad cuenta con (3) Centros de Datos, dos (2) ubicados en la sede administrativa principal y uno (1) en la sede operativa La Elvira. Los centros de cómputo de la sede administrativa tienen una categoría de Tier 1 ya que:

* El servicio puede interrumpirse por actividades planeadas o no planeadas.
* No hay componentes redundantes en la distribución eléctrica y de refrigeración.
* No tienes suelos elevados, generadores auxiliares.
* Tiempo medio de implementación, 3 meses.
* La infraestructura del Centro de Datos deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. (PRO, s.f.)

En estos Centro de Datos de la sede administrativa se tienen reunidos los servicios de Internet de las demás sedes, servicios de información y de configuración.

Están conformados por Rack de equipos y de comunicaciones y cuentan con sistemas de Refrigeración y respaldo eléctrico. Además, cuentan con control de acceso y bitácoras de asistencia que permiten regular y restringir el acceso a personal no autorizado.

Estos centros de cómputo están ubicados en los pisos 7 y 8 de la entidad y se comunican por un Backbone de fibra que permite la comunicación entre los usuarios de cada piso a cada centro de cómputo.

El Centro de Datos del 8 piso se puede considerar como el Centro de Datos principal, ya que en él se encuentran ubicados los equipos críticos de la sede administrativa. Entre ellos están los equipos de seguridad perimetral (Firewall), los equipos servidores On premise que dan las funcionalidades de acceso a los servicios de red, equipos de conectividad interna, equipos de conectividad con las demás sedes, equipos de conectividad a internet y los equipos servidores físicos donde se virtualizan varios servidores de respaldo a los servidores de Nube.

El Centro de Datos del piso 7 tiene alojados los equipos de conectividad interna y el sistema de CCTV (Sistema Integrado De Seguridad Electrónica) de la sede administrativa.

En el manejo de riesgo se detallarán los planes de contingencia para los equipos de estos dos centros de datos.

# ARQUITECTURA CLOUD

Una de las ventajas de tener los servicios de Oracle cloud es contar con la opción de realizar copias de seguridad de las instancias y discos de los diferentes servidores que allí se tienen, tanto manual como automáticamente. En cuanto a disponibilidad de la infraestructura de Oracle cloud los dominios de disponibilidad están aislados entre sí, son tolerantes a fallas y es muy poco probable que fallen simultáneamente. Debido a que los dominios de disponibilidad no comparten infraestructura como energía o refrigeración, o la red de dominio de disponibilidad interna, es poco probable que una falla en un dominio de disponibilidad dentro de una región afecte la disponibilidad de los otros dentro de la misma región.

Los dominios de disponibilidad dentro de la misma región están conectados entre sí por una red de baja latencia y alto ancho de banda, lo que le permite proporcionar conectividad de alta disponibilidad a Internet y local, y construir sistemas replicados en disponibilidad múltiple dominios para alta disponibilidad y recuperación ante desastres.

Otros servicios con los que cuenta la entidad alojados en Arquitectura Cloud son el correo institucional, el repositorio documental y el almacenamiento de información privada de los usuarios. Este servicio está contratado con la empresa Microsoft en un plan E1.

Dicha compañía cuenta con Centros de Datos tipo Tier 4, con generaciones de última tecnología en cuanto equipos de cómputo tipo servidor y almacenamiento y planes de contingencia y redundancia de alta calidad que pueden ofrecer disponibilidades de servicios de más del 99.7%.

La información que se aloja en los servidores de Microsoft es almacenada en varios centros de datos ubicados en diferentes zonas a nivel mundial lo que permite tener servicios en alta disponibilidad y con altos estándares de seguridad.

En la siguiente figura podemos observar la ubicación Geográfica de los Centros de Datos de Microsoft donde tiene la UMV los servicios anteriormente mencionados.



Adicional a esto se encuentra el documento intituladoBackup and disaster recover for Azure applications que se puede consultar en el siguiente Link**.**

<https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency/backup-and-recovery>

# POLÍTICAS DE SEGURIDAD

# 10.1 PROPÓSITO

La implementación de este documento de POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES, busca reducir la materialización de los riesgos, respecto a una amplia gama de amenazas que pueden ser accidentales o intencionales, estableciendo normas claras respecto de su divulgación, modificación o eliminación de la información considerada crítica sensible para el logro de los objetivos misionales de la Unidad, y proveer a la UAERMV de un documento formal en donde se contengan las buenas prácticas para una administración adecuada de los recursos tecnológicos, soporte a Usuarios, seguridad de la información y las comunicaciones de la Unidad.

# 10.2 POLÍTICAS ESPECIFICAS.

La UAERMV para el fortalecimiento de la POLÍTICA GENERAL DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIÓN, elaborará las siguientes políticas puntuales con el objetivo de proteger los activos, siguiendo como guía la norma ISO 27001:2013:

1. Políticas de navegación en internet.
2. Políticas de tratamiento y manejo de datos personales.
3. Políticas de seguridad de activos de información.
4. Política de protección y respaldo de la información.
5. Política del escritorio limpio y bloqueo de pantalla.
6. Política de seguridad para gestión de contraseñas
7. Política de responsabilidades operacionales y control de cambios.
8. Política de protección contra software nocivo.
9. Política de gestión de riesgos.
10. Política para el buen uso del correo electrónico institucional.
11. Política de registro histórico de actividades (log).
12. Política sobre el uso de equipos de cómputo y el acceso a la red.

# ROLES Y RESPONSABILIDADES

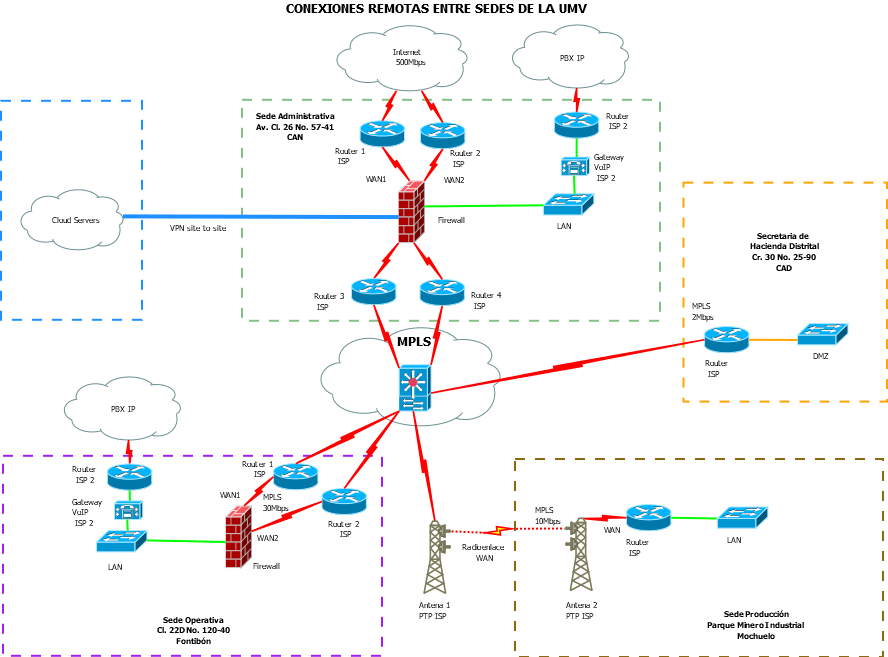
|  |  |  |
| --- | --- | --- |
| **ROL** | **RESPONSABLE** | **MECANISMOS** |
| Coordinador Plan de continuidad. | * Líder de Tecnología. * Líder de Infraestructura. * Líder de Desarrollo * Secretaría General. | Para crear y documentar el plan:   * Mesas de trabajo. * Análisis de la información. * Metodología de riesgos. * Inclusión en el plan de acción anual de las actividades. |
| Aprobación, Socialización y Pruebas del Plan de Continuidad. | * Comité Institucional Administrativo. * Grupo de Comunicaciones. * Grupo de Tecnología. | * Sesiones ordinarias y extraordinarias del Comité. * Boletín de noticias/intranet. * Sesiones de inducción y reinducción-Simulacros. |
| Activación del Plan de Emergencia y Plan de Restablecimiento. | * Comité de Crisis. | * Declaración escrita. * Comunicación telefónica. * Reuniones extraordinarias. |
| Restablecer Prestación de Servicio/Información. | * Secretaría General. * Líder de Tecnología. * Líder de Infraestructura * Líder de Desarrollo. | * Mesas de trabajo. * Análisis y pruebas. * Inspección y verificación. * Comunicación con los grupos de valor. |

# CONTROL DE ACCESO

Garantizamos el control de acceso físico con equipos biométricos en los Centros de Datos de las sedes Administrativa y de Operaciones de la entidad. Estos biométricos se administran desde un servidor de seguridad del cual se audita y se toma evidencia de privilegios de ingreso, también contamos con una planilla donde la persona que ingrese debe diligenciar para especificar el motivo del ingreso y tiempo utilizado.

# CANALES DE COMUNICACIÓN

Las conexiones entre sedes se realizan usando tecnologías de red como la conmutación de etiquetas multiprotocolo (MPLS) a través de un proveedor de servicios de internet (ISP) de tipo TIER III, garantizando disponibilidad mínima del servicio del 99,7%, con el cual se tiene implementado toda la infraestructura de canales de datos e internet.



La Sede Administrativa, es la sede principal, la cual alberga en uno de sus centros de datos los dispositivos de telecomunicaciones que prestan el servicio de internet y MPLS con el resto de sedes. Esta sede cuenta con dos (2) canales de internet dedicados de doble anillo de fibra óptica, con anchos de banda de 250Mbps cada uno, configurados en alta disponibilidad n+1 activo-activo, para un total de 500Mbps de ancho de banda disponible.

Además, cuenta con el servicio de telefonía IP con otro ISP, el cual posee un canal de voz para la conexión con la PBX virtual en la nube del ISP. Por otra parte, desde esta sede establece una conexión de red privada virtual (VPN) con la nube donde se encuentran los servicios misionales, la cual tiene la propiedad para ser configurada en alta disponibilidad.

La Sede Operativa, se conecta con la sede administrativa y al servicio de internet, a través de dos (2) canales MPLS redundantes configurados en n+1 activo-activo, con anchos de banda de 20Mbps y 10Mbps, para un total de 30Mbps de ancho de banda disponible. Además, cuenta con un servicio de telefonía IP y un canal de voz, ambos independientes al de la sede administrativa, para conectarse con la PBX virtual en la nube del ISP.

La sede de Producción se conecta con la sede administrativa y al servicio de internet, a través de un canal MPLS por radioenlace punto a punto que posee un ancho de banda de 10Mbps. Las extensiones telefónicas de esta sede se conectan directamente con la PBX virtual en la nube pública del ISP a través del servicio de internet.

# COPIAS DE RESPALDO.

Actualmente la entidad está realizando copias de seguridad a medios digitales externos. Discos Duros. Ya que el sistema de copia a Cintas no está respondiendo de manera satisfactoria por un daño en el servidor físico que tiene este rol.

Si embargo es importante resaltar que como medidas de contingencia para este caso se tiene configurado en cada equipo de cómputo la característica de versiones anteriores que permiten la salvaguarda de la información de mis documentos y escritorio de cada usuario.

Como segundo anillo de protección de la información de los usuarios y una forma de copia de seguridad se tiene implementado la configuración de la herramienta tecnológica OneDrive. Dicha herramienta se utiliza como medio de almacenamiento de la información de los usuarios y cuenta con los planes de contingencia implementados por la compañía Microsoft.

Para los equipos críticos se han creado imágenes a Disco Duro que permita en caso de daño o perdida poder restablecer los servicios en poco tiempo.

La información misional es almacenada en un sistema File server que se encuentra en la Nube de Oracle y que cuenta con todas las medidas de contingencia documentada en el numeral 9. ARQUITECTURA CLOUD.

La entidad se encuentra en la parte final del proceso de adquisición de un servidor de Archiving que permita el almacenamiento y copia de información en medios magnéticos (Cintas) por medio del equipo LTO con que cuenta el área de Infraestructura.

Para el aseguramiento de la información se establecen políticas de seguridad y se están implementando planes para el bloqueo de puertos USB que impida la conexión de medios externos y la propagación de software malicioso en los equipos de cómputo de la entidad.

Además, se realiza backup de los equipos activos y de seguridad de manera semanal para prevenir algún daño en la configuración que pueda afectar la continuidad de la entidad.

# SISTEMAS DE SEGURIDAD PERIMETRAL

En la Sede Administrativa, para la protección de las conexiones de red se cuenta con un (1) firewall Fortigate 100E, este establece las reglas de acceso, el enrutamiento entre las diferentes redes internas de usuarios, servidores y las redes externas, además posee perfiles de seguridad activos como antivirus, filtro web, filtro DNS, sistema de prevención de intrusos, antispam, firewall de aplicaciones web, control de aplicaciones.

En la sede Operativa, se cuenta con un (1) firewall Fortigate 100D, el cual establece el enrutamiento, las reglas de acceso y el filtrado mediante los perfiles de seguridad, apoyando así el trabajo realizado por el firewall de la sede administrativa.

La sede de Producción es cubierta por el firewall de la sede administrativa.

Los equipos de cómputo de los usuarios cuentan con sistemas operativos, antivirus, licenciados y actualizados, los cuales son administrados desde una consola de antivirus centralizada en la sede administrativa.

En las sede Administrativa y Operativa se cuenta con un control de acceso mediante dispositivos de lectura biométrica tanto para el acceso a las sedes como los centros de datos, apoyado por personal de la empresa de vigilancia.

La conexión a la red wifi se encuentra segmentada por VLAN corporativa e invitados, agregando un portal cautivo a la conexión de invitados.

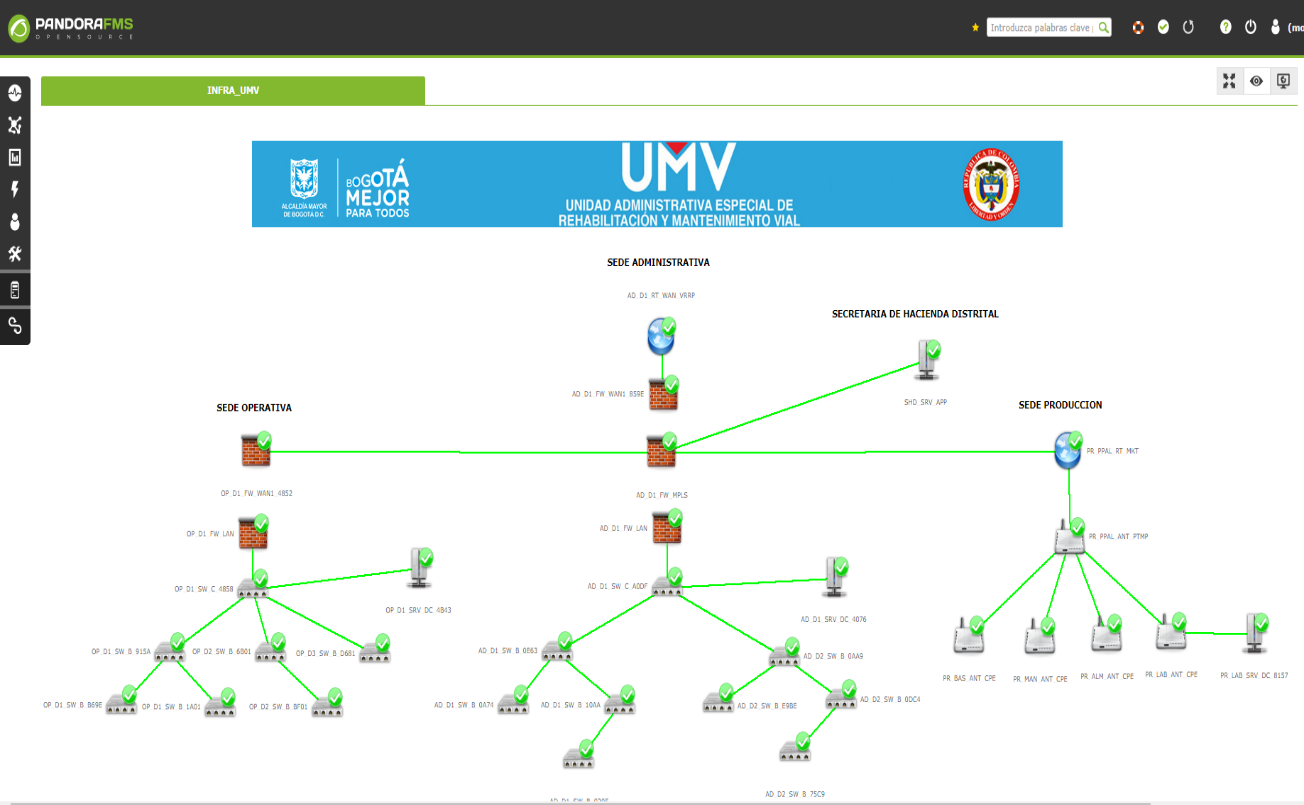
# INVENTARIOS DE INFRAESTRUCTURA TI

Los temas de inventario de la entidad de las diferentes áreas son administrados y gestionados por el departamento de Almacén. Sin embargo, el área de tecnologías cuenta con un inventario de toda la infraestructura tecnológica que ha tomado como base para los planes de Mantenimiento, Licenciamiento e instalación y configuración de aplicaciones de seguridad (Antivirus). Se tiene un inventario de infraestructura critica que se monitorea todos los días por medio de una herramienta tecnológica Web. El archivo de inventarios se intitula GSIT-FM-002-V3-Formato-Inventario. Este inventario se actualiza constantemente. Este documento como el de las hojas de vida de los equipos tecnológicos se encuentra ubicado en el Gestor de contenidos con el que cuenta la entidad. Dicho Gestor está en Arquitectura Cloud y cuenta con medidas de contingencia entregadas por el fabricante Microsoft.

# MONITOREO

La entidad cuenta con una herramienta tecnológica tipo web de Monitoreo que realiza seguimiento a la infraestructura critica de la UMV.

La herramienta es Pandora y además de realizar el monitoreo de la infraestructura envía alarmas cuando un equipo presenta una salida del sistema o una falla que no le permita operar normalmente.



Esto permite al área de infraestructura reaccionar ante una posible contingencia informática ya que como se explica anteriormente se envía un correo alarmando ante una eventualidad de falla y permite reaccionar de inmediato para dar continuidad a la operación.

Además de esta herramienta los sistemas perimetrales de seguridad también monitorean los canales de comunicación y permiten detectar fallas en el servicio, lo que posibilita atender estos incidentes en tiempos aceptables para la continuidad de la Operación.

# SISTEMAS WEB

La entidad tiene contratado un sistema hosting de producción externo y uno de respaldo en Oracle cloud.

Para temas de contingencia en caso de fallo de este servicio el web master de la entidad hace entrega por medio magnético de las copias de respaldo de la base de datos y de archivos mensualmente del ecosistema web.

Como medida adicional de contingencia se tiene habilitado un servidor con el protocolo ftp de consulta interna en la sede administrativa para que sean allí almacenados de manera redundante las copias de respaldo del ecosistema Web.

En caso de caída de hosting se restablecerán los backups con los últimos cambios en el hosting local OCI Classic.

# SISTEMA DE RESPALDO ELÉCTRICO

Las sedes Administrativa cuenta con respaldos eléctricos centralizados, ubicados en el centro de datos de cada piso mediante el uso de UPS online (sistema ininterrumpido de energía) y bancos de batería de alta capacidad con aproximadamente 30 minutos de autonomía, los cuales además de alimentar la operación del centro de datos, alimenta la operación de los puestos de trabajo de los usuarios. Adicionalmente, el edificio cuenta con una planta eléctrica, que el personal de mantenimiento activaría en caso de una falla eléctrica, procedimiento que se encuentra descrito en el documento de contingencia eléctrica del edificio.

La sede operativa también cuenta con respaldos eléctricos (UPS online) centralizados en los centros de datos y que alimentan los centros de datos y los puestos de trabajo.

# SISTEMA INTEGRADO DE SEGURIDAD ELECTRÓNICA (CCTV)

La entidad cuenta con sistemas de circuito cerrado de televisión en las tres (3) sedes, cuyos NVR (Grabadores de video de Red) se encuentran alojados en los centros de datos, cada sede cuenta con un cuarto de monitoreo, los cuales son custodiados por personal de la empresa de vigilancia.

La sede administrativa cuenta con 29 cámaras de seguridad, 83 cámaras en la sede operativa y 68 cámaras en la sede de producción con.

Es de aclarar que los sistemas SISTEMA INTEGRADO DE SEGURIDAD ELECTRÓNICA están administrados por la compañía de vigilancia que tiene asignado el actual contrato. Y que estos equipos de SISTEMA INTEGRADO DE SEGURIDAD ELECTRÓNICA fueron suministrados por el Arrendador de las instalaciones

# PRUEBAS

Para el modelo de pruebas se está realizando un plan que contemple pruebas en las áreas de aplicaciones y de infraestructura.

Se realizarán pruebas a nivel de redundancia de clúster en servidores de la arquitectura Cloud, Restauración de máquinas virtuales, pruebas de redundancia en servidores y en canales de comunicación.

Para los temas de Networking al momento no se pueden realizar pruebas ya que no se cuenta con los equipos de alta disponibilidad.

# RIESGOS DE SALUD OCUPACIONAL Y/O SISTEMAS DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO

Para la gestión de las eventualidades en materia de Riesgos de Salud Ocupacional y/o Sistemas de Gestión Seguridad y Salud en el Trabajo perteneciente a la Gestión del Talento Humano se cuenta con las siguientes herramientas:

* + - 1. **GTHU-S-DI-003** Política del Sistema de Gestión Seguridad y Salud en el trabajo.
      2. **GTHU-S-FM-019** Notificación de la Política de Alcohol y Drogas
      3. **GTHU-S-DI-005** Reglamento de higiene y seguridad industrial.
      4. **AII-PL-001** Plan institucional de Respuesta de Emergencia.
      5. **GTHU-S-DI-006** Planes operativos normalizados PON´S ¿Cómo actuar en caso de emergencia?
      6. **GTHU-S-DI-004** Matriz de Identificación de Peligros, Evaluación y Valoración de Riesgos.
      7. **THU-S-PR-001** Procedimiento para investigación de incidentes y accidentes de trabajo.
      8. **GTHU-S-DI-004** Procedimiento Solicitud y entrega Equipo de Protección Personal.

# RIESGOS DE GESTIÓN AMBIENTAL

En materia de Riesgos de Gestión Ambiental se cuenta con las siguientes herramientas:

1. **GAM-PL-005** Plan Institucional de Gestión Ambiental – PIGA, debidamente concertado con la Secretaría Distrital de Ambiente.
2. **IMVI – DI - 003** Manual de Buenas Prácticas Ambientales.
3. **GAM-PR-002** Procedimiento de Identificación y valoración de los Aspectos e Impactos Ambientales.
4. **GAM-PL-005** Plan de Contingencia para Manejo de Derrames de Hidrocarburos

# ANÁLISIS DE RIESGO Y VULNERABILIDAD

## OBJETIVOS ESPECÍFICOS

Los objetivos específicos del análisis de riesgos son los siguientes:

* Identificar y analizar los diferentes factores de riesgo que involucren peligros potenciales que podrían afectar las condiciones socioambientales de la Organización.
* Establecer con fundamento en el análisis de riesgos, las bases para la preparación del Plan de Emergencia y Contingencias.

**METODOLOGÍA ANÁLISIS DE RIESGOS POR COLORES**

En forma general y cualitativa permite desarrollar análisis de amenazas y análisis de vulnerabilidad de personas, recursos y sistemas y procesos, con el fin de determinar el nivel de riesgo a través de la combinación de los elementos anteriores, con códigos de colores.

Asimismo, es posible identificar una serie de observaciones que se constituirán en la base para formular las acciones de prevención, mitigación y respuesta que contemplan los planes de emergencia.

**ANÁLISIS DE AMENAZA**

**Amenaza:** condición latente derivada de la posible ocurrencia de un fenómeno físico de origen natural, socio-natural o antrópico no intencional, que puede causar daño a la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada.

Dependiendo de la actividad económica de la organización se pueden presentar diferentes amenazas, las cuales se pueden clasificar en: naturales, antrópicas no intencionales o sociales. A continuación, se dan ejemplos de posibles amenazas:

**Identificación de amenazas**

| **NATURAL** | **ANTRÓPICAS NO INTENCIONALES** | **SOCIAL** |
| --- | --- | --- |
| • Incendios Forestales  • Geológicos: se divide en Endógenos y Exógenos: Fenómenos de Remoción en Masa deslizamientos, (deslizamientos, derrumbes, caída de piedra, hundimientos.)  • Movimientos Sísmicos  • Eventos atmosféricos (vendavales, granizadas, tormentas eléctricas, etc.)  • Inundaciones por desbordamiento de cuerpos de agua (ríos, quebradas, humedales, etc.).  • Avenidas torrenciales.  • Otros | • Incendios (estructurales, eléctricos, por líquidos o gases inflamables, etc.)  • Perdida de contención de materiales peligrosos (derrames, fugas, etc.)  • Explosión (gases, polvos, fibras, etc.)  • Inundación por deficiencias de la infraestructura hidráulica (redes de alcantarillado, acueducto, etc.)  • Fallas en sistemas y equipos  • Otros | • Comportamientos no adaptativos por temor  • Accidentes de Vehículos  • Accidentes Personales  • Revueltas / Asonadas  • Atentados Terroristas  • Hurtos  • Otros |

Una vez identificadas las amenazas se procedió a evaluarlas, combinando el análisis probabilístico, con el comportamiento físico de la fuente generadora, utilizando información de eventos ocurridos en el pasado y se calificó de forma cualitativa con base en la siguiente escala:

POSIBLE: NUNCA HA SUCEDIDO Color Verde.

PROBABLE: YA HA OCURRIDO Color Amarillo.

INMINENTE: EVIDENTE, DETECTABLE Color Rojo.

**ANÁLISIS DE VULNERABILIDAD**

Luego de conocer la naturaleza de las amenazas de la **Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial,** se realizó un inventario de recursos internos y externos, con los que se cuenta para minimizar los efectos de una emergencia y atender correctamente la situación de peligro.

De acuerdo con lo anterior, se procedió a determinar la vulnerabilidad[[3]](#footnote-4), para su análisis se incluyeron los elementos sometidos al riesgo tales como:

|  |  |  |
| --- | --- | --- |
| 1. **PERSONAS** | 1. **RECURSOS** | 1. **SISTEMAS Y PROCESOS** |
| Gestión organizacional  * Capacitación y entrenamiento * Características de seguridad (dotación) | * Suministro * Edificación * Equipos | * Servicios públicos * Sistemas alternos * Sistemas de recuperación |

Cada uno de los anteriores aspectos se calificó así:

|  |  |
| --- | --- |
| **PUNTAJE** | **VALORACIÓN** |
| **1.0** | **SI.** Se cuenta con suficientes elementos |
| **0.5** | **PARCIAL.** Se cuenta parcialmente con los elementos o están en proceso de consecución |
| **0.0** | **NO.** Cuando se carece completamente o no se cuenta con recursos |

**Interpretación de la Vulnerabilidad por cada aspecto**

|  |  |
| --- | --- |
| **Calificación** | **CONDICIÓN** |
| **Bueno** | Si el número de respuestas se encuentra dentro el rango 0,68 a 1 |
| **Regular** | Si el número de respuestas se encuentra dentro el rango 0,34 a 0,67. |
| **Malo** | Si el número de respuestas se encuentra dentro el rango 0 a 0,33. |

Una vez calificado cada uno de los elementos se procedió a sumarlos y determinar el grado de vulnerabilidad tanto en las personas, recursos, sistemas y procesos de la siguiente manera:

|  |  |  |  |
| --- | --- | --- | --- |
| **PUNTAJE** | **INTERPRETACION** | **COLOR** | |
| **0.0 - 1.0** | **Alta** | **Rojo** |  |
| **1.1 - 2.0** | **Media** | **Amarilla** |  |
| **2.1 - 3.0** | **Baja** | **Verde** |  |

**NIVEL DE RIESGO**

**Riesgo**: el daño potencial que, sobre la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada, pueda causarse por la ocurrencia de amenazas de origen natural, socio-natural o antrópico no intencional, que se extiende más allá de los espacios privados o actividades particulares de las personas y organizaciones y que por su magnitud, velocidad y contingencia hace necesario un proceso de gestión que involucre al Estado y a la sociedad.

Una vez identificadas, descritas y analizadas las amenazas y para cada una, desarrollado el análisis de vulnerabilidad a personas, recursos y sistemas y procesos, se procede a determinar el nivel de riesgo que para esta metodología es la combinación de la amenaza y las vulnerabilidades utilizando el diamante de riesgo que se describe a continuación:

**Diamante de Riesgo**

PERSONAS

AMENAZA

SISTEMAS Y PROCESOS

RECURSOS

**ANÁLISIS DE AMENAZAS GLOBAL**



**ANÁLISIS DE VULNERABILIDAD GLOBAL EN LOS RECURSOS**



**ANÁLISIS DE VULNERABILIDAD GLOBAL EN LOS SISTEMAS Y PROCESOS**





|  |  |
| --- | --- |
| **NÚMERO DE ROMBOS** | **INTERPRETACIÓN** |
| **3** ó **4** rombos en **rojo** | Significa que los valores que representan la vulnerabilidad y la amenaza están en su punto máximo para que los efectos de un evento representen un cambio significativo en la comunidad, economía, infraestructura y el medio ambiente, con un porcentaje de incidencia entre el **75%** al **100%.** |
|  |
| **RIESGO ALTO** |
| **1** a **2** rombos **rojos** ó  **4** **amarillos** | Lo cual significa que los valores que representan la vulnerabilidad son altos o la amenaza es alta, también es posible que 3 de todos los componentes son, calificados como medios, por lo tanto las consecuencias y efectos sociales, económicos y del medio ambiente pueden ser de magnitud, pero se espera sean inferiores a los ocasionados por el riesgo alto, con un porcentaje de incidencia entre el **50%** al **74%.** |
|  |
|  |
| **RIESGO MEDIO** |
| **1** a **3** rombos **amarillos** y los restantes **verdes** | Lo cual significa que la vulnerabilidad y la amenaza están controladas. En este caso se espera que los efectos sociales, económicos y del medio ambiente representen perdidas menores, con un porcentaje de incidencia entre el **25%** al **49%.** |
|  |
|  |
| **RIESGO BAJO** |

**ANALISIS DE RIESGOS Y RECOMEDACIONES**

Las siguientes son algunas recomendaciones, teniendo en cuenta el Análisis de Vulnerabilidad de la Unidad:

**Gestión Organizacional**

* La divulgación de la política de emergencias, donde se indiquen los lineamientos de emergencia.
* Conformar, capacitar y entrenar al esquema organizacional (brigadas, SCI), bajo el modelo Sistema Comando de Incidentes.
* Promover la participación de los trabajadores, en programas de preparación de emergencias.
* Establecer relaciones de ayuda mutua con el comité local de emergencias.
* Divulgar el plan de emergencias y plan de evacuación a todo el personal de la Unidad.
* Desarrollar e implementar instrumentos de inspección, para identificar condiciones inseguras en las diferentes áreas.
* Desarrollar e implementar folletos, como material de difusión en temas de prevención y control de emergencias dirigida a visitantes y trabajadores de la Unidad.
* Socializar el plan de evacuación a todo el personal de la Unidad y visitantes.
* Definir un coordinador por área y darlo a conocer a todo el personal de la Unidad.
* Realizar simulacros por lo menos una vez al año. Llevar registro del ejercicio.
* Actualizar el plan de emergencias anualmente y articularlo con el del edificio.

**Capacitación y Entrenamiento**

* Fortalecer sus competencias mediante capacitaciones y ejercicios simulados, frente a los riesgos propios de la Unidad.
* Desarrollar e implementar folletos o carteleras con información en temas de prevención y respuesta a emergencias.
* Incluir en las inducciones, capacitación en temas de gestión del riesgo. Llevar registro.
* Realizar divulgación del plan de emergencias a todo el personal.

**Características de Seguridad**

* Se sugiere llevar lista del personal flotante, con datos como: fecha, hora de ingreso, nombres completos, número de cédula, EPS, ARL, nombre de una persona a quién se le puede avisar en caso de emergencia y su número de teléfono, persona a quién visita y hora de salida.
* El personal de las Brigadas de Emergencias debe contar con un distintivo que permita su rápida identificación en caso de emergencia. La identificación debe ser visible y en colores llamativos sin que esto sea un indicativo para aumentar los riesgos propios de la Unidad, a su vez debe contar con elementos de protección personal para la respuesta a emergencias (guantes, kit de primeros auxilios personal, etc.). Esta identificación se debe portar en todo momento.

1. TIER – Norma que describe los criterios para diferenciar las 4 clasificaciones de topología de infraestructura de sitio [↑](#footnote-ref-2)
2. TIA 942 - Guía para diseñadores e instaladores de centros de datos [↑](#footnote-ref-3)
3. VULNERABILIDAD: Entendida como la condición interna de un sujeto o sistema expuesto a una amenaza, que por su predisposición intrínseca puede ser susceptible a ser afectado sufriendo una perdida. [↑](#footnote-ref-4)