UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"DESARROLLO DE UN PLAN DE CONTINGENCIA DE SERVICIOS TI PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE IBARRA, APLICANDO EL MARCO DE TRABAJO ITIL V3."

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO

EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: MARÍA FERNANDA FARINANGO FARINANGO

DIRECTOR: MSC. FABIÁN GEOVANNY CUZME RODRIGUEZ.

ASESOR: MSC. MAURICIO HERNAN DOMINGUEZ LIMAICO.

IBARRA – ECUADOR

2023

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA.

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO		
CÉDULA DE IDENTIDAD	100390150-0	
APELLIDOS Y NOMBRES	Farinango Farinango María Fernanda	
DIRECCIÓN	San Antonio de Ibarra – Vía antigua a Otavalo	
EMAIL	mffarinangof@utn.edu.ec	
TELÉFONO	Fijo: 062 514 798	Móvil: 0996878949

DATOS DE LA OBRA	
TÍTULO	"DESARROLLO DE UN PLAN DE CONTINGENCIA DE SERVICIOS TI PARA EL DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE IBARRA, APLICANDO AL MARCO DE TRABAJO ITIL V3."
AUTOR	Farinango Farinango María Fernanda
FECHA DE APROBACIÓN	27 de julio del 2023
PROGRAMA	☐ **PREGRADO**
TÍTULO POR EL QUE OPTA	Ingeniería en Electrónica y Redes en Comunicación
DIRECTOR	Ing. Fabián Cuzme, MSc.

2. CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es la titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 02 días del mes de agosto del 2023

EL AUTOR:

María Fernanda Farinango Farinango

CI: 100390150-9

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGISTER FABIAN CUZME RODRIGUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACION CERTIFICA:

Que, el presente trabajo de Titulación "DESARROLLO DE UN PLAN DE CONTINGENCIA DE SERVICIOS TI PARA EL DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE IBARRA, APLICANDO AL MARCO DE TRABAJO ITIL V3." Ha sido realizada en su totalidad por la señorita: María Fernanda Farinango Farinango portadora de la cédula de identidad con número: 1003901509 bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

.....

Ing. Fabián Cuzme, MSc

DIRECTOR DE TESIS

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

"Nosotros somos como los granos de quinua si estamos solos, el viento lleva lejos. Pero si estamos unidos en un costal, nada hace el viento. Bamboleará, pero no nos hará caer".

Dolores Cacuango

Con amor, cariño, admiración y respeto, este trabajo te lo dedico a ti mi querido Padre Miguelito Farinango, que con tu ejemplo de constancia nos enseñaste a luchar por nuestros sueños, a ser mejores cada día. Este trabajo lleva grabado tu nombre, sé que donde quiera que estes, estas orgulloso de mi, esperare con ansias vengas a mis sueños con un abrazo de felicitación y un "Que bien hijita" como siempre lo hacías. Gracias, por ese ejemplo de superación que emitías día con día, por enseñarme a mí y a mis hermanos que el estudio es lo único que nos llevará por un mejor camino.

Padre querido, está solo es una de las promesas que prometí cumplir, aún faltan varias, pero ten por seguro que lo haré y todas serán en tu honor.

Fernanda Farinango

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTOS

Quiero agradecer infinitamente a mis Padres, que han sido mi apoyo en todo momento, un gracias a mi querido Padre Miguelito, por sus consejos, su cariño y amor, por sus noches en vela esperando mi llamada para irme a recoger después de cumplir con los trabajos de la Universidad.

A mi quería y admirada Madre María, por su compañía en este largo proceso, por sus consejos, por su ánimo y carisma. Infinitas gracias madrecita de mi vida. A mis hermanos, gracias por su compañía y amistad. Por estar unidos hasta en los peores momentos, por brindarme su ayuda incondicional, nada de esto sería lo mismo si no estuviesen a mi lado. A mi querido Esposo Erik, gracias por su apoyo incondicional, por las palabras de aliento, por creer en mí y por darme ese empujón que necesitaba. A mis queridos sobrinos Dylan y Oscar, gracias por ser el aliento de toda la familia, ese lado de paz y tranquilidad, el impulso que necesitamos para seguir adelante, porque sabemos que siguen nuestros pasos.

A mi Director de Tesis Ing. Fabián Cuzme y Asesor Ing. Mauricio Domínguez por su gran ayuda en la elaboración de este trabajo, por su paciencia, su tiempo y por compartir sus conocimientos a lo largo de mi vida estudiantil.

Infinitas gracias al personal de TIC´s del GAD-Ibarra, en especial Ing. Gabriel Bucheli, Ing. Samantha Mesa, Ing. Manuel Lara, Ing. Verónica Rosero por su ayuda en el cumplimiento de este gran sueño.

Fernanda Farinango

CONTENIDO

Índice de figuras

Índice de tablas

RESUMEN

El presente proyecto analiza una metodología para la elaboración de un Plan De Contingencia de Servicios TI para la Dirección de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal de San Miguel De Ibarra, aplicando al Marco De Trabajo ITIL V3, esta guía permite tener una continuidad en los servicios TI proporcionados por el GAD-Ibarra.

El plan de contingencia se divide en varias etapas, como etapa 1 se reliazo un levantamiento de información de la infraestructura física y lógica del GAD-Ibarra. En la etapa 2 se realizó el estudio de un Análisis de Riesgos haciendo uso de la Metodología MAGERIT V3, la cual permite recopilar información acerca de las amenazas que pueden afectar al funcionamiento de los servicios TI, el impacto, frecuencia, degradación y riesgo que esta tendría en caso de llegar de llegar a materializarse. un listado de amenazas que podrían llegar a materializarse. En la etapa 3 se procedió a la realización de un plan de contingencia funcional, aplicando el marco de trabajo ITIL V3, la cual establece determinar las buenas prácticas al momento de hacer uso de un servicio, cabe mencionar que en este desarrollo se ha elegido 2 servicios TI con los que se procedió a trabajar, es necesario recalcar que esta elección se la hizo con el personal de la Dirección de Tecnologías de la Información.

Como resultado de esta investigación, se obtuvo un documento guía, en el que se detallan normas y procedimientos que deben ser ejecutados para restablecer los servicios TI en el menor tiempo posible, para ello se realizó una tabla informativa en la que se muestra detalladamente el tipo de afectación físico o lógico que pueden tener los servicio TI, personas responsables de levantar el servicio y tiempos estimados de recuperación. Enlazando esta información a un manual de procedimientos en el que se detalla los pasos a seguir para el levantamiento de los servicios.

ABSTRACT

This project proposes to prepare an IT Services Contingency Plan for the Information Technology Department of the Municipal Decentralized Autonomous Government of San Miguel De Ibarra, applying the ITIL V3 Framework, this guide will allow continuity in the IT services provided by Gad-Ibarra in the event that a threat materializes and affects the network infrastructure.

The contingency plan is divided into several stages, one of which is carrying out a Risk Analysis using the Magerit v 3 Methodology, which establishes a list of threats that could materialize and cause some inconvenience in the proper functioning of the network, depending on the type of threat, we proceed to obtain the data of the level of risk of the service and the affectation that this would have. With the result of the Risk Analysis methodology, a functional contingency plan will be carried out, applying the ITIL V3 framework, which establishes determining good practices when using a service, it is worth mentioning that in this development, 3 IT services have been chosen, with which they proceeded to work. It is necessary to emphasize that this choice was made with the staff of the Information Technology Department.

As a result of this investigation, a guide document will be obtained, which can be taken as a reference for the creation of a continuity plan focused on the business, with this it will allow to reduce the response time of a network administrator when making a decision. decision to solve a problem.

Chapter I is made up of the background, general and specific objective, problem and other reference guidelines to start the investigation.

Chapter II is made up of the theoretical framework, in this section all the theoretical part referring to the topic of work presented is detailed.

Chapter III is made up of the current situation of the information technology department, in this section, everything related to infrastructure, personnel, computer equipment, among others, is described. additionally, the Magerit 3 management analysis is also developed.

CAPITULO I

1 Antecedentes

1.1 Tema

Desarrollo de un plan de contingencia de servicios TI para la Dirección de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, aplicando al marco de trabajo ITIL V3.

1.2 Problema

En la actualidad, es cierto que, las redes de información es el bien más preciado dentro de las empresas, pero no se ha dado importancia necesaria para salvaguardar su integridad, ya sea por fallas técnicas, humanas, e incluso desastres naturales. Los eventos que por lo general causan pérdidas económicas dentro de la empresa e inconformidad de los usuarios suelen ser: fallos de equipos, fallas eléctricas, incendios, inundaciones, ataques internos o externos entre otros.

El Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, es una institución pública al servicio de la ciudadanía, la misma que es encargada de suscitar el desarrollo de la ciudad, brindando a la población servicios eficientes en todos los entornos que este abarca. Esta entidad cuenta con distintos departamentos que cumplen funciones diferentes, entre ellos se encuentra la dirección de tecnologías de la información, la cual es la encargada de la administración, mantenimiento y buen funcionamiento de la red de datos, siempre tomando en cuenta que el objetivo principal es brindar integridad, confidencialidad y disponibilidad de la información en cualquier momento que esta requiera.

Una falla informática en esta área sería un gran problema debido a que, esta mantiene información relevante en sus bases de datos y representaría daños considerables en tiempo y dinero, porque, este es el centro principal de la distribución de redes con los demás departamentos

de la municipalidad que brindan diferentes servicios a las personas que acuden diariamente a la organización. El simple hecho de manejar información relevante obliga a que, las entidades cuenten con un plan de contingencia de servicio TI (Tecnologías de la Información) que permita actuar inmediatamente en el menor tiempo posible ante algún fallo, en donde, la acción y reacción debe ser la indicada para el restablecimiento del correcto funcionamiento de los servicios, para esto se debe estar en constante monitoreo, para determinar un posible fallo y establecer cómo actuar ante esto.

De esta manera, el diseño de un plan de contingencia de servicios TI, es fundamental dentro de una empresa, como es el caso el departamento de Hardware e Infraestructura, dado que es una de las áreas más importantes para el buen desempeño de las actividades diarias que el GAD Ibarra realiza en el entorno tecnológico.

1.3 Objetivos

1.3.1 Objetivo general

Diseñar un plan de Contingencia de TI para la Dirección de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, que permita asegurar la operatividad de todos los servicios, basado en las mejores prácticas de ITIL V3.

1.3.2 Objetivos específicos

- Realizar un estudio sobre norma ITIL V3 para determinar los lineamentos a seguir en la realización del plan de contingencia de servicios TI y todos los requerimientos que esta necesite.
- Establecer el nivel de importancia de los servicios TI que maneja el Departamento de Hardware e Infraestructura, con esto determinar el impacto que tendría la falla técnica de uno de estos, con el buen funcionamiento de la red.

- Evaluar el estado actual de la dirección de tecnologías de la información, identificando los tipos de riesgos a los que pueden estar expuestos los servicios TI, realizando un levantamiento de información que detalle información relevante que ayuden a la realización de este proyecto.
- Diseñar un plan de contingencia de servicios TI, tomando en cuenta toda la información recolectada, determinando las necesidades que aseguren la eficiencia de los servicios que ofrece la Dirección de Tecnólogas de la Información.
- Realización de pruebas de implementación del plan de contingencia, evaluando controles de seguridad mediante simulaciones de fallos que confirmen su correcto funcionamiento.

1.4 Alcance

La implementación del plan de contingencia se realizará en la Dirección de Tecnologías de la Información del Gobierno Autónomo Descentralizado de San Miguel de Ibarra, este se basa en ITIL el cual es, un marco de referencia que determina el manejo y las buenas prácticas para la administración de servicios TI (Procesos, Gente y Tecnología). El mismo se desarrollará enfocado a la administración de procesos, para ello, se documentarán lineamientos importantes que permita su desarrollo, basándolo en BCP; el cual es, un plan logístico práctico para que, una organización recupere y restaure funciones críticas de forma parcial o total dentro de un tiempo predeterminado después de una interrupción no deseada.

Se considerarán los puntos más relevantes de la norma ITIL V3, mismos que permitirán determinar la situación actual de la Dirección de Tecnologías de la Información en el aspecto de administración de procesos y administración de servicios TI, identificando por medio de estadísticas de servicio requerirá mayor importancia dentro de la entidad, y con esto continuar con las fases del plan de contingencia que la institución necesita.

Se realizará un levantamiento de información de todos los equipos y servicios activos, estos datos fueron obtenidos por personas que laboran en el departamento de hardware e infraestructura de la entidad. Así, identificar servicios más propensos a una falla, documentando esta información elaborando inventarios técnicos y administrativos. El diseño del plan de contingencia contendrá, medidas detalladas para, conseguir la recuperación del sistema en el menor tiempo posible; para esto, se necesita seguir las fases de un plan de contingencia como son: evaluación, planificación, realización de pruebas, ejecución y recuperación.

1.5 Justificación

El buen manejo de la información en una entidad pública o privada, es indispensable para el buen desempeño de la red de datos, esa es la razón por la cual, este recurso debe ser protegido en su totalidad, motivo por el cual la Dirección de Tecnologías de la Información del GAD Ibarra, debe cumplir requisitos necesarios para brindar asistencia eficiente a ciudadanos que acuden diariamente a sus instalaciones en busca de los servicios que la institución ofrece. Para brindar un servicio, aunque mantiene su eficiencia, la institución utiliza solo una plataforma para archivar su información; en el caso que sucediera algún evento o falla en el sistema el efecto sería negativo, esto ocurrirá debido a que, a más de perder la información, también existirán pérdidas económicas, lo que ocasionaría la inconformidad de las personas que hacen uso de estos servicios.

Esto indica que la seguridad de la información es un punto estratégico, por tanto, se propone desarrollar un plan de contingencia que permite controlar, prevenir y recuperar la información que de cierta manera haya sufrido algún daño. El mismo que debe plantearse de acuerdo a las necesidades de cada entorno, dependiendo de la estructura y de bienes activos que posea la empresa, lo que permitirá restablecer diversos servicios brindados en periodos de tiempo

mucho más pequeños, para con ello garantizar la disponibilidad, integridad, confidencialidad y confianza de la información.

CAPITULO II

2 Fundamento Teórico

En el presente capítulo se aborda una investigación teórica con el fin de complementar criterios relacionados con el desarrollo de un plan de contingencia, seguridad informática, ataques, amenazas, riesgos, marco de trabajo ITIL, además se revisan normas legales que avalan el correcto desarrollo del mismo, como la norma de control de la Contraloría General del Estado, Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley de Propiedad Intelectual. Así como también normas internacionales como la ISO/IEC 27001 y la metodología MAGERIT V3.

2.1 Seguridad de la información

Con la finalidad de evitar riesgos en el manejo de la información, la institución está dispuesta a implementar sistemas de prevención informáticos que permitan asegurar y mantener su integridad y disponibilidad. Esto se realiza diseñando estrategias que beneficien las necesidades tanto del servidor público como del usuario y que, las mismas se encuentren disponibles para que el servidor pueda acceder a esta con facilidad y con seguridad de que no se perderá ni filtrara perjudicando al usuario. Esto se plantea de acuerdo a objetivos claros en el entono material, intangible y virtual de la actividad humana.

Según Baca (2016):

> La seguridad informática se basa en la disciplina del seguimiento a las políticas y normas internas y externas de una organización, su principal función es proteger la integridad y privacidad de la información que se encuentre almacenada en un sistema informático.

De esta manera igualmente Gómez (2015) indica que la seguridad informática es:

> Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información,

comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

2.1.1 Importancia de la seguridad de la información

Según Baca (2016):

Cada empresa, organización o inclusive en cada hogar se prioriza ciertas cosas, en el caso de una empresa es la información que maneja, ya que de ella depende continuar con sus funciones; la pérdida de información de algún cliente sería un grave error, además del impacto económico que podría afectar tanto a la empresa como al cliente.

De la misma manera Areitio (2008) indica que:

La importancia que se le ha dado a la interconexión de redes, en computadores, aplicaciones móviles, e incluso dentro de servidores internos de una empresa han conllevado a que la seguridad de los sistemas de información sean una parte esencial a tratar. La información debe ser resguardada dependiendo de la importancia de la misma, como puede ser: información gubernamental, personal, comercio, documentos médicos, negocios, etc., su seguridad ha pasado de ser una disciplina cada más crítica, necesaria y obligatoria.

Se debe tener en cuenta que la seguridad de la información en la actualidad es en extremo importante, esto sucede debido a la cantidad de transacciones de diferentes indoles que se generan por minuto a nivel mundial. Esto lleva a tener gran cautela por la información de cada usuario u organización, debido a la existencia de personas inescrupulosas que buscan el acceso a la misma, esto para poder obtener beneficios de manera ilegal perjudicando a los propietarios de los mismos, esto conlleva buscar diferentes maneras de proteger los sistemas informáticos para así poder conservar la información de forma apropiada y segura.

2.2 Conceptos básicos en materia a seguridad informática

En la actualidad los sistemas informáticos permiten que todo esté digitalizado, y cuando esto sucede, en la mayoría de casos se pueda convertir en un problema, debido a que, muchas organizaciones no están preparadas, ni correctamente asesoradas para procesar y mucho menos almacenar cantidades de información considerables. Cuando eso no está correctamente planificado la cantidad de información reduce el espacio disponible, lo que causa problemas en procesos informáticos. No podemos dejar de lado que, el proceso de automatización agiliza servicios que cualquier organización ofrece, sobre todo, facilitara el análisis y procesamiento de información, pero surgen otras cuestiones relacionadas con estas instalaciones. Esto no vuelve más fácil el transferir información y aumenta posibilidades de que desaparezca, y con el paso del tiempo se complique el acceder a él. Esto dirige a planificar de forma urgente un programa que ayude a manejar y almacenar de forma correcta un sistema acorde a las necesidades de cada proceso y tamaño de información a manejarse.

Según Calderón (2015), “La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de un sistema de información”.

Según Fuquene (2019) indica que:

> A través de los avances diarios en materia de tecnologías de información se generar nuevos vectores de riesgo para la seguridad de la información, por ello es necesario que tanto el ámbito académico como el legislativo y judicial de cada país está a la vanguardia de las nuevas amenazas que pudieran surgir en un momento determinado.

De la misma manera Fuquene (2019) expresa que:

A partir de esta premisa se encuentran dos definiciones que abarcan la parte nacional e internacional para analizar y gestionar este tipo de amenazas que son ciberseguridad y ciberdefensa respectivamente, la primera desde un concepto territorial defiende o preserva la seguridad de la información y tecnologías internas de una nación, la segunda tiene básicamente la misma definición pero ataca vector de ataque a la nación, es decir, desde otras naciones y que afecten la seguridad nacional de un país.

2.2.1 Seguridad informática

Según Baca (2016)**:**

La seguridad informática está relacionada con las normativas legales dentro y fuera de la empresa u organización, ya que dependiendo de la normativa vigente se tomarán medidas con el fin de proteger la información que se encuentra almacenada en un sistema informático, intentado reducir los riesgos físicos, lógicos, activos y pasivos que cuenta la empresa.

2.2.2 Seguridad activa y pasiva

Como indica Aguilera López (2011):

La seguridad informática se divide en seguridad activa y seguridad pasiva. La seguridad activa es aplicada con el fin de evitar riesgos que involucren a la información, por lo contrario, la seguridad pasiva se encarga de dar mecanismos de soporte frente a una eventualidad suscitada.

Así mismo Aguilera López (2011):

La seguridad activa es la encargada de crear medidas de defensa ante posibles impactos, con el fin de prevenir o mitigar riesgos que impidan el correcto funcionamiento del sistema

o a su vez saber cómo actuar de manera inmediata ante algún inconveniente que se presente de manera inesperada.

Se la define también como medidas preventivas, con la finalidad de estar preparados ante un ataque y que este no afecte de manera significativa a la red. Taco (2018) afirma que "Sirve para evitar daños a los sistemas informáticos. Son tales como el empleo de contraseñas adecuadas, la encriptación de datos y el uso de software de seguridad informática" (p. 19), es decir, la seguridad activa hace referencia a antivirus, a la utilización de contraseñas fuertes, SO actualizados con parches de seguridad, Firewall, entre otras, con la finalidad de impedir daños.

De igual forma Taco (2018) menciona que:

La seguridad pasiva es la que entra en acción una vez que el evento haya impactado en la red, permitiendo la pronta recuperación y restauración de los datos en el menor tiempo posible, minimizando los efectos de los daños producidos, dentro de este tipo de seguridad se puede optar por las copias de seguridad, manuales de recuperación, plan de contingencia, mecanismos de redundancia física, entre otras.

2.2.3 Seguridad física y lógica

En lo referente a mecanismos de seguridad se encuentran la seguridad física y lógica. La seguridad física se encarga de brindar protección a equipos físicos en donde se almacena la información por lo contrario la seguridad lógica se encarga de resguardar la seguridad digital. Aguilera López (2011) menciona que "Los mecanismos físicos o lógicos de seguridad tienen como misión prevenir, detectar o corregir ataques al sistema, asegurando que los servicios de seguridad queden cubiertos" (p. 17).

Como Aguilera López (2011) indica que

La seguridad física es un mecanismo cuya función es proteger al sistema y por ende a la información, es la encargada de brindar protección a los activos físicos y lógicos de una organización. Esta seguridad permite hacer uso de los respaldos de datos (información), como por ejemplo el uso de copias de seguridad, además del uso de dispositivos físicos de protección como pararrayos, cámaras de seguridad, sensores biométricos, extintores, puertas de acceso, en caso de inundaciones, cortafuegos, a más de la señalización de seguridad dependiendo del caso.

Además Aguilera López (2011) agrega que:

La seguridad lógica se encarga de salvaguardar la seguridad de la información digital de manera que sólo las personas autorizadas puedan hacer uso de esta, entre los elementos que conforman la seguridad lógica se encuentra, el control de acceso, cifrado de datos, antivirus, cortafuegos, firma digital, certificados digitales. En las redes inalámbricas también se cuenta aplicaciones de seguridad lógica como, SSID, claves encriptadas WEP, filtrado de direcciones MAC, lo cual permite tener mayor seguridad de la información en cuanto se haga uso de la tecnología.

2.2.3.1 Principios de la seguridad.

Según Roa (2013):

Los principios de seguridad permiten que la información sea manejada de la mejor manera, brindando tanto al emisor y receptor, tener la certeza que su información mantendrá la integridad, confidencialidad, disponibilidad además de su autenticidad y no repudio a la misma, es decir, hacer uso de los recursos informáticos de una empresa respetando la información de los usuarios ya sea confidencial o pública. (p. 64)

Cada concepto referente a los principios de seguridad se detalla a continuación:

- **Confidencialidad.**

La confidencialidad hace referencia a que la información sea utilizada por las personas o máquinas debidamente autorizadas. Para garantizar la confidencialidad esta se basa en disponer de tres tipos de mecanismos como son: autenticación, autorización y cifrado (Roa Buendía, 2013).

Según Aguilera López (2011) la Organización para la Cooperación y el Desarrollo Económico (OCDE), define a la confidencialidad como "El hecho de que todos los datos o información estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada" (p. 17). Para asegurar la confidencialidad de la información, se pueden tomar ciertas medidas como puede ser, contraseñas de acceso, palabras claves, tiempos de acceso, carpetas o sitios definidos, entre otros.

- **Integridad.**

Según Roa (2013) indica que la integridad de la información se refiere a que los datos conserven su originalidad, asegura que la información no ha sido modificada por personas o entidades no autorizadas, en otras palabas él envió de un mensaje no puede ser alterado mientras este se encuentre en proceso de llegar a su destino.

Según Hernández James (2011) menciona la no modificación de la información es uno de los principales principios de la seguridad, ya que de esto depende el porcentaje de credibilidad de ella, a menos que esta sea modificada o cambiada por personas autorizadas y de manera controlada. Uno de los principales riesgos que corre una empresa en el manejo de información es el cambio drástico de datos, como por ejemplo una cuenta bancaria.

- **Disponibilidad.**

La disponibilidad se enfoca en que el servicio se encuentre operativo continuamente. Roa (2013) afirma que "La disponibilidad intenta que los usuarios puedan acceder a los servicios con

normalidad en el horario establecido" (p. 15). La disponibilidad de los servicios debe ser continua ya que de eso depende la eficiencia prestada a cada uno de los clientes.

Según la metodología Magerit (2012) define la disponibilidad como "El grado en el que el dato está en el lugar, momento y forma en el que es requerido por un usuario autorizado" (p. 7).

- No repudio.

Según Vivas, et al. (2015) menciona que el no repudio permite realizar la comprobación de la participación de las partes que establezcan una comunicación por medio de un elemento digital, como por ejemplo las firmas electrónicas o la emisión de certificados, por lo cual una persona no podrá negar haber realizado algún acto dentro de este entorno.

- Autenticación.

De acuerdo a Keffer & Gallart (2007) indica que la autenticación de la información o también conocido como aseguramiento del contenido, se basa en métodos de identificación y verificación. Se puede denominar como un documento original o fiel al original, se enfoca en confirmar que una persona o máquina es quien dice ser.

- **Trazabilidad**.

La trazabilidad permite conocer que persona hizo uso de un servicio determinado, ya que si una empresa no tiene esta información abriría las puertas al fraude e incapacitaría a la organización a realizar el seguimiento de algún delito y podría suponer el incumplimiento de obligaciones legales.

2.2.4 Administración de la Red

De acuerdo Baca (2016), este indica que la administración de la red se basa en un conjunto de técnicas con el fin de mantener una red operativa, eficiente, segura y contantemente monitoreada, además de contar con una documentación aprobada por el administrador de la red, donde el objetivo principal es hacer uso de la red de manera eficiente y utilizar de mejor manera los recursos de la red como el ancho de banda entre otros.

- **Gestión de la red.**

La gestión de la red consiste en monitorizar los recursos de la red con el fin de evitar que esta llegue a funcionar incorrectamente degradando el servicio. Se encarga de la planificación, organización, operación, supervisión, y control de todos los elementos informáticos.

- **Gestión de Software**

La gestión de software implica la adición y eliminación de software de sistemas independientes, para la gestión de servidores, switch, routers etc. El cual permite Gestión de Hardware y Gestión de Antivirus.

- **Gestión de Software**

La gestión de software implica la adición y eliminación de software de sistemas independientes, para la gestión de servidores, switch, routers etc. El cual permite Gestión de Hardware y Gestión de Antivirus.

- **Gestión de Software**

La gestión de software implica la adición y eliminación de software de sistemas independientes, para la gestión de servidores, switch, routers etc.

- **Gestión de Hardware**

La gestión del hardware implica una variedad de tareas, como diagnosticar fallas de hardware, actualizar componentes de hardware y reemplazar piezas defectuosas, es importante mantener todos los componentes de hardware en un sistema informático actualizados y funcionando correctamente para garantizar un rendimiento óptimo

- **Gestión de Antivirus.**

La gestión del antivirus juega un papel importante en la protección de un sistema informático contra el robo de datos, el software malicioso y otras amenazas cibernéticas, es necesario instalar, configurar y actualizar el software antivirus en el sistema para garantizar su seguridad. También se deben realizar escaneos regulares del sistema para detectar cualquier software malicioso que pueda haberse infiltrado en el sistema.

2.3 Plan de Contingencia

Según Ramirez (2014) menciona que un plan de contingencia es un proceso que se encarga de dar continuidad a los procesos en el caso que se presenten riesgos que puedan afectarlos, organizando a las personas responsables de cada área, actividades que ayuden a mitigar o evitar el impacto. Esta información será documentada en un texto totalmente claro y entendible con las medidas y normas a seguir de forma estratégica para su implementación. El objetivo principal de un plan de contingencia es mejorar la capacidad de respuesta frente a diversos eventos que afecten el buen funcionamiento del sistema. A más de ello el plan de contingencia pretende ayudar a las organizaciones empleando los recursos disponibles para poder enfrentar el escenario de riesgo.

2.3.1 Objetivos de un Plan de Contingencia

Según la NTE INEN-ISO/IEC 27002 y el registro oficial Nro. 039 GG (2013) menciona que un plan de contingencia informático debe contar con los siguientes objetivos:

a) Debe mantener a la medida de lo posible la continuidad de los servicios proporcionados por la organización denominados críticos en un nivel aceptable en caso de un plan de contingencia.
b) Establecer acciones y procesos que permitan mantener la operatividad de los sistemas de información en caso de una emergencia.

2.3.2 Importancia de un Plan de Contingencia

En la actualidad, la importancia de tener en vigencia un plan de contingencia en todas las instituciones públicas o privadas es de gran utilidad, esto se necesita en caso de ocurrir algún desastre natural, mecánico o humano, así, se puede responder de manera ágil y obtener una pronta recuperación de la información, para esto, es importante realizar un análisis de riesgos dentro de la organización para poder realizar el plan de contingencia de acuerdo a las necesidades del entorno.

Así mismo Méndez (2015), menciona que

> El manejo adecuado del plan de contingencia debe estar manejado por una persona que pueda estar al frente, además de ser encargado de la toma de decisiones en caso de que un desastre ocurra. Al hablar de desastre, este abarca la suspensión prolongada de los recursos informáticos, fallas prolongadas de los sistemas de información, fallas en la electricidad, suspensión del acceso a la información, o cualquier otro tipo de eventos que interrumpan el buen funcionamiento de los sistemas de información de la organización.

2.3.3 Tipos de Contingencias

Existen diferentes tipos de contingencias, determinando la afectación del evento en los sistemas de información las cuales se clasifican por niveles, empezando por el nivel bajo, medio, alto y crítico cada uno de estos se enfocan dependiendo la situación que la organización está atravesando (Méndez, 2015). Se define brevemente cada tipo de contingencia a continuación:

a) **Bajo:** Esta afectación es irrelevante a las actividades diarias de la empresa, las cuales se las puede reparar en el transcurso del día.

b) **Medio:** Esta afecta a las instalaciones físicas de la empresa, pero, no causa mayor problema en reanudar las actividades.

c) **Alto:** Se cataloga como alto cuando, las afectaciones en las instalaciones como a las operaciones son graves, pero no lo suficiente como para realizar el traslado a instalaciones alternas.

d) **Crítico:** Esta afectación es de gravedad, debido que, afecta a las instalaciones, a las operaciones y al bienestar de las personas, por lo cual es necesario el traslado de las instalaciones a un lugar alterno y el plazo de recuperación será prolongado.

El plan de contingencia está formado por tres sub planes como se muestra en la Figura 1. Cada uno de estos determina la toma de decisiones tomando en cuenta el tiempo de materialización de cualquier amenaza.

Figura 1

Ciclo de sub planes de un plan de contingencia.

Nota: Ciclo de un Plan de Contingencia

- **Plan de respaldo**

El plan de respaldo se encarga de contemplar las contramedidas preventivas antes que una amenaza se materialice, su objetivo principal es que la amenaza llegue a la materialización. Méndez (2015), afirma que "Contiene todas las medidas y procedimientos preventivos para asegurar la reanudación de las actividades antes de que la amenaza se materialice, el plan de respaldo es el más importante, permite disminuir y mitigar la probabilidad de ocurrencia de desastres" (p. 25).

- **Plan de emergencia**

El plan de emergencia es un conjunto de acciones y procedimientos para la atención de la materialización de amenazas con la finalidad de reducir daños materiales o humanos, este plan debe ser aplicado durante el incidente. En él se redacta detalladamente que se va hacer, como se va hacer y cuando se va hacer, al momento que ocurra algún evento catalogado como emergencia

dentro y fuera de las instalaciones de una empresa, con la finalidad de salvaguardar la seguridad intelectual de las personas como de los bienes materiales de la organización (Ramirez, 2014).

Desde Méndez (2015), afirma que:

> Son las acciones que se deben tomar durante o inmediatamente después de la materialización de la amenaza a fin de disminuirla, es un mecanismo que permitirá seguir proporcionando funciones de procesamiento de la información cuando la actividad principal no esté disponible. (p. 25)

- **Plan de recuperación**

El plan de recuperación contempla medidas necesarias a tomar después que la amenaza se haya materializado y posteriormente controlada. Su objetivo principal es restaurar el estado de las cosas y personas, tal como se encontraban antes de la materialización de la amenaza. Dicho de otra manera, este plan es el encargado de asesorar los pasos a seguir después que un desastre haya ocurrido o de haber controlado una amenaza, en este plan se detalla la información necesaria para la restauración adecuada de los equipos y actividades a su estado normal (Méndez, 2015).

2.4 ITIL (Information Technology Infrastructure Library)

La Biblioteca de Infraestructuras de Tecnologías de Información (ITIL) es un marco de trabajo que se enfoca en las mejores prácticas, brindando herramientas y métodos para el manejo de los servicios TI, garantizando la calidad de los servicios. Además, incluye una descripción detallada de los procesos más relevantes en una organización que la convierte en una guía útil para definir nuevos objetivos de mejores prácticas de los servicios que lleven a la organización a un crecimiento y madurez, esta normativa hace referencia de la relación gente-procesos-tecnología (Baud, 2016). Actualmente existen 3 versiones de ITIL, en la tabla 1 se muestra la comparación de cada una de estas.

Tabla 1

Comparación de las versiones ITIL

ITIL LIBROS	VERSIÓN 1	VERSIÓN 2	VERSIÓN 3
	Creada en 1988	**Creada en 2001**	**Creada en 2007**
	Se convierte en un estándar de países bajos.	Fue adoptada por entidades públicas y privadas de España.	Está presente en al menos 80 países alrededor del mundo.
	Formada por 31 libros.	Formada por 7 libros.	Formada por 5 libros.
	Se basa en la mejora de la efectividad y calidad de los servicios TI	Se basa en la gestión de los servicios TI	Se basa en un ciclo de vida de los servicios TI
		TI Service Manager	ITIL Expert ITIL Master (En desarrollo)

Se ha tomado en cuenta la utilización de la versión 3, por ser la más adecuada la para realización de un plan de contingencia, cuenta con 5 libros los cuales son, estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio (Baud, 2016)**.** La estrategia del servicio es el eje fundamental para que las demás fases del ciclo de vida ITIL V3 giren sobre esta como se muestra en la Figura 2, en esta fase se define las políticas se seguridad, además de establecer objetivos. Las fases de diseño, transición y operación de los servicios se realizan a partir de la primera fase, es decir, de la estrategia. La fase de mejora continua del servicio, se basa en el aprendizaje y mejora de todas las fases del ciclo de vida ITIL V3, se basa en seguir los objetivos planteados por la organización (Bon, et al., 2008).

Figura 2

Diagrama del ciclo de vida ITIL V3.

Nota. Fuente: Bon, et al. (2008).

2.4.1 Fases del ciclo de vida ITIL V3

El ciclo de vida ITIL V3 consta de 5 libros, estrategia del servicio, diseño del servicio, transición del servicio, operación del servicios y mejora continua del servicio, es así que se enfocan en ofrecer una visión global de un servicio desde que este se origine hasta su eventual abandono, sin ignorar todo el proceso que esto conlleva para ofrecer la prestación de un servicio (Bon, et al., 2008). Cada uno de estos libros se detallan a continuación.

2.4.1.1 Estrategia del servicio

Con el fin de planificar una buena estrategia es necesario la implementación de las llamadas cuatro P; Perspectiva, Posición, Plan y Patrón, estos ayudan a que una estrategia bien definida sea llevada a cabo con éxito dentro de la organización (Mintzberg, et al. (2007)**.** Es así que, a continuación, se detallan cada una de estas.

- **Perspectiva:** La estrategia debe poseer un enfoque, visión y expectativa totalmente clara del plan a emplearse.
- **Posición:** La estrategia debe acoger una postura bien definida.

- **Plan:** Se debe formar una serie de ideas ordenadas de cómo debe desarrollarse una organización.
- **Patrón**: Mantener la coherencia de decisiones y acciones, según lo planificado.

Por otro lado, un valor es la combinación entre los efectos de utilidad y garantía, estos elementos son necesarios para la creación de valor de un cliente. Bon, et al. (2008) afirma que "Desde el punto de vista del cliente, el efecto positivo es la utilidad de un servicio, mientras que la garantía es lo que asegura dicho efecto positivo" (p. 25). La utilidad se adecua a un propósito definiéndolo de manera concisa como "lo que hace" un servicio para satisfacer una necesidad, y la garantía se adecua a un uso que debe garantizar que un servicio o producto va a cumplir los requisitos acordados (disponibilidad, capacidad, continuidad y seguridad de la información).

La estrategia de servicio es el núcleo del ciclo de vida de ITIL V3, se refiere a las estrategias que se ha definido para ayudar a las organizaciones o empresas a pensar o actuar de manera estratégica frente a algún evento. La finalidad de este ciclo es definir servicios informáticos que van a proporcionar valor a la organización o empresa. Es importante clasificar el tipo de mercado en el que esta se encuentra, determinar que necesidades tienen sus clientes, entendiendo la competencia del departamento de informática, con un enfoque estratégico y basado en una lógica financiera (Baud, 2016). Los procesos de la fase de estrategia son cinco los cuales se definen en la tabla 2.

Tabla 2

Descripción de las fases de la Estrategia del servicio.

FASES	DESCRIPCIÓN
Definición de estrategia	Se define como la construcción de la política de seguridad y del sistema de información vigente para los siguientes años, su principal elemento es el esquema director, es decir, la estrategia es el camino que va a tomar el sistema informático en la empresa.

Gestión del portafolio de los servicios	Es un proceso que es generado con la finalidad de dar vida a los servicios de la empresa, además de gestionar de manera adecuada las inversiones para dar un valor agregado a la organización
Gestión de Demanda	Este proceso es el encargado de suministrar los elementos técnicos y no técnicos necesarios para la empresa con el fin de satisfacer la demanda de los clientes, este suministro debe depender del rendimiento de los servicios y de su capacidad.
Gestión Financiera	Se encarga de gestionar los costos financieros generados por el área de informática, deduciendo el valor proporcionado de los servicios, para con esto poder gestionar los presupuestos y las inversiones necesarias para departamento informático.
Gestión de la relación de las ramas del negocio	Esta gestión se encarga de establecer una buena relación administrativa entre las diferentes ramas del negocio y el departamento informático

Ahora se puede decir que, la estrategia del servicio proporciona entradas a cada fase del ciclo de vida, en la tabla 3 se detalla la forma en que la estrategia del servicio se relaciona con las de las fases.

Tabla 3

Relación entre la estrategia del servicio y demás fases del ciclo de vida ITIL V3.

RELACIÓN	DESCRIPCIÓN
Estrategia y diseño	Las estrategias de servicios llegan a la implantación a través de la provisión de la cartera en un segmento concreto del mercado. En la fase de diseño del servicio se promueven nuevos servicios o que requieran mejoras para responder a la demanda. El diseño puede estar dirigido por modelos de servicios, resultados, restricciones o precios.
Estrategia y transición	Para reducir el riesgo de fallo, todos los cambios estratégicos pasan por la transición del servicio. Los procesos de transición de servicio analizan, evalúan y dan a su aprobación a las iniciativas estratégicas. La estrategia del servicio proporciona las estructuras y restricciones a la transición del servicio.
Estrategia y operación	Las estrategias se plasman en la operación del servicio, por lo que la estrategia debe ser acorde a las capacidades y restricciones operativas. Los patrones de despliegue en la operación del servicio definen las estrategias operativas para los clientes.
Estrategia y mejora continua del servicio.	Debido a los contantes cambios, las estrategias nunca son estáticas. Las estrategias de servicio deben desarrollar, adoptar y revisar de modo continuo.

2.4.1.2 Diseño de los servicios.

El diseño de los servicios se enfoca en crear nuevos diseños o a su vez mejorar los ya existentes, referente al departamento informático de una empresa, por consiguiente, el diseño abarca las especificaciones necesarias para el desarrollo de las aplicaciones solicitadas y de los servicios que estas ofrecen, además de los elementos necesarios para su realización (Baud, 2016)**.** Esta fase del ciclo de vida ITIL V3 se basa al cumplimiento de 5 objetivos los cuales se detallan a continuación.

a) Diseñar nuevos servicios para, satisfacer las necesidades de las ramas del negocio, a través de los clientes, en esta fase también se va a tener en cuenta las obligaciones de los clientes en términos de calidad de servicio.
b) Simplificar el diseño de los servicios y optimizar los costes.
c) Identificar y gestionar los riesgos que se pueden producir durante la puesta en marcha del servicio. En las buenas prácticas ITIL V3 no hay procesos específicos para la gestión de riesgos, la misma que se reparte entre los procesos de las fases de la estrategia de los servicios y del diseño de los servicios.
d) Desarrollar las competencias idóneas que, necesitará el departamento informático para satisfacer las demandas tanto internas como de los clientes.
e) Desarrollar las aptitudes que necesitará el departamento de informática para satisfacer las necesidades de los clientes, es decir, la manera de trabajar (procesos, procedimientos, recomendaciones, etc.) y garantizar su efectividad y eficiencia.

2.4.1.3 Procesos de la fase de diseño de los servicios.

Los pasos de la etapa de diseño se catalogan en 8 gestiones diferentes:

- Catálogo de servicios.
- Niveles de servicios.

- Capacidad.
- Disponibilidad.
- Continuidad de los servicios TI.
- Seguridad de la información.
- Seguridad de proveedores.
- Seguridad de diseño.

En la tabla 4 se realiza una descripción de cada uno de estos:

Tabla 4

Procesos de la fase de diseño de servicios ITIL.

PROCESOS DE LA FASE DE DISEÑO	DESCRIPCIÓN
Gestión del catálogo de servicios	El objetivo de esta fase es el desarrollo de un catálogo de servicios que contenga los detalles de cada servicio existente, así como también los que se encuentran en desarrollo.
Gestión de los niveles de servicio	En esta fase se garantiza que se cumplan los niveles de servicios TI, dependiendo de los objetivos planteados por la empresa.
Gestión de la capacidad	Esta gestión es la encargada de mostrar las capacidades de la empresa en brindar mejorías hacia los clientes, atendiendo las necesidades presentes y futuras que se debe documentar en un plan de capacidades.
Gestión de la disponibilidad	Es la encargada de garantizar los niveles de disponibilidad de los servicios existente o modificados, esto depende de los términos acordados con los clientes y documentados en el plan de disponibilidad.
Gestión de la continuidad de los servicios TI	Se enfoca en garantizar la continuidad de negocio, además de asegurar la recuperación y restauración de las instalaciones TI en un tiempo establecido.
Gestión de la seguridad de la información.	Esta fase hace uso de las políticas de seguridad la cual establece requisitos legales para la protección de la información dependiendo del gobierno corporativo.
Gestión de los proveedores	Su objetivo es facilitar los suministros y contratos de proveedores de servicios que adquieran las empresas con el fin de brindar servicios eficientes a sus usuarios.
Gestión del diseño	Es la fase donde se desarrolla los requisitos de diseño, además de la gestión de la información, datos y aplicaciones.

Nota. Tomado de Baud (2016).

2.4.1.4 Transición de los servicios.

La transición de los servicios se enfoca en el desarrollo y mejora de capacidades técnicas o no técnicas, con el fin de dar paso a la producción de todos los servicios, ya sean estos nuevos o modificados, además se encarga de hacer que los productos y servicios definidos en la fase de diseño del servicio se integren en el entorno de producción y sean accesibles a los clientes (Baud, 2016). En la fase de transición de servicios se presentan 3 objetivos.

a) Garantizar que los recursos sean planificados y coordinados adecuadamente para cumplir las especificaciones del diseño.
b) Asegurar el uso de métodos y procedimientos estándares para garantizar eficiencia y calidad en cada uno de los cambios que se produzcan, de manera que se minimice el impacto en las incidencias del servicio que prestamos a nuestros clientes.
c) Supervisar y dar soporte a todo el proceso de cambio del nuevo (o modificado).

2.4.1.5 Operación de los servicios.

Es la que se basa en el mantenimiento correctivo, evolutivo y preventivo de la producción informática o de la transición del servicio. A esto se lo define en una frase "Service Operations" esta frase entra en funcionamiento inmediatamente cuando el servicio entra en marcha. Todas las fases del ciclo de vida ITIL se enfocan en la prestación de los servicios de manera adecuada, de nada serviría que la estrategia del servicio, diseño del servicio y la transición del servicio funcionen correctamente, si al momento de entrega u operación del servicio esta falla, en definitiva, la operación de los servicios se encarga que un servicio determinado llegue al usuario final sin ninguna falla (Baud, 2016)**.** La operación de los servicios cuenta con 3 objetivos a cumplir los cuales se detallan a continuación.

a) Coordinar e implementar todos los procesos, actividades y funciones necesarias para la prestación de los servicios acordados con los niveles de calidad aprobados.
b) Dar soporte a todos los usuarios del servicio.
c) Gestionar la infraestructura tecnológica necesaria para la prestación del servicio.

2.4.1.6 Mejora continua de los servicios.

La mejora continua de los servicios, está ligada a brindar continuidad al correcto funcionamiento de los mismos, estos deben adaptarse a las necesidades de las diferentes ramas de negocio de la empresa, para con esto, poder identificar, evolucionar e implementar mejoras en términos de efectividad y eficiencia, haciendo referencia a los procesos tecnológicos como a sus costos, siempre teniendo como prioridad la satisfacción de los clientes. Para ello es necesario realizar una comparación de los niveles de servicio deseados por los clientes con el fin de determinar su rendimiento. Esta fase trabaja con un único proceso que se denomina mejora continua que consta de siete etapas (Baud, 2016)**.**

2.5 Conceptos básicos de un análisis de riesgos

Con relación a un análisis de riesgos se debe tomar en cuenta algunos conceptos básicos como amenazas, vulnerabilidades, ataques informáticos entre los más nombrados, estos conceptos permitirán comprender mejor cada uno de los parámetros de un análisis de riesgos.

- Riesgos.

Los riegos de manera general siempre van a estar presentes, el objetivo primordial de un análisis de riesgos es evitar que estos se materialicen, previniendo pérdidas de información o daños a los elementos físicos del sistema. Los riesgos a los que está expuesto una empresa u organización pueden ser internos o externos, simples o extremadamente complejos, los cuales están presentes

continuamente en la organización, es por ello que se recomienda empezar por analizar las vulnerabilidades que la empresa posee con el fin de reducirlas o controlarlas (Roa Buendía, 2013)**.**

Según Baca (2016) menciona que "Existen cuatro etapas para la realización de un análisis de riesgos, las cuales son: planeación, dirección, localización, y control, que serán ejecutadas y monitoreadas desde el centro de informática" (p. 23). Una de las estrategias del análisis de riesgos es también enfocarse en el aspecto económico, ya que es necesario realizar un estudio del mantenimiento de los elementos físicos y lógicos con los que se compone el sistema informático, determinando si es necesario mantenerlos o sustituirlos, esto también incluye al aparato administrativo de la organización (Baca, 2016).

- **Amenazas.**

En la seguridad informática, las amenazas se definen como uno o más factores que puedan afectar de manera significativa al sistema si se llegaran a materializar, existen amenazas físicas y lógicas que pueden ser de gravedad o de bajo nivel. Las amenazas lógicas se refieren al tipo de software, herramientas de seguridad, puertas traseras, virus, gusanos, etc. que afectan significativamente correcto funcionamiento del sistema. Y las amenazas físicas, se refieren básicamente a todo lo que pueda ocasionar daños hacia la empresa como puede ser robos, destrucción de sistemas, condiciones atmosféricas adversas, catástrofes naturales o artificiales (Roa Buendía, 2013).

- **Vulnerabilidad informática.**

Una vulnerabilidad es un defecto ya sea de los elementos físicos y lógicos del sistema o de parte de las personas que los manejen. Existen dos tipos de vulnerabilidades que son: reconocidas y no reconocidas. Las reconocidas, son aquellas que el suministrador tiene conocimiento que existen y tienen parches para poder corregirlas, pero también se encuentran las que no lo tienen y

debe ser desactivado el servicio hasta que pueda ser corregida o colocada el parche y las vulnerabilidades no reconocidas que son las más peligrosas, ya que el suministrador ignora su existencia y estas se encuentran en constante peligro de ser atacadas sin notarlo (Roa Buendía, 2013).

- **Ataques**

Los ataques son amenazas materializadas que afectan y ocasionan grandes daños en el sistema. Entre los ataques más conocidos tenemos la interrupción del servicio, interceptación, modificación de la información, ingeniería social, phishing, kyloggers, fuerza bruta, spoofing, sniffing, DoS, DDoS, entre otros (Roa Buendía, 2013).

2.6 Metodologías de análisis y gestión de riesgos de los sistemas de la información

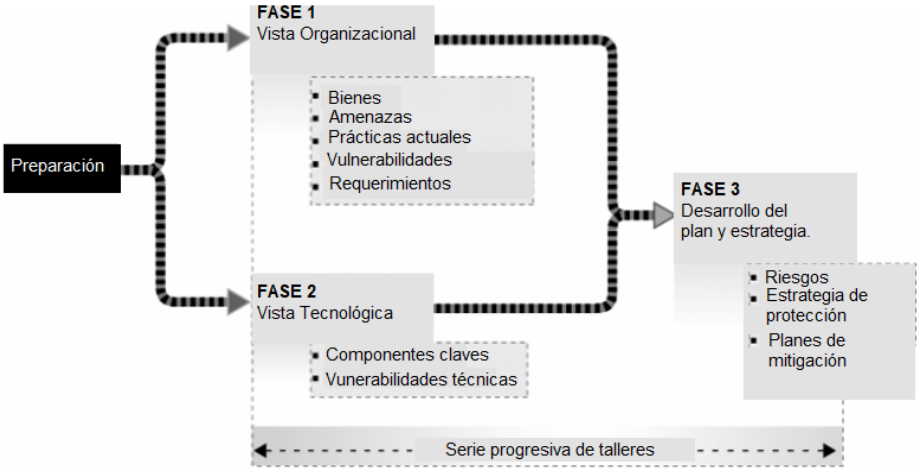
La metodología de análisis y gestión de riesgos establece un conjunto de principios que permitan que las organizaciones desarrollen, implementen y mejoren continuamente aplicando un modelo de trabajo que permita integrar el proceso de un análisis de riesgos, en los procesos de estrategia, planificación, documentación, aplicación de políticas y valores en toda la organización (Novoa & Barrera, 2015).

2.6.1 Octave (Operationally critical threat, Asset, and vulnerability evaluation)

Esta metodología fue desarrollada por la Universidad Carnegie Mellon en el 2001, se encarga de analizar los tres principios de la seguridad como la confidencialidad, integridad y disponibilidad, se basa en analizar los riegos de seguridad de la información, proponiendo como objetivo principal la concientización de sus trabajadores acerca de la importancia de proteger la información, no solo en la parte teórica si no también realizando una reorganización de tareas con la finalidad de que esto se cumpla en su totalidad (Novoa & Barrera, 2015). Además, la metodología octave se la utiliza con mayor preferencia en organizaciones gubernamentales.

Habrá que decir también que, para la implementación de esta metodología, la organización debe contar con al menos 300 empleados o más, ya que fue creada específicamente para mantener su propia infraestructura informática, además de tener la capacidad de ejecutar herramientas de evaluación de vulnerabilidad y saber cómo interpretarlos (Caralli, et al., (2007). En la figura 3 se muestra cómo trabaja la metodología octave en cada una de sus fases. En la fase 1 o vista organizacional, el equipo de análisis identifica cada uno de los activos más relevantes relacionados con la información y la estrategia que se utilizará para la protección de esos activos, luego se determina los más críticos, se documenta toda la información e identifica cualquier tipo de amenazas que puedan interferir en sus objetivos. En la fase 2 o vista tecnológica, el equipo de análisis realiza una evaluación de la infraestructura de información para complementar la información del análisis de riesgos realizados en la fase 1 e informa sobre sus resultados a la fase 3. En la fase 3 o estrategia y desarrollo el plan, el equipo de análisis realiza actividades de identificación de riesgos y desarrolla un plan de mitigación de riesgos para los activos críticos. (Caralli, et al., (2007)**.**

Figura 3 Fases del método Octave



Nota. Tomado de Rincón, et al. (2018).

2.6.2 OSSTMM (Open-source security testing methodology manual)

El Manual de metodología de pruebas de seguridad de código abierto, fue creada en 2001 por Pete Herzog. Este manual complementa otros marcos de trabajos enfocados a la seguridad como son ISO 27001, 27002 e ITIL entre otras, lo que lo hace uno de los más completos al momento de su implementación en las organizaciones (ISECOM, 2010).

De tal forma, su principal propósito es brindar una metodología que se encargue de realizar un testeo sobre la seguridad interna y externa, además de emitir guías para la realización de auditorías de sistemas que requieran una certificación del Instituto para la Seguridad y Metodologías Abiertas (ISECOM). Su documentación es muy detallada bridando la información adecuada para el desarrollo de un test de seguridad operacional. Esta metodología abarca aspectos físicos, humanos, de telecomunicaciones, medios inalámbricos, redes de datos y cualquier otra derivada a la métrica real (ISECOM, 2010).

Asu vez, el ámbito se enfoca en abarcar toda la seguridad operativa, donde se incluyen la seguridad física, la que contiene el factor humano y físico, la seguridad de las comunicaciones se

refiere a los datos y telecomunicaciones y la seguridad del espectro electromagnético se encarga de las comunicaciones inalámbricas que hacen uso de las señales electromagnéticas. (ISECOM, 2010)**.** En la tabla 5 se muestra en detalle cada uno de estos ámbitos.

Tabla 5

Ámbito de OSSTMM

CANAL	SECCIÓN	DESCRIPCIÓN
Seguridad Física	Humano	Personal que labora y hace uso de la organización.
	Físico	Objetos tangibles de la organización.
Seguridad de las comunicaciones	Redes de datos	Sistemas electrónicos y redes de datos.
	Telecomunicaciones	Comunicaciones digitales y analógicas.
Seguridad del espectro electromagnético	Comunicaciones inalámbricas	Señales electromagnéticas utilizadas.

Nota. Hace referencia al ámbito de la metodología OSSTMM. Tomada de ISECOM *(2010)*

2.6.3 MAGERIT V (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Magerit) responde a la metodología ISO 31000, la cual establece procesos de gestión de riesgos dentro de un marco de trabajo para que las organizaciones tomen decisiones basándose en los riesgos derivados del uso de tecnologías de la información, este método cubre la fase de Análisis y Gestión de Riesgos (AGR). Fue elaborada por el Consejo Superior de Administración Electrónica de España, su última actualización fue en el 2012 en su versión 3 (Ministerio de Hacienda y Administraciones Públicas, 2012). Esta metodología ayuda a que se pueda llevar a cabo las siguientes acciones.

a) Realiza el análisis de riesgos de cualquier tipo de sistema de seguridad de la información (SSI), que permite obtener un índice único de las vulnerabilidades y posibles amenazas e impactos que pueden presentarse.

b) Realiza la gestión de riesgos, este paso se deriva de los resultados del análisis de riesgos, se opta por tomar medidas adecuadas con la finalidad de poder prevenir, impedir, reducir o controlar los riesgos identificados disminuyendo así la potencialidad de un riesgo presentado.

2.6.4 Objetivos MAGERIT V

El objetivo principal de Mageritv es la evaluación, homologación y certificación de la seguridad de sistemas de la Información (Ministerio de Hacienda y Administraciones Públicas, 2012), para ello se debe seguir los siguientes objetivos.

a) Concientizar a los responsables del sistema de información la presencia de riesgos y la importancia de mitigarlos a tiempo.

b) Ofrecer un método sistemático para analizar los riesgos, haciendo uso de las tecnologías de la información y comunicaciones (TIC).

c) Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

d) Preparar a la organización para los procesos de evaluación, auditoria, certificación o acreditación según corresponda el caso.

2.6.5 Estructura Magerit

La metodología Magerit V3 consta de 3 libros; método, que se refiere a la parte conceptual del análisis de riesgos, el catálogo de elementos proporciona terminologías y me todos para el desarrollo del análisis de riesgos y guías técnicas, los cuales permiten el buen desarrollo de un

análisis y gestión de riesgos, mediante tablas, algoritmos, diagramas de flujo etc. En la tabla 6 se resume cada uno de estos libros de manera concisa.

Tabla 6

Resumen de los libros de MAGERIT

LIBROS	**DESCRIPCIÓN**
Libro 1: Método	Presenta de manera conceptual el proceso del análisis y gestión de riesgos de forma general.
	Detalla cada uno de los pasos a seguir para la realización del análisis de riesgos y así poder gestionar su mitigación.
	Proporciona recomendaciones prácticas para el desarrollo de cada uno de los procesos a seguir.
Libro 2: Catálogo de Elementos	Proporciona modelos estándares que puedan ser utilizadas como guías para el desarrollo de cada uno de los procesos del proyecto.
	Proporciona una terminología y criterios uniformes con el objetivo de homologar los resultados del análisis.
Libro 3: Guías Técnicas	Describe un conjunto de técnicas específicas como el análisis mediante el uso de tablas, análisis algorítmico, árboles de ataque etc. y generales como el análisis costo-beneficio, diagramas de flujo de datos, diagramas de

	procesos, técnicas gráficas, planificación de proyectos, valoración Delphi etc.

Nota. Se toma los tres libros al realizar un análisis de riesgos. Tomada de Ministerio de Hacienda y Administraciones Públicas (2012).

2.6.6 Fases de la Metodología Magerit

En la Tabla 7 se resume las fases de la metodología Mageritv con cada una de sus tareas a cumplir ya que esta metodología se enfoca en el buen cumplimiento del análisis y gestión de riesgos, con el fin de determinar tanto el análisis de riesgos intrínseco o efectivo que se encuentran presentes en los sistemas de información.

Tabla 7

Fases de la metodología MAGERITV

FASE 1	**DESCRIPCIÓN**	**TAREAS**
Estimación del riesgo intrínseco	Se encarga de analizar la posibilidad de que una amenaza se materialice, sin tomar en cuenta las salvaguardas existentes. Esta fase determina el efecto real de las amenazas.	Identificar y tipificar los activos relevantes de la organización.
		Dimensionar los activos de la organización.
		Realizar la valoración de los activos en cada dimensión.
		Identificar las amenazas que estarían expuestos los activos de la organización.
		Realizar la valoración de las amenazas de cada uno de los activos (degradación y frecuencia).
		Cálculo del valor del impacto al relacionar los parámetros de valor de activo y degradación.
		Cálculo del riesgo intrínseco, al relacionar el impacto y frecuencia, sin tomar en cuenta las salvaguardas existentes.
FASE 2	**DESCRIPCIÓN**	**TAREAS**
Estimación del Riesgo Efectivo	Determina la posibilidad de que una amenaza se materialice, pero éste toma en cuenta las salvaguardas existentes de un sistema informático. Ayuda a determinar los niveles de riesgos actuales	Identificar y tipificar las salvaguardas existentes de tipo preventivo o limitante, que se encuentren implementadas en la organización.
		Evaluar la eficiencia de las salvaguardas no existente, poco efectiva, efectiva y muy efectiva.
		Analizar las métricas de degradación y frecuencia, tomando en cuenta las salvaguardas existentes, para posteriormente utilizar estos valores para el cálculo del impacto y del riesgo efectivo.

Nota. Tomado de Ministerio de Hacienda y Administraciones Públicas (2012).

2.6.6.1 Cuadro comparativo entre metodologías de análisis y gestión de riesgos.

La tabla 8 muestra una comparativa de cada una de las metodologías antes expuestas con el fin de elegir la que mejor se adapte a cada una de las necesidades de la organización, hay que tener en cuenta diferentes aspectos para la elección de una de ellas como sus características, fases, ámbito de aplicación, ventajas y desventajas (Mogollón, 2014).

Tabla 8

Comparativa entre metodologías de análisis de riesgos.

METODOLOGÍA	FASES	APLICACIÓN	VENTAJAS	DESVENTAJAS
OCTAVE	-Visión de organización. -Visión tecnológica -Planificación de medidas de reducción de riesgos.	PYMES	-Metodología auto dirigida, es decir, el análisis y gestión de riesgos se lo realiza a través de un equipo multidisciplinario. - Involucra a todo el personal de la entidad. - Es una de las más completas ya que incluye a su modelo de análisis: procesos, activos y dependencias, recursos vulnerabilidades, amenazas y salvaguardas.	-No toma en cuenta el no repudio. -Utiliza muchos documentos anexos, lo que complica su entendimiento o actualización. -Conocimientos técnicos. - No explica de manera adecuada la definición y determinación de activos de información.
OSSTMM	Seguridad de la información. -Seguridad de procesos. -Seguridad en las tecnologías de internet.	Productos, negocios y servicios	Valores de evaluación de riesgos. -Utiliza fórmulas matemáticas que mejoran la credibilidad del documento.	- Existe únicamente en el lenguaje inglés. - el cambio continuo de versión, actualizan las

	-Seguridad en comunicaciones. -Seguridad inalámbrica. -Seguridad Física.		-Los RAV son cíclicos.	plantillas de documentación. - Cualquier información obtenida por eta metodología no puede ser modificada o vendida sin el consentimiento de ISECOM, se puede hacer uso de esta gratuitamente si se relaciona con pruebas, educación, consultoría o investigación.
MAGERITV	-Análisis de riegos. -Caracterización de activos: amenazas, salvaguardas, estimación del estado del riesgo, gestión de riesgos.	Gobierno, Organismos, compañías grandes, PYME, compañías comerciales y no comerciales.	- Manual en lenguaje español. - Se considera con un alcance completo tanto en el análisis de riesgos como en la gestión. - Posee archivos de inventarios manejables en lo referente a recursos de la información, amenazas y tipo de activo. - Permite un análisis cualitativo y cuantitativo. - No requiere autorización previa a su utilización.	-No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir. - No posee un inventario completo en lo referente a políticas.

Nota. Tomado de Mogollón (2014).

Por consiguiente, tomando en cuenta los aspectos de ámbito de aplicación, fases, ventajas y desventajas se ha realizado la elección de la metodología MAGERITV para la realización del análisis y gestión de riesgos en una organización gubernamental, ya que esta presenta ventajas con respecto a las demás metodologías de análisis de riesgos planteadas.

Por ejemplo. metodología MAGERITV puede ser aplicada en Gobierno, Organismos, compañías grandes, PYME, compañías comerciales y no comerciales, al contrario de OSSTMM que es aplicable a productos, negocios y servicios, mientras que OCTAVE se enfoca básicamente en PYMES. Por otra parte, OSSTMM ofrece la aplicación de fórmulas matemáticas que mejoran la credibilidad del documento; OCTAVE por lo contrario ofrece una metodología auto dirigida, es decir, el análisis y gestión de riesgos se lo realiza a través de un equipo multidisciplinario; Mientras que MAGERITV entre sus múltiples ventajas no requiere de algún tipo de autorización previo a su uso, permite realizar un análisis cualitativo y cuantitativo, trabaja con inventarios detallados de la información recolectada, además de considerarse con un alcance completo tanto en el análisis de riesgos como en la gestión.

2.6.7 Evaluación de los riesgos en la seguridad de la información

Los riesgos en la seguridad de la información son permanentes, ya que al momento que un elemento potencial falle o sea comprometido, este puede provocar efectos insatisfactorios al buen desarrollo del sistema. Es necesario tener una planificación que permita actuar de manera inmediata al momento que algo de esto sucediese, en primera instancia entendiendo el problema, consiguiente detectándolo y controlando (Sánchez, et al., (2003). Entre los riesgos de la seguridad se especifica a la identificación de escenarios, evaluación de riesgos, valoración de activos e impacto de riesgos, consiguiente se define cada uno de estos.

- **Identificación de escenarios.**

La identificación de escenarios hace referencia al reconocimiento de manera general al entorno en el que posible riesgo pueda materializarse, identificando los posibles factores que lo ocasionen. Incluye un estudio detallado que permite tener información acerca de los recursos necesarios para su mitigación, relacionado con la intensidad, magnitud y frecuencia del mismo. Así como las condiciones de fragilidad y resiliencia de los elementos expuestos (población, infraestructura, actividades económicas, entre otros) (CENEPRED, 2015).

- **Evaluación de riegos.**

La evaluación de riesgos se refiere a la realización de una planificación de posibles riesgos que se pudiesen presentar dentro o fuera de una organización, evaluando el costo de un posible daño de los elementos activos de manera individual, para con ello tener un presupuesto anticipado ante un posible fallo. En un principio se debe conocer que se quiere proteger, donde y como, especificando la prioridad de cada uno de los activos de la organización (Aznar, 2016).

- **Valoración de activos.**

La valoración de activos hace referencia al costo original de la adquisición de elementos físicos y lógicos de una organización para que esta pueda funcionar correctamente entorno al ámbito tecnológico, físico o humano. Para el análisis de la valoración de activos se toma en cuenta el costo original del activo, el valor acumulado por pérdida de confidencialidad, disponibilidad e integridad y el impacto generado para la organización por daños o suspensión de los servicios, este se catalogará por niveles dependiendo a su importancia, como crítico, alto, medio y bajo (Méndez, 2015).

- **Impacto de riesgos.**

El impacto de riesgos se define como las consecuencias causadas por la materialización de una amenaza, ya sea en uno o varios elementos activos del sistema. Este impacto puede ser clasificado de manera cuantitativa, que hace referencia al costo económico que pueda causar el impacto al buen funcionamiento de la organización y a su pronta restauración; y cualitativa al impacto no cuantitativo, es decir, esta puede actuar en contra de la integridad de una persona.

2.7 Marco legal y normativo

Este apartado trata la normativa legal Nacional e Internacional referente a la realización del plan de contingencia, se ha tomado en cuenta la Constitución Nacional del Ecuador, secretaria nacional de Riesgos y Emergencias, Normativa de Control Interno de la Contraloría General del Estado, a la Ley de Transparencia y Acceso a la Información Pública, Ley de la Propiedad Intelectual, Código Orgánico Integral Penal y a normativas internacionales como la ISO 27001, 27002 (ISO/IEC 27001, 2013; ISO/IEC 27002, 2013).

2.7.1 Constitución de la República del Ecuador

La Constitución de la República del Ecuador (2008) es una norma jurídica suprema en estado vigente. Reemplazo a la Constitución de 1998, fue redactada entre los años 2007 y 2008 y para su aprobación que fue sometida a un referéndum constitucional.

En la sección cuarta se encuentra el apartado Acción de acceso a la información pública, el cual menciona en su Art. 91

> La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información…" (p. 65).

2.7.2 Código Orgánico Integral Penal

El Código Orgánico Integral Penal (COIP) es un organismo que se encarga de obligar el cumplimiento de normas jurídicas de carácter punitivo, es decir un compendio legislativo que establece la gravedad del delito y establece penas conforme al sistema penal ecuatoriano (COIP, 2014).

Haciendo mención a lo relacionado con la investigación de este proyecto se hace referencia al Art. 190:

> Apropiación fraudulenta por medios electrónicos. - La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes…" (p. 84).

Art 191 "Reprogramación o modificación de información de equipos terminales móviles. - La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años" (p. 84)

> Art. 192:
>
> Intercambio, comercialización o compra de información de equipos terminales móviles. - La persona que intercambie, comercialice o compre bases de datos que contengan Código Orgánico Integral Penal 85 información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años (pp. 84-85).

2.7.3 Secretaria Nacional de Riesgos y Emergencias

La secretaria nacional de Riesgos y Emergencias es una entidad pública que se encarga de garantizar la seguridad de la ciudadanía ante posibles desastres naturales, implementando políticas de seguridad y estrategias que permitan identificar, analizar, prevenir y mitigar riesgos y como

hacer frente a cada uno de estos. La Secretaria de Gestión de Riesgo (2010) menciona “La Gestión de Riesgos es un proceso complejo dirigido a la reducción de los riesgos, al manejo de las emergencias y desastres, y a la recuperación ante eventos adversos que afectan nuestras vidas y recursos” (p. 3). El tener un plan de emergencias institucional es una obligación que deben tener las empresas públicas o privadas, el cual será gran utilidad si se lo lleva a cabo con ayuda del personal de las instituciones (Secretaria de Gestión de Riesgo, 2010).

2.7.4 Normas de control interno de la contraloría general del estado

El desarrollo de la Norma de Control Interno de la Contraloría General del Estado incluye normas generales, y otras especificaciones relacionadas con la administración financiera y gubernamental. El artículo 410 de esta normativa hace referencia al uso de la tecnología de la información, tomando aspectos de gran relevancia como: la organización informática, segregación de funciones, plan informático estratégico de tecnología, políticas y procedimientos, entre otras.

De tal manera su énfasis con respecto a esta investigación se analizará lo referente al plan de contingencia, la cual muestra una idea concisa de la importancia de mantener la continuidad en las actividades y procesos desarrollados en la empresa. La Contraloría General Del Estado (2009) define en su Art. 410-11 que este:

> Corresponde a la unidad de tecnologías de la información de definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión del procesamiento de la información por problemas en equipos, programas o personal relacionado” (p. 73).

Los aspectos a tomar en cuenta en un plan de contingencia que se detallan en esta normativa se muestran a continuación:

a) El plan de respuesta a los riesgos en el cual se incluirá, los roles críticos, con la finalidad de administrarlos, asignación de responsabilidades con respecto a la seguridad de la información, ya sea física o lógica.
b) Definición y ejecución del procedimientos y control de cambios, con el objetivo que el plan de continuidad se mantenga actualizado, para que este sea utilizado cuando se los requiera.
c) Plan de continuidad de operaciones, el cual contará con una infraestructura alterna o de uso compartido con un Data center Estatal, este se hará uso mientras dure la contingencia, restableciendo las comunicaciones, así como también restaurando la información de los respaldos.
d) Plan de recuperación de desastres, el cual se enfoca en las actividades previas al desastre (bitácora de operaciones), actividades durante el desastre (Plan de emergencia, entrenamiento) y las actividades después del desastre.
e) Asignar responsables en cada área, los cuales son encargados de tomar acciones de contingencia en el caso de que ocurra un desastre.
f) El plan de contingencia será documentado de manera confidencial para la empresa, el cual contendrá procedimientos a seguir en caso de que ocurra una emergencia intencional o no intencional que afecte el correcto funcionamiento de la empresa, la aplicación del plan de contingencia permitirá la pronta restauración del sistema y la recuperación a un nivel aceptable de la información afectada durante el evento, asegurando con ello la integridad y seguridad de la información.

g) Al momento que el plan de continuidad sea aprobado por las personas encargadas, este será difundido hacia el personal responsable de su ejecución y será sometido a pruebas que verifiquen su correcto funcionamiento.

2.7.5 Ley orgánica de transparencia y acceso a la información pública

Tomando como referencia el Art. 81 de la Constitución Política del Ecuador, que garantiza el derecho del acceso a las fuentes de información, para ejercer una participación democrática con respecto a la información pública (LOTAIP, 2004). Los aspectos más relevantes para tomar en cuenta en esta ley son:

a) El acceso a la información pública es un derecho de las personas que garantiza el estado.
b) La ley tiene la obligación de hacer efectivo el principio de publicidad de contratos, acciones y gestiones de instituciones del Estado que son financiadas con recursos públicos.
c) Esta ley se rige a todos los organismos que conforman el sector público, personas jurídicas cuyas acciones sean parte del estado, fundaciones y ONGs que mantengan convenios con cualquier entidad estatal.
d) La entrega de información se encuentra limitada por un plazo de 10 días, con prorroga de 5 días más debidamente justificados.
e) Los funcionarios públicos señalados en el Art. 1 de la ley orgánica de transparencia y acceso a la información pública, que nieguen el acceso a la información pública, serán sancionados según la gravedad de la falta, las cuales se detallan a continuación:
    - Multa equivalente a un mes de sueldo o salario que perciba en la fecha de la sanción.
    - Suspensión temporal de sus funciones por un lapso de 30 días calendario, si derecho a remuneración.
    - Destitución del cargo en caso de no acceder a la entrega de información, después de las sanciones anteriormente expuestas.

2.7.6 Ley de Propiedad Intelectual

Según la Organización Mundial de la propiedad Intelectual, se define como toda creación que proviene de la mente humana, tales como las obras artísticas, literarias, científicas, e industriales, así como también los nombres, logos, imágenes que puedan ser utilizados para la comercialización de un producto (SENADI, 2019)**.**

El Servicio Nacional de Derechos Intelectuales (SENADI) es el encargado de dar seguimiento a que se cumplan cada uno de las normativas impuestas en la Ley de Propiedad Intelectual, y que ser cumplida por personas nacionales o extranjeros, domiciliarios o no en el Ecuador (SENADI, 2019)**.**

La Ley de Propiedad Intelectual menciona en su Art. 1 que "El Estado reconoce, regula y garantiza la propiedad intelectual adquirida de conformidad con la ley, las Decisiones de la Comisión de la Comunidad Andina y los convenios internacionales vigentes en el Ecuador" (p. 1)**.**

2.7.7 Análisis de la norma técnica ISO/IEC 27001

Es una norma a nivel internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de la misma, en la última actualización de esta normativa se ha incluido la evaluación y aprendizaje de los eventos de seguridad TI que se centra en la respuesta a incidentes (ISO/IEC 27001, 2013).

- Sistemas de Gestión de la Seguridad de la Información.

La ISO/IEC 27001 para los sistemas de gestión de seguridad se encarga de la asegurar la disponibilidad, confidencialidad e integridad de la información, permite además, a las organizaciones la realización de un análisis de riesgo y la aplicación de controles necesarias para contrarrestarlos (ISO/IEC 27001, 2013). Es así que, la estructura de la norma ISO/IEC 27001

cuenta con 14 dominios, 35 objetivos de control, y 114 controles; los dominios deben ser evaluados incluyendo los siguientes objetivos:

- Dominio de la política de seguridad requiere dependencia de poseer un compromiso acerca de la relevancia de la seguridad de la información.
- Dominio de la organización en cuanto a la seguridad de la información.
- Dominio de gestión de activos.
- Dominio de seguridad de los recursos humanos.
- Dominio en cuanto la seguridad física y del medio ambiente.
- Dominio de gestión de las comunicaciones y operaciones.
- Dominio de control de acceso es uno de los objetivos más importantes de cumplir.
- Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información.
- Dominio de gestión de incidentes en la seguridad de la información.
- Dominio de gestión de continuidad del negocio.
- Dominio de cumplimiento.

2.7.8 Análisis de la norma técnica ISO/IEC 27002

La ISO/IEC 27002 es un estándar para la seguridad de la información publicada por la Organización Internacional de Normalización y la comisión Electrotécnica Internacional, su versión más reciente fue publicada en al año 2013. Esta normativa proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a las organizaciones interesadas en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información (ISO/IEC 27002, 2013). En Ecuador existe el Esquema Gubernamental de la Seguridad de la Información (EGSI), el cual está basado a la norma ecuatoriana INEN ISO/IEC 27002 para la gestión de seguridad de la información y está dirigido a Instituciones de Administración pública.

La normativa ISO/IEC 27002 cuenta con 14 dominios, 35 objetivos y 114 controles, los cuales se han adecuado de la mejor manera para que la aplicación de la misma sea óptima. Entre estos están las Políticas de seguridad, Aspectos organizativos de la seguridad de la información, Gestión de activos, Seguridad ligada a los recursos humanos, Seguridad física y del entorno, Gestión de comunicaciones y operaciones, Control de acceso, Adquisición, desarrollo y mantenimiento de sistemas de la información, Gestión de incidentes en la seguridad de la información, Gestión de la continuidad del negocio y Cumplimiento.

CAPITULO III

3 Análisis de la Situación Actual de la red de datos del GADM San Miguel de Ibarra.

Este capítulo hace referencia a la recopilación de información actualizada acerca del estado actual de la infraestructura tecnológica, enfocándose primordialmente al Data Center del edificio matriz del Gobierno Autónomo Descentralizado San Miguel de Ibarra. Obteniendo la información de fuentes confiables, para hacer uso de ella con responsabilidad y respetando la confidencialidad de la misma.

3.1 Descripción general del Gobierno Autónomo Descentralizado San Miguel de Ibarra

El Gobierno Autónomo Descentralizado San Miguel de Ibarra (GADM San Miguel de Ibarra), se encuentra ubicado entre las calles Simón Bolívar y García Moreno (esquina), como se muestra en la Figura 4. Su edificación central cuenta con tres plantas en las cuales se distribuyen cada uno de los departamentos que cumplen diferentes funciones de acuerdo a su dependencia, éstas trabajan conjuntamente para ofrecer un buen desempeño en cada uno de los servicios brindados por esta entidad. A continuación, se presenta la misión y visión del GADM San Miguel de Ibarra.

Figura 4 *Mapa de la ubicación geográfica del GAD-Ibarra*

Nota. Tomada de Google Maps (2023)

- **Misión del GAD San Miguel de Ibarra**

Somos un gobierno municipal que promueve el desarrollo y bienestar integral de la comunidad con servicios de calidad y calidez, de manera eficiente, honesta y responsable. Involucrando la participación ciudadana en pro del bien común del cantón Ibarra (GADM San Miguel de Ibarra, 2023)**.**

- **Visión del GAD San Miguel de Ibarra**

En el año 2023 seremos un gobierno municipal transparente, seguro, humano, inclusivo, participativo y moderno. Promoviendo el desarrollo social, económico y productivo en beneficio del cantón Ibarra, convirtiéndonos en un referente nacional de la gestión pública (GADM San Miguel de Ibarra, 2023)**.**

Distribución Departamental

En la Tabla 9, se detalla la distribución de cada uno de los departamentos del GADM San Miguel de Ibarra, clasificándolos por el número de planta, tipo de departamento y descripción del mismo. Cabe recalcar que la información mostrada en esta Tabla 9 corresponde a los departamentos del edificio matriz, que fue recolectada por medio de carteleras informativas colocadas en cada planta de la institución.

Tabla 9

Distribución departamental en las instalaciones del GAD-IBARRA

PLANTA	DEPARTAMENTO	DIRECCIÓN
Baja	Parqueadero Institucional	
Primera	Administración de Gestión Presupuestaria	Dirección Financiera
	Administración de Gestión de Tesorería	
	Administración de Gestión Contable	
	Unidad de Servicios Tributarios	

Segunda	Recepción de Documentos	
	Coordinación de Seguridad y Salud en el Trabajo	Dirección de Talento Humano
	Unidad de Administración de Talento Humano	
	Unidad de Seguridad Industrial y Salud Ocupacional	
	Unidad de Desarrollo de Talento Humano	
	Coordinación de Formación Ciudadana	Dirección de Participación Ciudadana e Inclusión Social
	Coordinación de Vinculación Social y Deliberación	
	Coordinación de Presupuesto Participativo	
	Coordinación de Inclusión Socia	
	Unidad de Intervención Social	
	Archivo	
	Unidad de Administración de Activos Fijos	Dirección Administrativa
	Unidad de Administración de Existencias	
	Unidad de Contratación Pública	
	Unidad de Servicios Generales	
	Gestión Financiera	Dirección Financiera
	Procuraduría Síndica	Unidad de Asesoría Jurídica
	Secretaría de Consejo	Consejos Cantonales
	Alcaldía	Concejo Municipal
	Gestión de comunicaciones y RRPP.	
	Secretaría de Comisiones	
Tercera	Unidad de Patrimonio Natural	Dirección de Gestión Ambiental
	Unidad de Calidad Ambiental y Áridos y Pétreos	
	Unidad De Residuos Sólidos	
	Unidad de Fiscalización	Dirección de Obras y Construcciones
	Unidad de Construcciones	
	Unidad de Mantenimiento Vial	
	Unidad de Catastro Urbana	Dirección de Avalúos y Catastros
	Unidad de Catastro Rural	

	Unidad de Desarrollo de Software	Dirección de Tecnologías de la Información
	Unidad de Infraestructura y Comunicaciones	

Nota. Fuente: GAD-Ibarra San Miguel de Ibarra 2023.

Así mismo, el GADM San Miguel de Ibarra, cuenta con sucursales departamentales fuera del edificio matriz, los cuales complementan a la institución para mejorar el servicio a la ciudadanía. En la Tabla 10 se detalla cada uno de estos.

Tabla 10

Sucursales Departamentales del GAD-IBARRA

SUCURSAL	**DESCRIPCIÓN**
Centro de revisión vehicular	Comisaria de construcciones
Fe de Ligas	Activos Fijos
Bodega Municipal	Mecánica
	Unidad de activos de desechos solidos
	Seguridad ocupacional
	Oficinas de Bodega
Parque Ciudad Blanca	Suministros
	Casa de los derechos
Casa de la Ibarreñidad	Departamento de cultura
	Radio Municipal
Teatro Gran Colombia	Seguridad Ciudadana
CECAMI	Centro de capacitación municipal
Mercado Amazonas	Administración de mercados
Esquina del coco	Dirección de Turismo actualizar

Nota. Fuente: GADM San Miguel de Ibarra (2023)

3.1.1 Servicios prestados por el GADM San Miguel de Ibarra.

Al ser una entidad pública el GAD San Miguel de Ibarra brinda diferentes servicios, los cuales son indispensables para que la población pueda realizar sus funciones diarias y cumplir con sus obligaciones. En la Tabla 11 se muestra los servicios más relevantes proporcionados por la institución. Obteniendo esta información de manera verbal de parte del personal de la Dirección de Tecnologías de la Información.

Tabla 11

Servicios prestados por el GADM San Miguel de Ibarra.

SERVICIOS	**DESCRIPCIÓN**
Administración de Mercados	Administración y gestión del buen funcionamiento de los mercados de la ciudad.
Permisos de funcionamiento de instalaciones con carácter comercial o institucional.	Otorgación de permisos de funcionamiento de locales comerciales.
Pago de impuestos.	Recaudación de impuestos de la ciudadanía sin fines de lucro.
Servicios de redes inalámbricas en espacios públicos.	Servicios de internet inalámbrico a espacios públicos urbanos y rurales del cantón.
Avalúos y Catastros.	Sistema que se encarga de registrar de manera lógica, georreferenciada y ordenada la información acerca de los catastros urbanos y rurales.
Biblioteca.	Espacio de la Municipalidad que brinda servicios de préstamo de libros, revistas o equipos informáticos.
SISMERT	Encargada del cobro del parqueo tarifado en la ciudad de Ibarra.
Dirección de Salud	Atención médica a empleados de la institución.
Procuraduría Síndica	Administraciones legales de contratos, revisión de ordenanzas, presupuestos, asesorías legales, etc.
Control Ambiental	Se encarga del buen manejo de los desechos generados en el cantón, en base a normativas de control ambiental.
Obras Públicas	

Nota. Fuente: Dirección de Tecnologías de la Información (2022).

3.1.2 Servicios consumidos por el GADM San Miguel de Ibarra

Para el buen desarrollo de las actividades diarias de los funcionarios del GADM San Miguel de Ibarra, es necesario recurrir a la adquisición de servicios externos. En la Tabla 12 se detalla los servicios adquiridos por esta entidad con su número de contacto.

Tabla 12

Servicios consumidos por el GADM San Miguel de Ibarra.

EMPRESA	SERVICIO	DIRECCIÓN	TELÉFONO
EMEL NORTE	Electricidad	Eusebio Borrero y Manuel de la chica Narváez, esquina.	(06) 299-7100
EMAPA	Agua Potable	Antonio José de Sucre 777 y Pedro Moncayo.	(06) 295-1670
IESS	Seguridad Social	Sánchez y Cifuentes y Pedro Moncayo.	(06) 260-3266
Policía Nacional	Seguridad	Sánchez y Cifuentes Nº125 y Jaime Roldós Aguilera (esquina)	911
Bomberos	Emergencias	Av. Víctor Manuel Peñaherrera y Luis Fernanda Villamar.	
TELCONET		Francisco Salazar, Quito	(02) 396-3100
SAITEL		José Olmedo y Germán Grijalva	
Correos del Ecuador	Mensajería	Salinas N°6-71 y Oviedo	(06) 264-3135
Banco del Pacifico	Financiero	Pedro Moncayo y José Olmedo	(06) 295-7031
Mutualista Imbabura		Miguel Oviedo 7-29 y Bolívar	(06) 295-0522
Banco del Austro		Cristóbal Colón y Bolívar	(06) 264-2172
SRI	Pago de Impuestos	Simón Bolívar (Parque Pedro Moncayo)	(06) 295-5031
REGISTRO CIVIL	Cedulación	Juan de Velasco y Vicente Rocafuerte	(06) 373-1000

Nota. Fuente: GADM San Miguel de Ibarra (2023)

3.2 Organigrama de la Institución

El GADM San Miguel de Ibarra, en su estructura organizativa actualizada en el 2023 (GADM San Miguel de Ibarra, 2023) ha clasificado cada una de sus dependencias en 4 partes (ver ANEXO 1) las cuales se divide en gobernantes, habilitantes de asesoría, agregadores de valor y habilitantes de apoyo.

En la sección de GOBERNANTES, se encuentran los consejos cantonales de salud, protección de derechos, seguridad ciudadana y planificación, del mismo modo, alcaldía donde se despliega la secretaria general, auditoría interna, asesoría técnica y la unidad de asesoría jurídica.

En la sección de HABILITANTES DE ASESORÍA, se encuentran la dependencia de coordinación general donde se encuentran las direcciones de participación ciudadana, macroproyectos, gestión estratégica y relaciones externas, comunicación y relaciones públicas y planificación de desarrollo urbano y rural.

En la sección de AGREGADORES DE VALOR, están las direcciones de cultura y educación, gestión ambiental, avalúos y catastros, deportes y recreación, obras y construcciones y desarrollo económico local e inclusión social.

Por último, la sección HABILITANTE DE APOYO, se encuentra la dirección administrativa, gobernabilidad y seguridad ciudadana, talento humano, tecnologías de la información y financiera.

Los cuales en su conjunto hacen que la funcionalidad de esta institución sea eficiente y eficaz, de manera continua y permanente, por este motivo, el presente proyecto está enfocado a la realización de un plan de contingencia para brindar una continuidad del servicio TI, hacia los usuarios internos y externos, por lo cual se lo llevará a cabo en la Dirección de Tecnologías de la Información de esta entidad, ya que éste desarrolla, administra y gestiona cada uno de estos

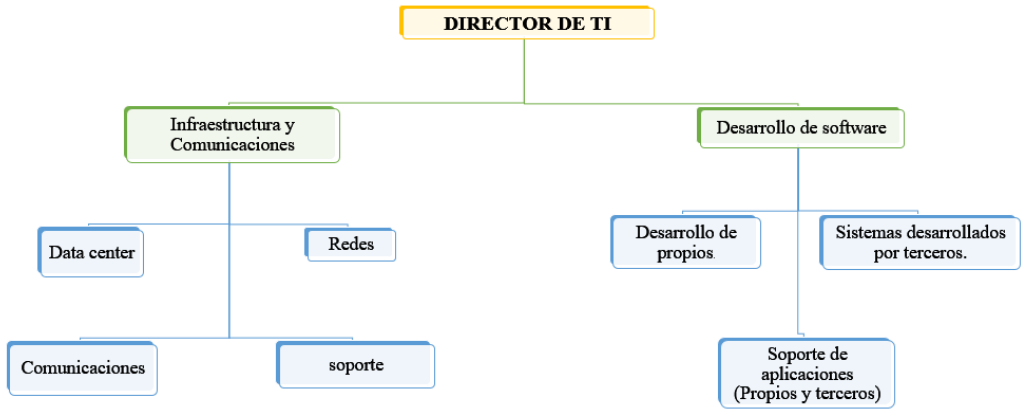
servicios, es por esto que a continuación se presenta la información de la situación actual de esta dependencia.

3.2.1 Organigrama de la Dirección de Tecnologías de la Información del GADM San Miguel de Ibarra.

La Dirección de Tecnologías de la Información se encuentra ubicada en la sección *"Habilitantes de Apoyo"*, la cual está formada por el Director de TI y dos dependencias, la primera es Infraestructura y Comunicaciones, donde se encuentra las instalaciones del Data Center, redes, comunicaciones y soporte; la segunda, es la dependencia de desarrollo de software, la cual se dedica a la realización de software para el uso de la institución, además del desarrollo de sistemas y soporte de aplicaciones propias y de terceros (GADM San Miguel de Ibarra, 2023). En la Figura 6 se muestra el organigrama actual de la Dirección de Tecnologías de la Información del GADM San Miguel de Ibarra.

Figura 5

Organigrama de la Dirección de tecnologías de la Información.



Nota. Fuente: Dirección de Tecnologías de la Información GADM San Miguel de Ibarra (2022).

3.3 Estructura actual de la red de datos

En la actualidad el GADM San Miguel de Ibarra cuenta con una infraestructura de red cableada e inalámbrica, las cuales proveen servicios de internet e intranet a los diferentes departamentos de la institución por medio de redes locales, estas redes están interconectadas por medio de fibra óptica dentro de la institución, así como también en las sucursales descritas en la Tabla 10 de este documento; de igual manera se hace uso de las redes inalámbricas con el fin de brindar servicios en los diferentes espacios dentro y fuera de la institución.

3.3.1 Cuarto de telecomunicaciones

El cuarto de telecomunicaciones del GADM San Miguel de Ibarra se ha definido como un TIER 3, el cual certifica su disponibilidad garantizada del 99.982%, estas instalaciones se encuentran ubicados en el tercer piso del edificio matriz. Éste cumple con especificaciones impuestas en la normativa TIA-942, la cual dispone de un diseño eléctrico, control ambiental, protección contra riesgos físicos, almacenamiento de datos además de control de accesos; la red local de datos está basada a la tecnología ethernet.

El Data Center cuenta con un área de $12m^2$, posee mecanismos de redundancia los cuales son 1 UPS de 8KVA y un generador eléctrico, éste abastece alrededor de 48 horas después del corte de energía, el UPS entra en funcionamiento de manera inmediata al detectar un corte eléctrico, ya que el generador eléctrico toma 1 minuto en activarse; además, posee aire acondicionado con una temperatura de precisión y uno de confort de reserva que trabaja a 17°C. En la Tabla 13 se describe los equipos que se encuentran en el cuarto de telecomunicaciones.

Tabla 13

Equipos del Data Center

UBICACIÓN	EQUIPO	MARCA	MODELO	CANTIDAD
DATA CENTER	FIREWALL CHECK POINT 4600	CHECKPOINT	4610	1
DATA CENTER	SMART EVENT	CHECKPOINT	SMART 1.5	1
DATA CENTER	SWITCH CORE CHASSIS	CISCO	4503 -E	1
DATA CENTER	ROUTER BORDER	CISCO	2800	1
DATA CENTER	SWITCH ADMINISTRATION	CISCO	X4013-TS	1
DATA CENTER	SWITCH DISTRIBUTION	CISCO, 2 COM	X4548-GB, 4500G	2
DATA CENTER	SWITCH DE ACCESSO	CISCO. 3 COM	WSC296048PSTL, WSC296024TCS, 5500 SI 52P, 4250T	6
DATA CENTER	CHASIS BLADE	HP	C 3000	1
DATA CENTER	ONBOARD ADMINISTRATOR	HP	SERVIDOR BLADE HP BLADESYSTEM ONBOARD ADMINISTRATOR	1
DATA CENTER	ONBOARD ADMINISTRATOR BACK UP	HP	SERVIDOR BLADE HP BLADESYSTEM ONBOARD ADMINISTRATOR BACK UP	1
DATA CENTER	BLADE SWITCH	HP	BLADE GBE2C LAYER 2/3 ETHERNET	1
DATA CENTER	BLADE SWITCH BAY 2	HP	BLADE GBE2C LAYER 2/3 ETHERNET	1
DATA CENTER	SAN SWITCH	HP	HP B-SERIES 8/12 C SAN SWITCH BLADESYSTEM C-CLASS BAY 3, HP B-	2

			SERIES 8/12 C SAN SWITCH BLADESYSTEM C-CLASS BAY 4	
DATA CENTER	SWITCH LAN 1 DELL HYPER CONVERGENCIA	DELL	S4128F-ON	2
DATA CENTER	SWITCH SAN DELL	DELL	DS-6610B	1
DATA CENTER	SERVIDORES FÍSICOS	HP, DEL	NODE R740XD, BLADE 460 C GEN 9 BAY 2, DL 380 G6, DL 160 G5, ML 150 G6, DL 380 G7, HP DL 380 G6 - G5, BL 460 G6, P2000G3 FC/ISCS, MSA2040.	22
DATA CENTER	SERVIDORES VIRTUALES	VIRTUALES	SO V CENTER 7, UBUNTU	84
			TOTAL	131

Nota. La información planteada en esta tabla se la obtuvo mediante fichas de recolección de datos. Ver ANEXO 3. Fuente: GADM San Miguel de Ibarra (2023).

3.3.2 Cableado de datos, horizontal y vertical

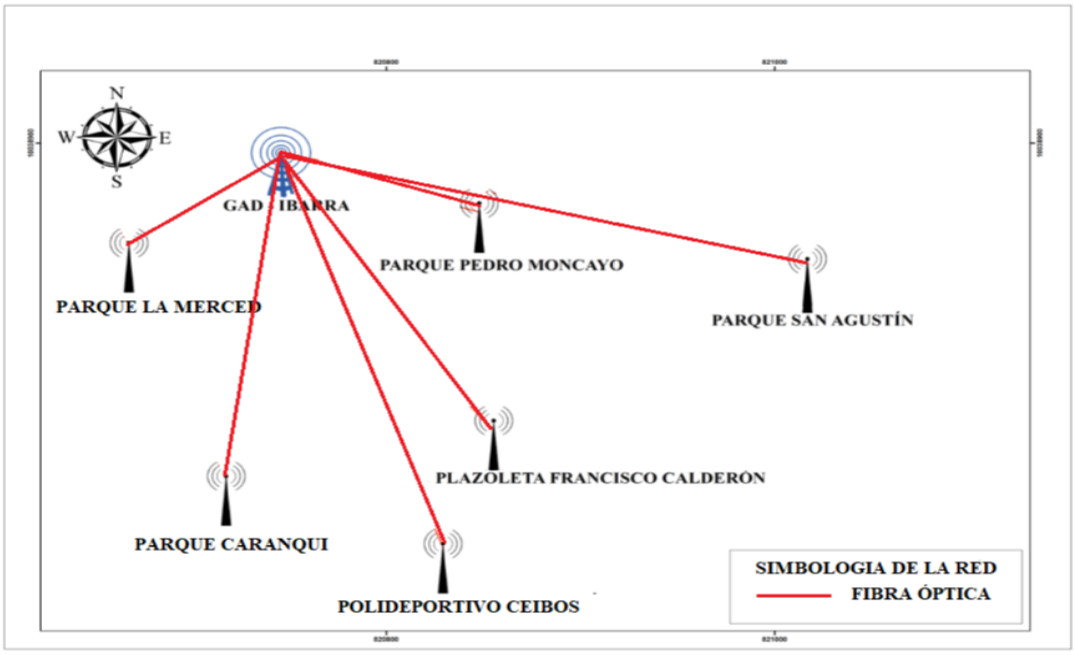
El cableado horizontal y vertical de la municipalidad se encuentra constituido por cable UTP categoría 6A y fibra óptica. Éstos en su conjunto permiten que la municipalidad brinde servicios tecnológicos eficientes y permanentes:

El cableado horizontal se encuentra instalado desde el área de trabajo hasta el cuarto de telecomunicaciones, el cual no sobrepasa la distancia de 90 m, los cables son transportados por medio de paredes cubiertos por canaletas plásticas o a su vez por tubería de ¾ pulgadas las cuales se encuentran de manera interna en las paredes, además se hace uso de rejillas metálicas instaladas en el techo de las áreas de trabajo para brindar conexión entre el edificio matriz y el centro cultural El Cuartel; para los equipos terminales se tiene colocados cajetines sobrepuestos simples y dobles con salidas RJ-45; en ciertos casos se incumple con el radio de curvatura dispuesto en la normativa ANSI/EIA/TIA 569-A ya que este diámetro de curvatura debe ser al menos cuatro veces el diámetro exterior del cable, es decir, el cable categoría 6A tiene un diámetro exterior de 0.25” por lo cual el radio de curvatura debería ser de 1” aproximadamente 25.4 mm

Por otra parte, el cableado vertical o backbone cumple la función de interconectar el cableado horizontal con cada una de las plantas del edificio principal por medio de cable UTP o fibra óptica que se encuentra construido por ductos y bandejas, que además brinda una mayor protección a los cables de comunicación ante posibles afectaciones físicas con el paso del tiempo, el backbone se comunica a través de fibra óptica con equipos instalados en edificios externos como en el Centro Cultural El Cuartel (planta baja), Dirección de Turismo, Planificación y la Dirección de Cultura (Casa de la Ibarreñidad, tercer piso) y diferentes parques ubicados alrededor de la ciudad como se muestra en la Figura 8.

Figura 6

Enlaces de Fibra Óptica brindados por el GADM San Miguel de Ibarra.



Nota. Tomado de Dirección de Tecnologías de Información (2022)

Los cuales llegan al área de distribución principal ubicada en el Data Center del edificio central (tercer piso), cabe recalcar que la municipalidad no cumple con una certificación de cableado estructurado, pero cuenta con la etiquetación pertinente de todos los equipos, facilitando la identificación de cada uno de los medios de transmisión de inicio a fin. Por último, en el aspecto de puesta y conexiones a tierra, la municipalidad cumple con los requerimientos dispuestos en la norma ANSI/TIA/EIA-607, que sugiere la creación de caminos adecuados con la capacidad de dirigir corrientes eléctricas y altos voltajes hacia la tierra, salvaguardando así, la integridad de las personas y equipos de comunicación.

3.3.3 Topología física de la red

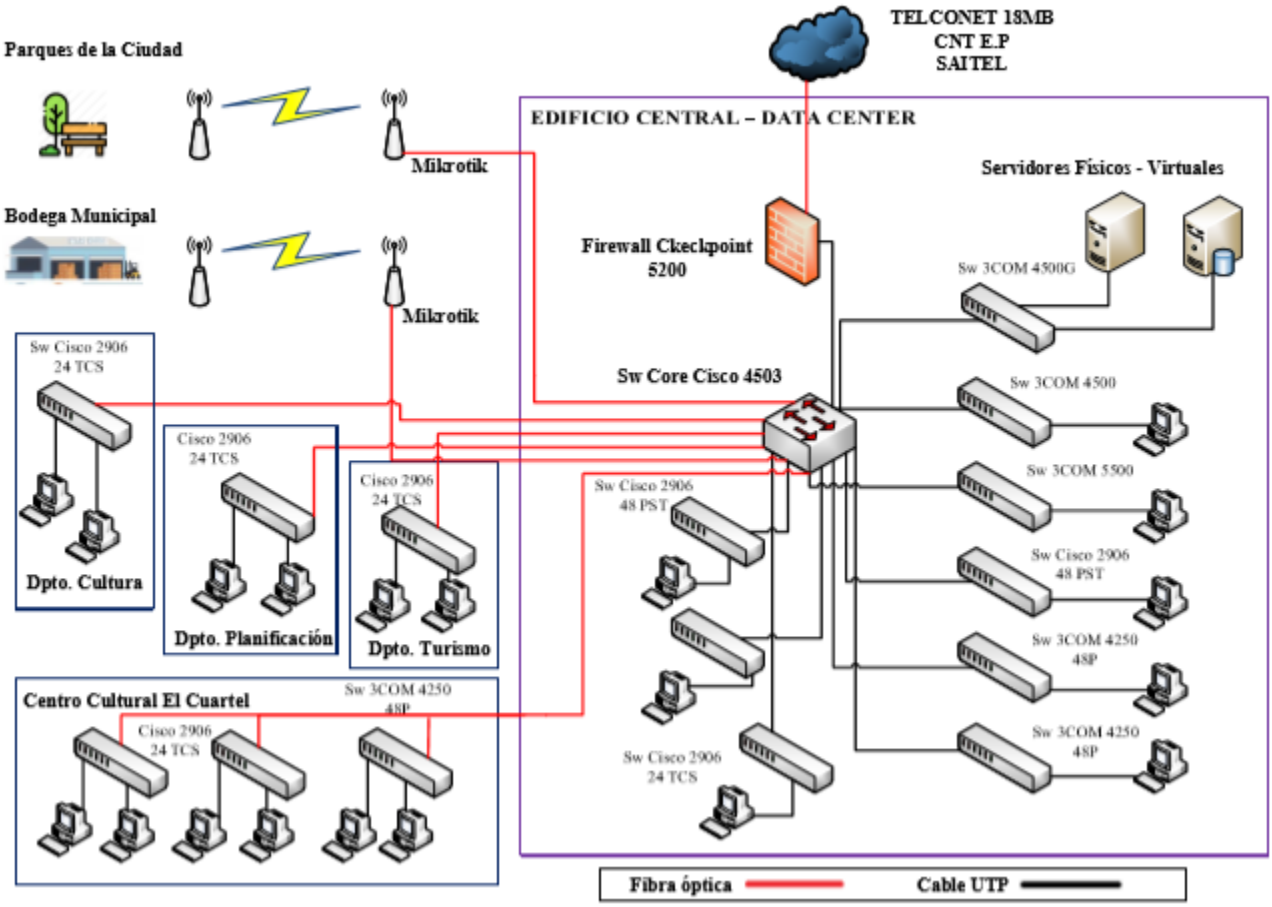
La topología física de la red cableada está configurada en árbol, la cual cuenta con una switch capa 3 central, esta topología permite la interconexión de todos sus nodos, la falla de uno

de estos no afectará al funcionamiento de los demás ya que trabaja en modo difusión y por ende la información se propaga en todas las estaciones.

Por ello, esta red está en la capacidad de transmitir y receptar señales de voz, datos y video, acceso a internet, además de permitir la compartición de archivo, servicios de correo, base de datos, web, financiero, sistemas administrativos entre otros. Cabe destacar que la red del GADM San Miguel de Ibarra en toda su extensión está conformada por el protocolo ipv4. El proveedor de servicio de internet principal es TELCONET el cual proporciona un ancho de banda de 160 Mbps por medio de fibra óptica, que través de un Switch Core de marca Cisco modelo 4503 que distribuye el servicio, como se muestra en la Figura 7.

Figura 7

Topología física GADM San Miguel de Ibarra.



Nota. Fuente: Jácome (2019).

3.3.4 Análisis de la infraestructura lógica de la red de datos.

La red LAN del GADM San Miguel de Ibarra, está compuesta por un direccionamiento IPV4 de clase B, su red principal es 172.16.8.0 con una máscara de red 255.255.248.0 (2048 host disponibles) que se le ha considerado como la VLAN general, a la red también está incorporada la VLAN denominada *"TICS"* la cual trabaja en la red 172.19.4.0 con máscara 255.255.255.0 (254 host disponibles) y la VLAN denominada *"VIDEO"* ésta trabaja en la red 172.19.4.0 con máscara 255.255.255.0 (254 host disponibles). Hasta el momento este rango de direcciones IP satisface las

necesidades de los usuarios, ya que el equipamiento permite también al administrador la escalabilidad y crecimiento de red.

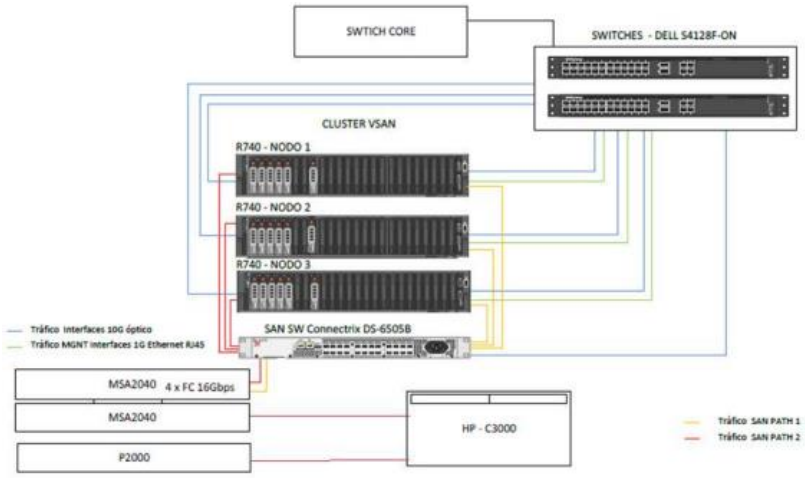
3.3.5 Implementación de Hiper convergencia en el Data Center del GAD-IBARRA.

La Hiper convergencia implementada en el GAD-Ibarra se encarga de centralizar el software de los recursos se computación, almacenamiento y virtualización en un único sistema que generalmente es de hardware x86. La ventaja de la implementación de la Hiper convergencia es que ya no se tiene que gestionar equipos de software por separado y esto permite tener una mejor administración de la red y facilitar al administrado manejar la información de todos los equipos incluidos en este sistema.

El GAD-Ibarra hace uso de la herramienta Vcenter server la cual permite crear cluster vSAN y HA, es necesario también hacer uso de switches Hiper convergencia, switch SAN, creación de Vdisk, instalación de sistemas de respaldo Veeam Back up e incluir las máquinas virtuales al sistema hiper convergente.

En la Figura 6 se muestra como esta implementado físicamente dentro del Datacenter los equipos que cumplen la función de Hiperconvergencia.

Figura 6 Estructura física de equipos de Hiperconvergencia implementados por el GAD-Ibarra



3.3.6 Proveedores de internet hacia el GADM San Miguel de Ibarra

Existen 2 proveedores de internet hacia el GADM San Miguel de Ibarra, los cuales son: SAITEL y TELCONET. El proveedor de servicio TELCONET llega por medio de fibra óptica con un ancho de banda de 160 Mbps hacia un switch de capa 3 que se encuentra en el Data Center, este se encarga de suministrar el servicio dentro del edificio central. A su vez SAITEL suministra el servicio por medio de fibra óptica de 2 hilos con un ancho de banda de 80 Mbps, el cual se conecta a un router Mikrotik de manera cableada a la antena de la municipalidad, de ella se desprende el servicio punto a punto de internet por fibra óptica hacia los diferentes parques urbanos de la cuidad como: Pedro Moncayo, La Merced, Polideportivo los Ceibos, San Agustín, Caranqui, plazoleta Francisco Calderón, con una velocidad de 1 GB hasta el punto.

Tabla 14

Parroquias urbanas y rurales del cantón Ibarra

PARROQUIAS DEL CANTÓN IBARRA

PARROQUIAS URBANAS		PARROQUIAS RURALES	
1	Caranqui	1	Ambuquí
2	Guayaquil de Alpachaca	2	Angochagua
3	Sagrario	3	La Esperanza
4	San Francisco	4	Salinas
5	La Dolorosa del Priorato	5	San Antonio

Nota. Fuente: Dirección de Tecnologías de la Información GADM San Miguel de Ibarra (2022).

Por consiguiente, mediante entrevistas al personal técnico de la Dirección de Tecnologías de la Información, se pudo recolectar la información de los enlaces alámbricos e inalámbricos que brinda la municipalidad a dependencias externas.

Nota. Fuente**:** Dirección de Tecnologías de Información GADM San Miguel de Ibarra (2022).

3.4 Activos de Hardware del Data Center

Entre los activos de hardware se encuentran los servidores, routers, switch, PCs, impresoras, escáner entre otros. A continuación, se detallan los equipos más relevantes para una red de comunicación.

- **Servidores**

Actualmente el Data Center del GADM San Miguel de Ibarra cuenta con 22 servidores físicos y 84 virtuales (ANEXO 2), lo cuales permiten brindar servicio tecnológicos internos y externos.

- **Switch**

Los equipos de conmutación son administrables, su conexión se encuentra en modo jerárquico como se muestra en la Tabla 15, por lo tanto, esta red se divide en 3 capas que cumplen funciones específicas, permitiendo a la red un crecimiento y mantenimiento de manera fácil y adecuada. Su principal conexión sale de un switch de Core, seguido por un switch de distribución y finalmente hacia los switches de acceso.

Tabla 15

Jerarquía de la Red del GAD de Ibarra.

JERARQUÍA	MARCA	MODELO
Core	Cisco	4503 –E
Distribución	CISCO	X4013-TS
Acceso	CISCO. 3 COM	WSC296048PSTL, WSC296024TCS, 5500 SI 52P, 4250T

Nota. Fuente: Dirección de Tecnologías de Información GADM San Miguel de Ibarra (2022).

Dentro del modo jerárquico en la sección de acceso se encuentran también el equipamiento inalámbrico, por lo cual se detallan cada uno de estos activos a continuación:

- **Accesos Inalámbricos Wifi GAD-IBARRA.**

Para comunicación dentro de la municipalidad también se hace uso del medio inalámbrico, por lo cual se ha implementado Access Point en cada departamento con la finalidad que cubran el servicio de internet inalámbrico. Es así que, existen 37 puntos habilitados (GAD-Ibarra, 2023), en la Tabla 16 se muestra cada uno de estos con su marca y lugar de ubicación

Tabla 16

Equipos inalámbricos del GAD IBARRA

N° EQUIPO	MARCA	UBICACIÓN	CANTIDAD
1	Ubiquiti AP-LR	Avalúos y catastros	2
2	Ubiquiti AP-LR	Dirección de TICS	1
3	Ubiquiti AP-LR	Obras Públicas	1
4	Ubiquiti AP-LR	Sala de Concejo	1
5	Ubiquiti AP-LR	Dirección Financiera	1
6	Ubiquiti AP-LR	Ingreso GADI	1

7	Ubiquiti AP-LR	Auditorio Ms Leónidas	1
8	Ubiquiti AP-LR	Medio Ambiente	1
9	Ubiquiti AP-LR	Alcaldía	1
10	Ubiquiti AP-LR	Comunicación Social	1
11	Ubiquiti AP-LR	Participación Ciudadana	1
12	Ubiquiti AP-LR	Secretaria de Comisiones	1
13	Ubiquiti AP-LR	Dirección Administrativa	1
14	Ubiquiti AP-LR	Salón Rojo	1
15	3 COM	Dirección de TICS	1
16	Mikrotik Groove 5hpnd	Vice Alcaldía	1
17	Mikrotik Groove 5hpnd	Alcaldía	1
18	TPLINK 941 ND	Secretaria de Comisiones	1
19	Ubiquiti AP-LR	Desarrollo Económico	1
20	Mikrotik Groove 5hpnd	Auditorio Casa de la Ibarreñidad	1
21	Ubiquiti AP-LR	Auditoría Interna	1
22	Cisco WAP4410N	Dirección Cultura	1
23	TPLINK 941 ND	Consejo de la Salud	1
24	Cisco Linksys E2500	Bodega Municipal Transporte	1
25	Ubiquiti AP-LR	Cuartel Antiguo Administración	1
26	Ubiquiti AP-LR	Comisaria de Construcciones	1

27	Ubiquiti AP-LR	Unidad de Medio Ambiente	1
28	Cisco Linksys E2500	Macroproyectos	1
31	Ubiquiti AP-LR	Seguridad Ocupacional	2
32	Mikrotik Groove 5hpnd	Centro Emprendedores	1
32	Mikrotik Groove 5hpnd	Comité de Fiestas	1
34	Ubiquiti M2	Teatro Gran Colombia Transmisiones	1
35	Mikrotik Groove 5hpnd	Transmisión	1
		Total	37

3.5 Activos de Software

Los activos de software dependen de las funciones que se desempeñan en los departamentos del GADM San Miguel de Ibarra, estos pueden ser licenciados o a su vez desarrollados por el personal de la Dirección de Tecnologías de la Información, en la Tabla 17 se describe el tipo de software utilizado.

Tabla 17

Activos de Software del GADM-IBARRA

APLICACIÓN	DESCRIPCIÓN
Antivirus ESET 9	Licenciado
Microsoft Windows server 2012	Equipos Licenciados

Microsoft Windows server 2022	Equipos Licenciados
ArcGIS	Licenciado
ERPODO sistema financiero	Licenciado
FIEL WEB 14 licencias asesoramiento jurídico	Licenciado
Base de Datos	Software Libre
DNS	Software Libre
DHCP	Software Libre
WEB	Software Libre
Correo	Software Libre
Firma electrónica	Software Libre

Nota. Fuente: Dirección de Tecnologías de la Información del GADM San Miguel de Ibarra (2022).

3.6 Dispositivos de soporte

La Dirección de Tecnologías de la Información realizó la adquisición de UPS Power Ware y generadores eléctricos, ya que en el caso que exista un corte eléctrico, en trabajo conjunto pueden abastecer de energía eléctrica por un lapso de 48 horas continuas. Estos equipos se los utiliza con la finalidad de que los equipos de comunicaciones, servidores y sistemas no dejen de funcionar de forma abrupta en caso de una interrupción de este tipo.

3.7 Administración de software

La administración del sistema de red es de vital importancia para que los servicios tengan un buen funcionamiento, para el caso de GADM San Miguel de Ibarra el administrador de red hace uso de la herramienta Storage Management Utility para poder monitorear el equipo de red HP SAN P2000G3 el cual se encarga básicamente del almacenamiento de los equipos, adicional se hace uso del software ILO (Integrated Lights Out) el cual se encarga de la monitorización de

los servidores físicos y de la monitorización de los servidores virtuales se lo hace atravesó de la herramienta Putty, utilizando el acceso remoto SHH o TELNET para switch, router internos de la institución.

3.7.1 Gestión de red

Para la gestión de software se utiliza herramientas de software libre como NAGIOS, DUDE Y WIRESHARK, los cuales en trabajo conjunto permiten tener operativa la red y evitar en el mayor rango posible incidentes que afecten al funcionamiento de los sistemas:

Nagios es un sistema de monitorización de redes, utilizado por la Dirección de Tecnologías de la Información con la finalidad de vigilar los equipos activos y servicios configurados en el sistema, éste alerta cuando el comportamiento de uno de los dispositivos configurados empieza a tener comportamientos no deseados. Sus principales características se encuentran los servicios de red como SMTP, POP3, HTTP, SNMP, también este software permite la monitorización de recursos de sistemas de hardware como la carga del procesador, uso de discos, memoria, estado de puertos, etc. Permite además la posibilidad de monitorización de forma remota mediante conexión SSL cifrados y SSH.

También hace uso de otras herramientas de gestión como son: Vsphere client que se usa para la gestión y monitoreo de software, VMware utilizada en la solución de Hyper convergencia, Veam one para la gestión y monitoreo de máquinas de virtuales, Veam back up para la gestión de respaldo de archivos y máquinas virtuales, Zabbix monitoreo de servicios y servidores de base de datos.

Por otra parte, Dude es utilizado para monitorear enlaces inalámbricos, este software explora automáticamente todos los dispositivos conectados a la red y emite una alerta en el caso que exista problemas, entre sus ventajas este muestra el descubrimiento automático de cualquier

tipo de marca y dispositivo, fácil instalación y uso, admite la supervisión SNMP, ICMP, DNS y TCP para dispositivos compatibles, monitoreo de enlaces individuales y gráficos, etc.

Por último, se hace uso de la herramienta Wireshark, el cual es usado como un analizador de protocolos y permite visualizar de forma clara el tráfico de datos en tiempo real; tiene una interfaz gráfica amigable. También permite analizar la información capturada ya que emite una serie de detalles y sumarios por paquetes, aparte de identificar si los puertos se encuentran abiertos o no.

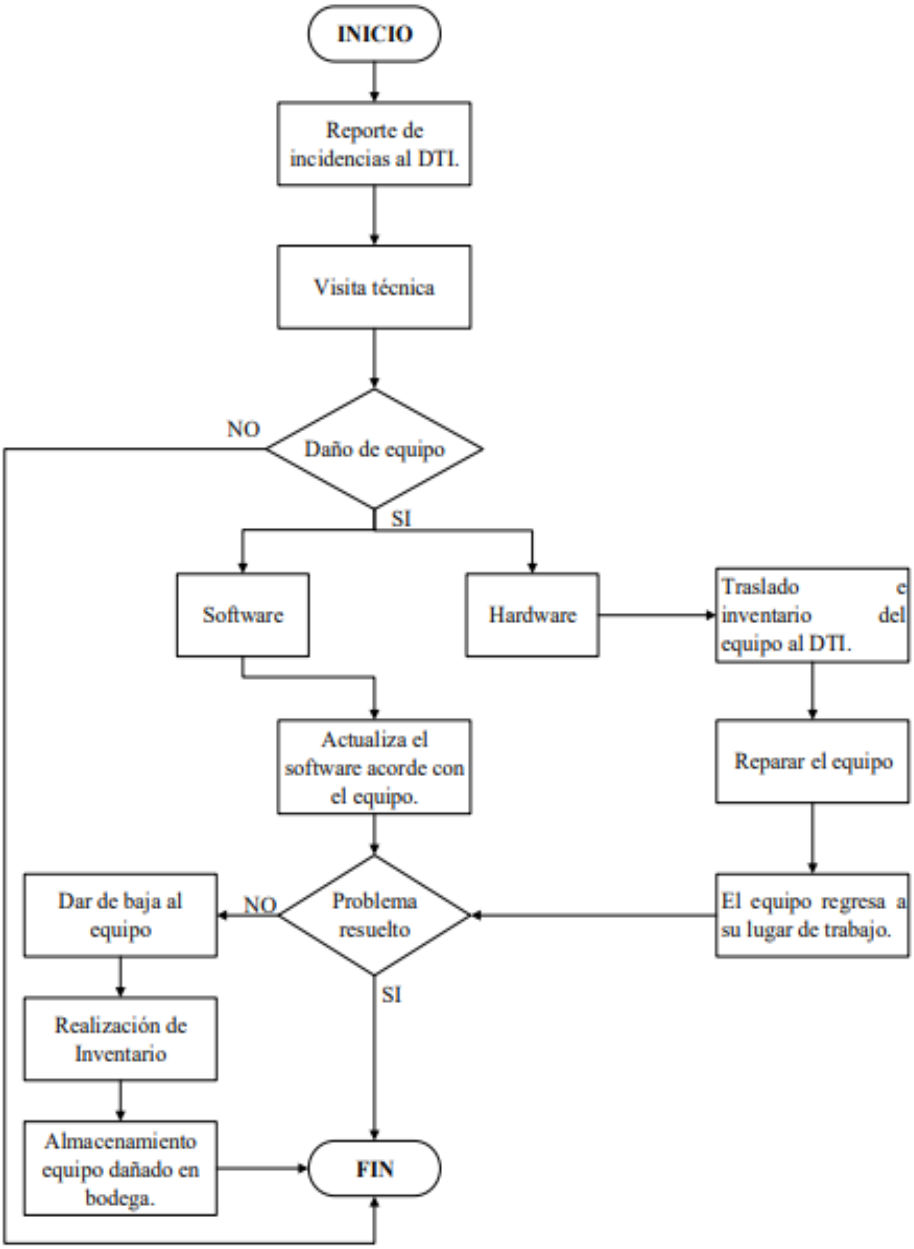
3.7.2 Gestión de Hardware.

Al momento que la organización entrega un activo informático a un departamento o empleado en específico, éste debe responsabilizarse del mismo, en caso que este equipo o dispositivo presente alguna falla, el empleado o encargado de este activo debe subir al sistema denominado Osticket help desk, detallando el nombre del activo y la falla que presenta, el sistema determinara la criticidad del ticket y el tiempo de respuesta dependiendo de la gravedad. Si existe un caso de avería en algún equipo, un técnico se dirige hacia el lugar y verifica si el problema de funcionamiento se trata de hardware o software, en el caso que la falla sea de baja gravedad el técnico procede a la reparación de inmediato, pero de no ser así, éste traslada el equipo al área de infraestructura y comunicaciones para darle el mantenimiento necesario solucionando el problema y enviándolo nuevamente a su lugar de trabajo.

Cuando el equipo haya cumplido su vida útil, éste es retirado y dado de baja luego que un técnico encargado certifique que ya no tiene reparación. Se lo almacena en bodega y se realiza un informe sobre el mismo, y finalmente cumpliendo con todos los requisitos administrativos se lo envía a una recicladora. El proceso de ingreso de tickets se muestra en la Figura 7 a través de un diagrama de flujo.

Figura 7

Diagrama de flujo de la gestión de Hardware.



Nota. Fuente**:** Dirección de Tecnología de la Información (2022)

3.7.3 Gestión de Antivirus.

La administración de gestión de antivirus es manejada por ESET 9 con un licenciamiento original por el lapso de un año, por medio de este software se puede gestionar estaciones Windows,

Mac, Linux o teléfonos móviles desde la consola del servidor físico ubicado en el Data Center de la municipalidad; este software contribuye a la protección contra códigos maliciosos y por consiguiente permite a los administradores TI brindar una respuesta inmediata frente a diversos ataques informáticos.

3.8 Responsabilidades de la Dirección de Tecnologías de la Información del GADM San Miguel de Ibarra

La Dirección de Tecnologías de la Información del GADM San Miguel de Ibarra cuenta con un sinnúmero de responsabilidades, entre la más importante es la de mantener la operatividad de todos los servicios que la municipalidad ofrece a sus usuarios internos y externos como: energía eléctrica, comunicación de datos, servicios tecnológicos, portales web, telefonía, servicio de internet, entre otras.

- **Misión DTI GADM San Miguel de Ibarra.**

Gestionar eficiente y eficazmente el gobierno electrónico, la infraestructura y servicios tecnológicos institucionales mediante la administración, mantenimiento y desarrollo de sistemas de información y servicios informáticos que apoyen los procesos realizados por usuarios internos y externos (Dirección de Tecnologías de la Información, 2022).

- **Atribuciones y responsabilidades.**

La Dirección de Tecnologías de la Información debe cumplir ciertos parámetros para que la municipalidad funcione adecuadamente en cuanto al tema de conectividad se refiere. Por ello a continuación se detalla cada una de las obligaciones que esta Dirección debe poner en práctica (Dirección de Tecnologías de la Información, 2022).

a) Formular y gestionar el plan estratégico de TIC alineado al plan estratégico institucional y a las políticas de la institución.

b) Diseño de planes y programas especializados en materia de desarrollo de software, y soporte técnico, redes de comunicación de datos, seguridad de la información y gobierno electrónico.

c) Administrar la infraestructura de software y hardware de manera eficiente para brindar servicios de calidad.

d) Brindar asesoramiento en materia de TIC a las autoridades, funcionarios y servidores de la institución.

e) Proponer, implementar y controlar la aplicación de políticas y normativas para el uso de las TIC.

f) Garantizar la disponibilidad, seguridad y continuidad de las aplicaciones y servicios informáticos.

g) Apoyar tecnológicamente para la automatización de procesos institucionales.

h) Formular y gestionar la estrategia de gobierno electrónico para brindar servicios en línea e incrementar el acceso y la transparencia de la información pública.

- **Productos**

Entre los productos ofertados por la Dirección de Tecnologías de la Información se divide en dos, desarrollo de software e infraestructura y comunicaciones. Cada uno de estos cumplen con funciones de acuerdo a su dependencia como se muestra en la Tabla 18.

Tabla 18

Funciones de la Dirección de Tecnologías de la Información.

DEPENDENCIA	FUNCIONES
Desarrollo de Software	Gestión de acceso a servicios aplicaciones. Respaldo y restauración de d electrónicos

	Atención, capacitación y soporte téci al usuario. Desarrollo de software. Mantenimiento de software desarroll y de terceros.
Infraestructura y comunicaciones	Gestión de licencias de softv adquirido Gestión de proyectos tecnológicos infraestructura. Gestión de proyectos tecnológicos infraestructura. Administración de equipos comunicación y servidores. Instalación y ampliación de la red de y datos. Soporte y mantenimiento del par informático.

Nota. Fuente: Dirección de Tecnologías de la Información (2022).

- **Personal**.

Dentro de la Dirección de Tecnologías de la Información se encuentran trabajando 13 personas, las cuales cumplen diferentes funciones, en la Tabla 19 se detalla el cargo, el encargado y la descripción del trabajo a realizar (Dirección de Tecnologías de la Información, 2022).

Tabla 19

Personal de la Dirección de Tecnologías de la Información del GADM-IBARRA

CARGO	**ENCARGADO**
Director de la Dirección de Tecnologías de la Información	Ing. Carlos Gudiño
Responsable de la unidad de Desarrollo de software	Lic. Sonia Bosano.
Responsable de la unidad hardware e Infraestructura.	Lic. Miguel Tobar.
Analista de Sistemas	Ing. Gabriel Bucheli
Analista de Sistemas	Tnlgo. Jhon Sarauz
Analista de Sistemas	Ing. Cristian Romero.
Analista de Sistemas	Ing. Verónica Rosero.
Analista de Sistemas	Ing. Manuel Lara.
Analista de Sistemas	Ing. Jairo Álvarez.
Analista de Sistemas	Ing. Alexandra Guerrero.

Analista de Sistemas	Ing. Esteban Táez.
Analista de Sistemas	Ing. Samantha Mesa.
Analista de Sistemas	Ing. Fernando Terán
Analista de Sistemas	Ing. Evelin Ochoa

Nota. Fuente: Dirección de Tecnologías de la Información (2022).

3.9 Análisis de riesgos en la red administrativa del GAD-IBARRA siguiendo la Metodología MAGERIT V3

Para la realización del análisis de riesgos siguiendo la Metodología MAGERIT V3 en una institución gubernamental, es fundamental conocer todos los recursos o activos informáticos que la institución posee; identificar además cuales serían las posibles amenazas de las que es necesario protegerse, la probabilidad de ocurrencia y la degradación que estas ocasionarían sobre los activos y el riesgo a los que estos están expuestos. MAGERIT V3 sugiere la clasificación de activos dividiéndolos por: servicios, datos, equipos informáticos, aplicaciones, redes de comunicaciones, instalaciones, equipos de soporte y personal. Cada uno de estos activos deben pasar por un proceso de valorización dependiendo de la importancia que este representa para la organización, se asigna prioridad de uno a otro en valores numéricos del 0 -10, además, se de establecer las amenazas, degradación, impacto, frecuencia y por último el riesgo de cada activo.

3.9.1 Clasificación de los activos

Para la asignación de un activo dentro de una categoría se debe tener en cuenta su función y la información que maneja; El activo puede pertenecer a diferentes categorías, como son: Servicios, Aplicaciones, Datos, Equipos Informáticos, Redes de Comunicación, Soportes de Información, Equipamiento auxiliar, Instalaciones y Personal.

A continuación, se presentan los resultados obtenidos en la realización de inventarios en al área de servicios.

- **Servicios**

Los servicios son los encargados en satisfacer las necesidades de los usuarios a través de sistemas informáticos presentados por la Organización, los cuales están encargados de mejorar o agilitar un proceso.

- **Descripción**

Los servicios prestados por la municipalidad se enfocan hacia los usuarios finales, éstos pueden ser internos o externos a la organización. Entre los servicios más relevantes están: Portal Ciudadano, base de datos, sistema SIGM, Sistema De Gestión Documental Quipux.

- **Datos**

Los datos es la raíz que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o a su vez, será transferido de un lugar a otro por algún medio de transmisión de datos.

    - Descripción:

Dentro de la sección Datos, se ha considerado las bases de datos que dan soporte a aplicaciones con las que trabaja la institución, como: base de datos Olympo, Quipux, ODOO, correo electrónico, SCRIPTCASE, entre otros.

- **Aplicaciones [SW]:**

Las aplicaciones se la conocen con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) esta sección se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

  - Descripción**:**

Dentro del activo Aplicaciones se encuentran los aplicativos de desarrollo propio y contratado, entre las aplicaciones de desarrollo propio se encuentran: portal ciudadano, sistema de participación ciudadana, portal web, sistema de gestión municipal, reportes de servicios internos, sistema de parquímetros, sistema de registro de obras, módulo de consulta de impuestos y predios, sistema de administradores TIC´s, módulo de partes policiales, sistema de notificación y multas, sistema de tránsito y transporte, SISMERT, SIGM, sistema de ventanilla única, sistema de transferencias de dominio, sistema de control vehicular, sistema de control de turnos, sistema SITAC (SRI). Aplicaciones contratadas como: Olympo (Contabilidad y Presupuestos), Balance Score Card (Gestión Municipal) y el Quipux (Gestión documental). Gestores de bases de datos PostgreeSQL, MySQL, Post GIS, Eset Nod 32, Autocad, Office, Mozilla Firefox, Internet Explorer, pandora FMS, y sistemas operativos como: Debian, Centos, Ubuntu, Windows, Mac OS.

- **Equipos Informáticos [HW]:**

Los equipos informáticos son los medios físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

  - Descripción:

Dentro de esta sección se encuentran los equipos informáticos que están albergados en el Data Center de la municipalidad como son: servidores físicos, switch, routers, PCs entre otros.

- **Redes De Comunicación [COM]:**

Las redes de comunicación se definen como un conjunto medios físicos, tecnologías, protocolos que son necesarios para el intercambio de información entre usuarios de una red.

  - Descripción:

Entre los activos de redes de comunicación se encuentran las redes LAN, WLAN, MAN, Y WAN que brinda el servicio de conectividad dentro y fuera de la municipalidad.

- **Soportes de Información:**

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempos.

  - Descripción:

Dentro de este activo se encuentran: Discos externos de respaldo de información y datos, CD, DVD, Storage Blade, USB y material impreso como: proyectos, planes, evaluaciones, informes, entre otros.

- **Equipamiento Auxiliar:**

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

- Descripción**:**

Dentro de esta sección de activos se encuentran: fuentes de alimentación, equipos de climatización, cableado estructurado, fibra óptica, sistema de alimentación ininterrumpida (ups) y generador eléctrico.

- **Instalaciones:**

En esta sección entran los lugares donde se hospedan los equipos informáticos y redes de comunicaciones, denominados nodos en el Análisis de Riesgos.

- Descripción**:**

Para este apartado se ha tomado en cuenta las instalaciones de la Dirección de Tecnologías de la Información la cual cuenta con: Data Center, Oficinas TIC, Sala de reuniones, y 17 nodos que se encuentran ubicados en diferentes puntos de la ciudad.

- **Personal:**

En esta sección se detalla a las personas que laboran en la Dirección de Tecnologías de la Información del Gad-Ibarra.

- Descripción**:**

Se ha clasificado entre usuarios internos (personal de la Dirección de TICs), externos (ciudadanía en general) y proveedores de los diferentes servicios.

3.9.1.1 Dimensionamiento de los activos:

Esta tarea consiste en determinar en qué dimensión es valioso un activo, de acuerdo a su tipo. Entre las dimensiones a considerar están (Magerit, 2012):

- **Disponibilidad [D]:** Garantiza a los usuarios autorizados el acceso permanente a la información y sus activos asociados cuando éstos lo requieran.
- **Integridad [I]:** Asegura la no modificación sin ningún tipo de autorización de la información y sus métodos de procesamiento.
- **Confidencialidad [C]:** Garantiza que la información o su procesamiento sea tratado de manera privada y no sea accesible a usuarios no autorizados.
- **Autenticidad de los usuarios del servicio [A_S]:** Asegura que el usuario que acceda al servicio sea quien dice ser.
- **Autenticidad del origen de los datos [A_D]:**

  Garantiza que en todo momento se pueda conocer la fuente de los datos (No repudio).
- **Trazabilidad del servicio [T_S]:** Asegura que en todo momento se pueda identificar al usuario que hizo uso de un servicio, para qué y en qué periodo.
- **Trazabilidad de los datos [T_D]:** Asegura que en todo momento se pueda identificar al usuario que accedió a los datos, para qué y en qué periodo.

3.9.1.2 Valoración de activos.

Para la valoración de los activos, MAGERIT recomienda la asignación de valores del 0 – 10 como se muestra en la tabla 20. Donde el 0 (cero) se asigna al activo que no tenga mayor importancia y en el caso que una amenaza llegara a materializarse no tendría una afectación significativa dentro de la organización, por lo contrario, si su valoración es de 10 quiere decir que si una amenaza llegara a materializarse su afectación podría causar la paralización de las actividades diarias de la organización.

Tabla 20

Criterios de valorización de los Activos

Valor Activo	Nivel	Criterio
10	Muy Alto (MA)	Daño muy grave a la organización
7 – 9	Alto (A)	Daño grave a la organización
4 – 6	Medio (M)	Daño importante a la organización
1 – 3	Bajo (B)	Daño menor a la organización
0	Muy Bajo (MB)	Irrelevante a efectos prácticos

Nota. Fuente: Libro 2 "Catálogo de Elementos" MAGERIT V3 (Magerit, 2012).

Anadir un valor al activo es el primer paso para poder continuar con el cálculo y determinar el riesgo que puede tener el activo, para esto se necesita previamente obtener los datos del nivel de degradación, el nivel de impacto y frecuencia. Por lo que a continuación, se muestra la Tabla 21 el nivel de degradación definiendo el porcentaje de 0 a 100%; Cabe mencionar que para obtener el valor de la degradación del activo hay que tomar en cuenta el tipo de amenaza que puede afectar al activo, por lo que por cada nivel de degradación se ha asignado un tipo de amenaza dependiendo del tipo de activo (VER ANEXO 4)

Tabla 21

Nivel de Degradación del Activo

DEGRADACIÓN		
Nivel	**Porcentaje**	**Amenazas**
MA	100%	A.5, A.11, A.24
A	80%	E.24. A.4, A.29, A.30
M	50%	E.3, E.4, A.7, A.9, A.13
B	10%	E.1, E.2, E.9
MB	1%	

Nota. Fuente: Libro 2 "Catálogo de Elementos" MAGERIT V3 (Magerit, 2012).

Así, para complementar la información en la Tabla 22 se muestra el valor con respecto al impacto del activo, siguiendo la ecuación (1). Según el Catálogo de Elementos de MAGERIT V3.

	***Nivel del Impacto** = Nivel del Activo * Degradación*	(1)

Tabla 22

Valorización del Impacto del activo.

IMPACTO		**DEGRADACIÓN**				
		1% (MB)	**10% (B)**	**50% (M)**	**80% (A)**	**100% (MA)**
NIVEL DE ACTIVO	**MA**	M	A	MA	MA	MA
	A	B	M	A	A	A
	M	MB	B	M	M	M
	B	MB	MB	B	B	B
	MB	MB	MB	MB	MB	MB

Nota. Fuente: Libro 2 "Catálogo de Elementos" MAGERIT V3 (Magerit, 2012).

Ejemplo: Se calcula el nivel de impacto siguiendo la Tabla 22. Según los datos obtenidos en la calificación de activos se determina el nivel de un activo. Para este ejemplo se tomará el nivel **A** (Alto) y el tipo de degradación de un 80% (**Alto**), como se muestra a continuación:

Nivel de Impacto = MA * A = MA

De esta manera se calculará el nivel de impacto de todos los activos dependiente el valor del activo y el nivel de degradación. En este caso el valor del activo es Muy Alto y el valor de la degradación Alta, tendremos como resultado un nivel de impacto Muy Alto hacia el activo.

Para poder calcular la frecuencia del impacto se muestra en la Tabla 23, determinando el tiempo en el que una amenaza puede presentarse.

Tabla 23

Frecuencia del Impacto

FRECUENCIA DEL IMPACTO		
Frecuencia	**Tiempo**	**Amenaza**
Muy Frecuente (MF)	Diario	
Frecuente (F)	Mensual	
Frecuencia Normal (FN)	Anual	E.1, E.2, E.3, E.24, A.7, A.24.
Poco Frecuente (PF)	Cada Varios Años	E.4, E.9, A.4, A.5, A.9, A.11, A.13, A.29, A.30.

Nota. Fuente: Libro 2 "Catálogo de Elementos" MAGERIT V3 (Magerit, 2012).

Por último, para determinar el riesgo que corre un activo en cuanto a las amenazas se toma en cuenta el valor de impacto y la frecuencia en que este pueda ocurrir, como se muestra en la Tabla 24 y siguiendo la ecuación (2).

	$\boldsymbol{Riesgo} = Nivel\ de\ impacto * Frecuencia$	(2)

Tabla 24

Impacto de la amenaza con respecto a la frecuencia

RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
NIVEL IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Nota. Fuente: Libro 2 "Catálogo de Elementos" MAGERIT V3 (Magerit, 2012).

Ejemplo: Se calcula el nivel de Riesgo siguiendo la ecuación (2). Según los datos obtenidos de las Tablas 23 y 24. Para este ejemplo se tomará el nivel **M** (Medio) y el tipo de frecuencia **F** (Frecuente), como se muestra a continuación:

Nivel de Riesgo = M * F = A

Si, el nivel de impacto es Medio y el nivel de frecuencia es Frecuente, tendríamos como resultado que el activo se encuentra en un riesgo **Alto**, el cual está catalogado en niveles de 7 a 9 de 10.

De esta manera se calculará el nivel de impacto de todos los activos dependiente el valor del activo y el nivel de degradación.

Con estos datos obtenidos se debe tomar en cuenta la importancia de la función que realiza el activo dentro de la organización, por lo que, se toma en cuenta los principios de la seguridad como son la Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad. Su análisis y valoración fue asistida por el personal de la Dirección de Tecnologías de la Información por medio de encuestas realizadas a 5 miembros de la Dirección; Con los datos obtenidos, se da una breve descripción de los resultados del proceso de valorización de los activos de cada clasificación, para esto se ha tomado en consideración los valores de niveles Alto y Muy Alto para un mejor entendimiento. En el ANEXO 6 se muestra detalladamente el proceso de valorización tomando en cuenta los demás parámetros que permitieron obtener estos datos.

- **Valoración de Activos de Tipo SERVICIOS**

Dentro de esta clasificación se ha considerado los principios de seguridad como: Disponibilidad, Integridad, Confidencialidad autenticidad y trazabilidad del servicio. En la Tabla 25 se muestra como resultado los activos que se ha catalogado en riesgos en niveles altos y muy Altos.

Tabla 25

Tabla de resultados de los activos denominados Servicios.

Activo	Disponibilidad		Integridad		Confidencialidad		Autenticidad del servicio		Autenticidad de los datos	
	Valor	Riesgo	Valor	Riesgo	Valor	Riesgo	Valor	Riesgo	Valor	Riesgo

Bases De Datos	10	MA	10	MA	10	MA	10	MA	10	MA
Portal Ciudadano	10	MA	10	MA	10	MA	10	MA	10	MA
SIGM	10	MA	10	MA	10	MA	10	MA	10	MA
Sistema de Gestión Document al Quipux	10	MA	10	MA	10	MA	10	MA	10	MA
Internet	10	MA	10	MA	10	MA	10	MA	10	MA
Seguridad Perimetral	10	A	10	MA	10	MA	10	MA	10	MA

Nota. Los datos fueron obtenidos a través de encuestas realizadas al personal de Tics.

Para la muestra de los resultados en esta sección se ha tomado los valores en niveles Muy Altos, en cuanto a la valorización de los principios de la seguridad en la Disponibilidad, Integridad, Confidencialidad, autenticidad y trazabilidad del servicio. Con estos resultados se ha llegado a la conclusión que los servicios más críticos de la municipalidad son: El servicio de Portal Ciudadano, base de datos, SIGM, Sistema de documentación Quipux, Internet y seguridad perimetral.

- **Valoración de Activos de Tipo DATOS**

Dentro del activo Datos se ha considerado las dimensiones de: Disponibilidad, Integridad, Confidencialidad, Autenticidad de los datos y Trazabilidad de los datos. En la Tabla 26 se muestra los resultados en cuanto a los datos obtenidos en esta clasificación.

Tabla 26

Tabla de resultados de los activos denominados Datos.

Activo	**Disponibilidad**		**Integridad**		**Confidencialidad**		**Autenticidad De los datos**		**Trazabilidad De los datos**	
	Valor	**Riesgo**	**Valor**	**Riesgo**	**Valor**	**Riesgo**	**Valor**	**Riesgo**	**Valor**	**Riesgo**
Base de datos **ODOO** (Master y Replica)	10	MA	10	MA	10	MA	10	MA	10	MA

Servidor SCRIPTCASE V8	10	MA	10	MA	10	MA	10	MA	10	MA
Servidor SCRIPTCASE V9	10	MA	10	MA	10	MA	10	MA	10	MA
Bases de datos de Producción: Alfanumérica, Espacial y Binaria (Master y Replica)	10	A	10	A	10	A	10	A	10	A
Base de Datos Quipux (Master y Replica)	10	A	10	A	10	A	10	A	10	A
Base de Datos Firma Electrónica (Master y Replica)	10	A	10	A	10	A	10	A	10	A
Bases de Datos fotos de Avalúos y Catastros y Tareas activiti (Master y Replica)	10	A	10	A	10	A	10	A	10	A
Base de Datos SQL SERVER OLYMPO (Histórico)	9	A	9	A	10	MA	9	A	9	A

Base de Datos de Correo Electrónico	7	A	10	MA	10	MA	10	MA	7	A
Servidores de Aplicaciones GADI: ()	10	A	10	A	10	A	10	A	10	A
Registros de Actividad (LOG) (equipos, servicios, antivirus)	7	A	9	A	9	A	9	A	7	A

Nota. Los datos fueron obtenidos a través de encuestas realizadas al personal de Tics.

En la muestra de resultados de esta sección, se calificó los principios de seguridad como son: Disponibilidad, Integridad, Confidencialidad, Autenticidad de Datos y Trazabilidad de los Datos**,** en los cuales se obtuvo como resultados las bases de datos de ODOO, SCRIPT CASE V8 Y V9 con un nivel Muy Alto de criticidad. Las bases de datos de Bases de datos de Producción: Alfanumérica, Espacial y Binaria (Master y Replica), Base de Datos Quipux (Master y Replica), Base de Datos Firma Electrónica (Master y Replica), Bases de Datos fotos de Avalúos y Catastros y Tareas Activiti (Master y Replica), Base de Datos SQL SERVER OLYMPO (Histórico), Base de Datos de Correo Electrónico, Registros de Actividad (LOG) (equipos, servicios, antivirus), se han catalogado con un nivel de criticidad Alto, ya que han sido calificados con valores entre 7 – 9.

- **Valoración de Activos de Tipo APLICACIONES**

Dentro de este apartado denominado aplicaciones se ha considerado los principios de seguridad como: Disponibilidad, Autenticidad del servicio y Trazabilidad del servicio. En la Tabla 27 se muestra los resultados obtenidos en cuanto a esta clasificación.

Tabla 27

Tabla de resultados de los activos denominados Aplicaciones.

Activo	Disponibilidad		Integridad		Confidencialidad		Autenticidad del servicio		Trazabilidad del servicio	
	Valor	Riesgo	Valor	Riesgo	Valor	Riesgo	Valor	Riesgo	Valor	Riesgo
Portal de información geográfica del Gad-Ibarra	9	MA	10	MA	10	MA	10	MA	7	MA
Módulo de consulta de impuestos y predios	7	MA	9	MA	9	MA	9	MA	7	MA
Sistema SIGM (web)	10	MA	10	MA	10	MA	10	MA	7	MA
Sistema de ventanilla Única	10	MA	10	MA	10	MA	10	MA	7	MA

Nota. Los datos fueron obtenidos a través de encuestas al personal de Tics.

Dentro de esta sección se ha dividido los activos entre aplicaciones propias y contratadas. Los activos calificados en nivel Muy Alto (10) en la dependencia de Disponibilidad, Integridad,

Confidencialidad, Autenticidad y Trazabilidad de los Datos se encuentran las aplicaciones de: Sistema de información geográfica del GAD Ibarra, Módulo de consulta de impuestos y predios, Sistema SIGM (web) y Sistema de ventanilla Única.

Entre el nivel Alto están: Portal ciudadano, Sistema de control de turnos, Sistema operativo CentOS y aplicaciones de Microsoft.

- **Valoración de Activos del Tipo EQUIPOS INFORMÁTICOS**

Dentro de esta sección de activos se ha considerado las dimensiones de: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de los datos. En la Tabla 28 se muestra los resultados en cuanto a los datos obtenidos pertenecientes a esta clasificación.

Tabla 28

Tabla de resultados de los activos denominados Equipos Informáticos.

Activo	**Disponibilidad**		**Integridad**		**Confidencialidad**		**Autenticación del servicio**		**Trazabilidad del servicio**	
	Valor	**Riesgo**	**Valor**	**Riesgo**	**Valor**	**Riesgo**	**Valor**	**Riesgo**	**Valor**	**Riesgo**
Firewall Check Point 4600	10	MA	10	MA	10	MA	10	MA	10	MA
Switch Core Chasis	10	MA	10	MA	10	MA	10	MA	10	MA
SAN Switch	10	MA	10	MA	10	MA	10	MA	10	MA
Almacenamiento	10	MA	10	MA	10	MA	10	MA	10	MA
Swichlan1 DELL HYPERCONVERGENCIA	10	MA	10	MA	10	MA	10	MA	10	MA
Swichlan2 DELL	10	MA	10	MA	10	MA	10	MA	10	MA

HYPERCONVERGENCIA										
Swich SAN DELL	10	MA	10	MA	10	MA	10	MA	10	MA
Servidor De Almacenamiento Storage (I)	10	MA	10	MA	10	MA	10	MA	10	MA
Free NAS Almacenamiento	10	MA	10	MA	10	MA	10	MA	10	MA
Servidor ERP ODOO	10	MA	10	MA	10	MA	10	MA	10	MA
Servidor Aplicaciones SIG Producción	10	MA	10	MA	10	MA	10	MA	10	MA
Servidor BDD Producción	10	MA	10	MA	10	MA	10	MA	10	MA
Servidor Dell Host 1	10	MA	10	MA	10	MA	10	MA	10	MA
Servidor Dell Host 2	10	MA	10	MA	10	MA	10	MA	10	MA
Servidor Dell Host 3	10	MA		MA	10	MA	8	MA	10	MA

Nota. Los datos fueron obtenidos a través de encuestas al personal de Tics.

Los equipos físicos como servidores, routers y switch son los que soportan las aplicaciones, datos, configuraciones y todo lo relacionado para que una red de comunicaciones llegue a su fin por la cual fueron instaladas, por ende, todos los equipos son de vital importancia para la institución, por ello se los ha calificado con valores de 10 y 9 que se encuentran en los niveles Muy Altos.

- **Valoración de Activos del Tipo REDES DE COMUNICACIÓN**

Dentro de este activo se ha considerado las dimensiones de: Disponibilidad y Confidencialidad. En la Tabla 29 se muestra los resultados en cuanto a los datos obtenidos pertenecientes a esta clasificación.

Tabla 29

Tabla de resultados de los activos denominados Redes de comunicación.

Activo	Disponibilidad		Confidencialidad	
	Valor	**Riesgo**	**Valor**	**Riesgo**
Red LAN	8	A	10	MA
Red W LAN	9	A	10	MA
Red MAN	9	A	10	MA
Red WAN	9	A	10	MA
CONÉCTATE IBARRA	8	A	9	A

Nota. Los datos fueron obtenidos a través de encuestas al personal de Tics.

Como parte de estos activos se encuentran la parte física y lógica para que exista comunicación entre dos equipos de hardware, en este caso las redes en la municipalidad se tiene las redes LAN, W LAN, WAN, MAN y CONÉCTATE IBARRA. Las cuales se ha valorizado entre niveles Altos y Muy Altos

- **Valoración de Activos de Tipo SOPORTES DE INFORMACIÓN**

Dentro de este activo se ha considerado las dimensiones de: Disponibilidad. En la Tabla 30 se muestra los resultados en cuanto a los datos obtenidos pertenecientes a esta clasificación.

Tabla 30

Tabla de resultados de los activos denominados Soportes de Información.

Activo	Disponibilidad		Confidencialidad	
	Valor	**Riesgo**	**Valor**	**Riesgo**
Discos externos de respaldos	4	M	5	M

de información (Sistema y Datos)				
CD	4	B	5	B
DVD	4	B	5	B
Storage Blade	10	A	10	A
Proyectos, Planes, Evaluaciones, Informes de TIC	5	B	5	B
UBS	4	B	5	B

Nota. Los datos fueron obtenidos a través de encuestas al personal de Tics (Ver Anexo 5).

Dentro de esta clasificación se ha tomado en cuenta el parámetro de calificación Disponibilidad y Confidencialidad, donde destacan los soportes que almacenan mayor cantidad de información o la más sensible, en los que se encuentran los soportes de información como: Storage Blade el cual se encuentra con un valor catalogado como alto.

- **Valoración de Activos del Tipo EQUIPAMIENTO AUXILIAR**

Dentro de este activo se ha considerado las dimensiones de: Disponibilidad. En la Tabla 31 se muestra los resultados en cuanto a los datos obtenidos pertenecientes a esta clasificación.

Tabla 31

Tabla de resultados de los activos denominados Equipamiento Auxiliar.

Activo	**Disponibilidad**	
	Valor	**Riesgo**
Fuentes de Alimentación (servers)	10	MA
Sistemas de Alimentación Ininterrumpida (Servers)	10	MA

Generador eléctrico	10	A
Cableado Estructurado	9	A
Fibra Óptica	9	A

Nota. Los datos fueron obtenidos a través de encuestas al personal de Tics.

Dentro de esta clasificación se ha tomado en cuenta el parámetro de calificación Disponibilidad**,** entre los activos de mayor riesgo en este clasificado se encuentran: La fuente de Alimentación de los servidores con valores Muy Altos y generador eléctrico, cableado estructurado y Fibra óptica calificados con un nivel alto de criticidad.

- **Valoración de Activos del Tipo INSTALACIONES [L]**

Dentro de este activo se ha considerado las dimensiones de: Disponibilidad. En la Tabla 32 se muestra los resultados en cuanto a los datos obtenidos pertenecientes a esta clasificación.

Tabla 32

Tabla de resultados de los activos denominado Instalaciones.

Activo	Disponibilidad		Integridad		Confidencialidad		Autenticidad de los Datos	
	Valor	**Riesgo**	**Valor**	**Riesgo**	**Valor**	**Riesgo**	**Valor**	**Riesgo**
Data Center	10	A	10	M	10	A	10	A
Oficinas TIC	9	B	10	M	6	MB	9	B
Sala de reuniones	5	MB	10	M	5	MB	5	MB
Nodo 16	7	B	10	M	7	B	7	B

Nota. Los datos fueron obtenidos a través de encuestas al personal de Tics.

La Dirección de Tecnologías de la Información cuenta como infraestructura física con un Data Center, Oficias, Sala de reuniones, y 17 nodos, los cuales valorizándolos con respecto a la amenaza que se ha asignado como *Acceso no autorizado, fuego, otros;* El valor de riesgo se ha determinado entre *alto, bajo y muy bajo.*

- **Valoración de Activos de Tipo PERSONAL [P]**

Dentro de este activo se ha considerado las dimensiones de: Disponibilidad. En la Tabla 33 se muestra los resultados en cuanto a los datos del valor, nivel, degradación, impacto, frecuencia y riegos de cada uno de los activos pertenecientes a esta clasificación.

Tabla 33

Tabla de resultados de los activos denominado Personal.

Activo	Disponibilidad		Integridad		Confidencialidad		Autenticación de los Datos	
	Valor	**Riesgo**	**Valor**	**Riego**	**Valor**	**Riesgo**	**Valor**	**Riesgo**
Administradores de BDD	10	A	10	MA	10	MA	10	MA
Administrador de redes y comunicaciones	10	A	10	MA	10	MA	10	MA
Analistas de Sistemas	8	A	10	A	10	A	10	A
Técnicos de Soporte	9	A	10	M	10	M	9	B
Proveedores Olympo	9	A	10	MA	10	MA	10	MA
Proveedores Fiel Web	8	A	10	MA	9	A	10	MA
Proveedor de Equipos	8	A	10	MA	10	MA	10	MA
Proveedores de Internet	9	M	10	A	10	A	10	A
Usuarios Internos	6	M	9	A	9	A	10	MA

Nota. Los datos fueron obtenidos a través de encuestas al personal de Tics.

Dentro de esta sección se ha tomado como referencia el personal en riesgo Alto y Muy Alto, en cuanto a disponibilidad, integridad, Confidencialidad y Autenticación de los Datos se refiere. Entre éstos se encuentran los proveedores de servicios y personal técnico de la Dirección de Tecnologías de la Información del GAD Ibarra.

CAPITULO IV

4 Desarrollo del plan de contingencia

Este capítulo muestra la parte teórica del Plan de Contingencia de los servicios TI siguiendo el modelo que propone ITIL V3. Toda la información que se presenta en este capítulo tiene como objetivo ayudar a acelerar los procesos de restauración de servicios que presenten alguna falla tecnológica, tomando en cuenta los resultados obtenidos en el Análisis de Riesgos presentados en el capítulo III. Para este estudio se ha determinado desarrollar el plan de Contingencia de dos servicios catalogados con Riesgo Muy Alto, los cuales son las Bases de Datos y el Sistema Integrado de Gestión Municipal.

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PLAN DE CONTINGENCIA BASE DE DATOS DEL GADMI

VERSIÓN 1.0

JULIO, 2023

4.1 Propósito de un Plan de Contingencia

Para el Gobierno Autónomo Descentralizado San Miguel de Ibarra, es indispensable contar con los servicios TI que ofrece la Dirección de Tecnologías de la Información, es importante que estos servicios estén siempre operativos, ya que cuentan con información relevante para el buen funcionamiento de los servicios que ofrece la entidad hacia la ciudadanía.

Por este motivo al estar fuera de servicio las bases de datos y sus aplicativos por un lapso mayor a 1 hora seria causal de perdida de información, falta de atención al público y paralización de las funciones en ciertas áreas afectadas.

Es de gran importancia saber cómo actuar en el caso de presentarse algún tipo de inconveniente que afecte el buen funcionamiento de los servicios TI, determinando responsables, procesos a seguir y recursos a usar. Para ello se hace uso del contingente propuesto para el servicio de Base de Datos y el Sistema Integrado de Gestión Municipal. Ver en ANEXO 6 y 7.

4.2 Introducción

El presente documento se ha denominado Plan de Contingencia de servicios TI implementado el marco de trabajo ITIL v3. En el cual se determinan las fases a seguir para conseguir un plan de continuidad del negocio, estableciendo objetivo, alcance, definiciones, Base Legal, Responsables, ejecución o contenido, referencias, anexos y control de cambios. Ver ANEXO 6 y 7.

4.3 Metodología

Para el desarrollo del Plan de Contingencia se ha elegido trabajar con el Marco de Trabajo ITIL v3, la cual involucra una seria de buenas prácticas en la gestión TI, esta metodología abarca

la infraestructura del área, el mantenimiento y la operación de los servicios TI, sirve para crear un entorno de TI estable y escalable para así, promover una mejor prestación del servicio y atención del cliente.

Su objetivo es asegurar una gestión eficiente de sus procesos y garantizar una buena experiencia con los clientes, por lo tanto, tiene como objetivo principal, entregar un trabajo que garantice la calidad y satisfacción del cliente.

El desarrollo del Plan de Contingencia de los dos servicios elegidos a través del análisis de riesgos se ha estructurado de la siguiente manera:

- **Portada:** Se coloca logo de la Institución, Título, fecha y versión del documento.
- **Objetivo:** Se define el objetivo de realizar un plan de contingencia del servicio propuesto.
- **Alcance:** Se establece el alcance que va a tener el Plan de Contingencia.
- **Definiciones:** Se especifica la definición de varios términos utilizados en el Plan de Contingencia.
- **Base Legal:** Normativas legales que permiten realizar Planes de Contingencia.
- **Ejecución/Contenido:** En este apartado se muestra el desarrollo del Plan de Contingencia.
- **Referencias:** Documentar referencias bibliográficas.
- **Anexos:** Documentación Anexada al Plan de Contingencia.
- **Control de Cambios:** Registro de cambios dentro del Plan de Contingencia.

(VER DESARROLLO DE PLANES DE CONTINGENCIA EN ANEXO 6 y 7).

CONCLUSIONES

- Un plan de contingencia efectivo debe ser detallado, específico y estar disponible para todos los miembros de la Dirección de Tecnologías de la Información, en especial a los miembros que son encargados de mantener operativos los servicios que el GAD-Ibarra ofrece a la ciudadanía.
- La recolección de información de la situación actual de la Dirección de Tecnologías de la Información fue de gran ayuda para el desarrollo del Plan de Contingencia, ya que permitió identificar como está estructurada la red de la municipalidad, el personal encargado de cada área, estructura del Data Center, tipos de Software y Hardware.
- La Dirección de Tecnologías de la Información ha implementado Hiperconvergencia en cuanto a la realización de copias de seguridad, esto permite que la pérdida de información sea casi nula ya que cuenta con un servidor principal, servidor espejo y un servidor de respaldo, permitiendo así, asegurar la información en tiempo real y que, en el caso de caída de alguno de los servidores, el servicio al cliente no se detenga.
- El Análisis de Riesgos permitió conocer las amenazas a las que están expuestos los servicios TI del GAD-Ibarra, determinando también el impacto, la frecuencia y el riego que éstas tendrían en el caso de llegar a materializarse.
- La normativa ITIL V3, permitió estructurar de mejor manera el desarrollo del Plan de Contingencia, mediante el Catálogo de Diseño del Servicio, el cual establece 4 fases que se deben cumplir para dar una continuidad del servicio dentro de una organización.
- La asignación de responsables dentro de un equipo de trabajo es indispensable ya que éste será el encargado de dar respuestas a incidentes que ayuden a minimizar el impacto

de cualquier interrupción de los servicios TI, permitiendo también acelerar su recuperación.

- Dentro del desarrollo del Plan de Contingencia se optó por aplicar un Plan de Acción, en el cual se documentó los posibles fallos que pueden tener los servicios TI tratados en este trabajo, se dividió en físicos y lógicos. Cada uno de estos cuenta con responsables, manual de procedimiento de recuperación y tiempo estimado para levantar y poner en funcionamiento el servicio.
- En las pruebas de funcionamiento se realizó un check list, en el cual se detalló cada uno de los posibles fallos que puedan tener los servicios TI, en el cual aplicando el plan de acción presentado dentro del Plan de contingencia se obtuvo que todos los fallos fueron solventados.

RECOMENDACIONES

- Las pruebas y simulaciones regulares pueden ayudar a identificar posibles debilidades en el presente plan de contingencia y permitir que los equipos encargados de cada servicio TI practique los procedimientos de respuesta en caso de interrupción.
- Es importante que el equipo encargado de activar el plan de contingencia, esté compuesto por miembros con habilidades y experiencia relevantes, y que se realicen simulaciones y ejercicios regulares para mantener sus habilidades y conocimientos actualizados.
- Es importante que el Plan de Contingencia se mantenga actualizado y se revise regularmente para asegurarse de que sigue siendo efectivo en la protección de las operaciones de la organización.
- Es de vital importancia la creación de un nuevo Data center fuera de la Municipalidad como mecanismo redundante al actual, que cuente con las mismas características del principal, para así, en caso de requerirlo, tener un respaldo físico y lógico de toda la información de la municipalidad.
- Realizar reuniones constantes con el personal de la Dirección de Tecnologías de la Información del GAD-Ibarra, para tratar temas respecto a la seguridad de la información y la comprobación del cumplimiento de las políticas, normas y plan de contingencia establecidos en la institución.

BIBLIOGRAFÍA

Aguilera López, P. (2011). *Seguridad Informática.* Editex.

Areitio, J. (2008). *Seguridad de la Información - Redes Informáticas y Sistemas de la Infromación.* Paraninfo Cengage Learning.

Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador.*

Aznar, F. (2016). *Análisis evaluación riesgos informáticos*. Obtenido de https://francescaznar.com/analisis-evaluacion-riesgos-informaticos/

Baca, G. (2016). *Introducción a la seguridad informática.* Editorial Patria.

Baud, J. (2016). *ITIL V3 : entender el enfoque y adoptar las buenas prácticas.* Ediciones ENI. Obtenido de https://books.google.com.ec/books?id=5xmsQeWfQqoC&printsec=copyright&redir_esc=y#v=onepage&q&f=false

Bon, J. v., Jong, A. d., Kolthof, A., Pieper, M., Tjassing, R., Veen, A. v., & Verheijen, T. (2008). *Gestión de Servicios TI basado en ITIL® V3 - Guia de Bolsillo.* Van Haren.

Calderón Arateco, L. L. (2015). *Seguridad informática y seguridad de la información.* Universidad Piloto de Colombia.

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Obtenido de http://www.sei.cmu.edu/publications/pubweb.html

CENEPRED. (2015). *Escenario de Riesgo.* Obtenido de https://cenepred.gob.pe/web/escenario-riesgos/

COIP. (2014). *Código Orgánico Integral Penal.* Retrieved from https://www.justicia.gob.ec/wp-content/uploads/2014/05/código_orgánico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Congreso General del Estado. (1998). Ley de Propiedad Intelectual. 2.

Contraloría General Del Estado. (2009). Normas De Control Interno De La Contraloria General Del Estado. 73–77. Retrieved from http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Dirección de Tecnologías de la Información. (2022). *ORGANIGRAMA POR PROCESOS-RESOLUCIÓN 013-DAM-2016.* GAD Ibarra.

Fuquene Bogoya, E. D. (2019). *Rol de la legislación colombiana en la evolución de la seguridad informática y de la información.*

GADM San Miguel de Ibarra. (2020). *Resolución administrativa n° 286/Servidores y Accesos*.

Gómez Vieites, Á. (2015). *Seguridad Informática Basico.* Ecoe Ediciones.

Hernández James, F. J. (2011). Seguridad física y lógica en el manejo de la información policial. *3*(1).

ISECOM. (2010). OSSTMM. *3*(43).

ISO/IEC 27001. (2013). *Dominios ISO 27001:2013: Motivos para conocer mejor la nueva norma.* Obtenido de https://www.pmg-ssi.com/2017/04/dominios-iso-27001-2013/

ISO/IEC 27002. (2013). *ISO27002: Buenas prácticas para gestión de la seguridad de la información.* Obtenido de https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi

Jácome, V. (2019). *Plan de seguridad para la gestión de riesgos en el datacenter de la facultad de ingeniera en ciencias aplicadas con la metodología magerit v3.0.*

Keffer, A., & Gallart, N. (2007). *La preservación de recursos digitales: El reto para las bibliotecas del siglo XXI.* Editorial UOC.

LOTAIP. (2004). Ley Organica de Transparencia y Acceso a la Informacion Pública. 1–10. Obtenido de https://doi.org/10.1111/jfr3.12162

Lovos, F. D. (2011). *Seguridad Física y Lógica.* Obtenido de https://lovosfrancisco.jimdo.com/app/download/9167889769/SEGURIDAD+FISICA+Y+LOGICA.pdf?t=1504554721

Magerit. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Ministerio de Hacienda y Administraciones Públicas. Retrieved from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Méndez, K. (2015). *Seguridad.* Universidad Técnica del Norte.

Méndez, K. (2015). *Seguridad.* Universidad Técnica del Norte.

Ministerio de Hacienda y Administraciones Públicas. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas.

Mintzberg, H., Nicolau Medina, J., & Gozalbes Ballester, M. (2007). *Mintzberg y la dirección.* Ediciones Díaz de Santos.

Mogollón, A. (2014). *Análisis Comparativo: Metodologías de análisis de riesgos.*

Novoa, H., & Barrera, C. (2015). Metodologías para el análisis de riesgos en los SGSI. *Publicaciones e Investigación, 9*(0), 73–86. Obtenido de http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Ramirez, J. (2014). *Elaboración de un Plan de Emergencia y Desarrollo e Implementación del Plan de Contingencia, ante Riesgo de un Incendio en el Palacio muy Ilustre Municipio de Guayaquil.* Universidad de Guayaquil. Obtenido de

http://repositorio.ug.edu.ec/bitstream/redug/4806/1/Tesis Maestria Riesgos y Desastres JUAN RAMIREZ.pdf

Rincón, H., Antonio, J., Prieto, N., Gabriela, I., Chan, I., & Cabrera, M. (2018). Implementación de la metodología octave para el diagnóstico de seguridad informática. *Aristas, 6*. Obtenido de http://fcqi.tij.uabc.mx/usuarios/revistaaristas/nume

Roa Buendía, J. F. (2013). *Seguridad Informática.* McGraw/Interamericada de España.

Sanchez, J. S., Chalmeta, R., Colltel, O., Monfort, P., & Campos, C. (2003). *Ingenieria de proyectos informaticos: actividades y procedimientos.* Graphic Groups.

Secretaria de Gestión de Riesgo. (2010). Plan de Emergencia Institucional. Gestión De Riesgos. *1*, 1–76. Retrieved from www.snriesgos.gov.ec

SENADI. (2019). *Instituto Ecuatoriano de la Propiedad Intelectual*. Retrieved from https://www.propiedadintelectual.gob.ec/

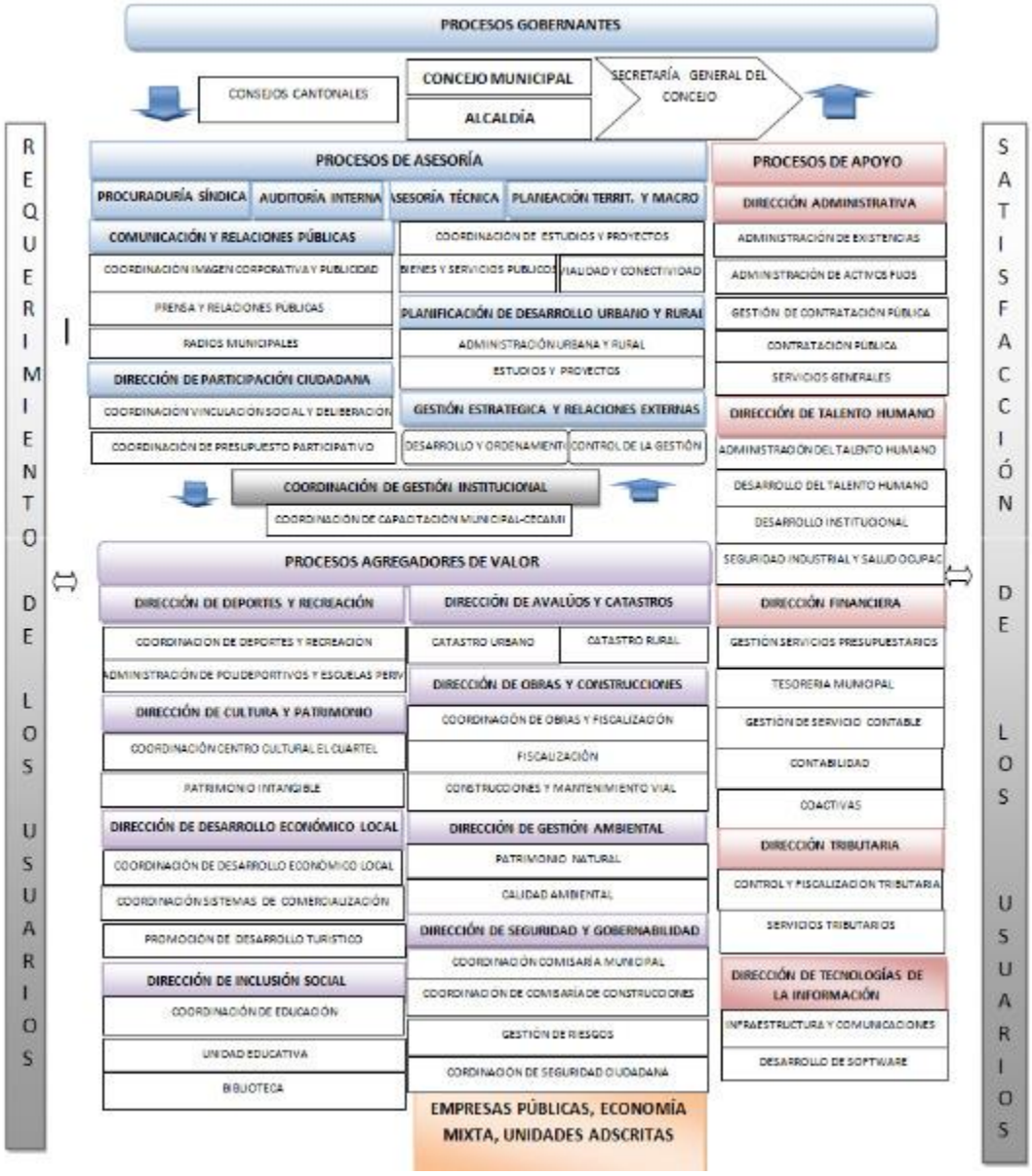
Taco, J. (2018). *Modelo de gestión energética para la determinación de indicadores de eficiencia eléctrica en el sector residencial.* Universidad Politécnica Salesiana.

Urbina Baca, G. (2016). *Introducción a la Seguridad Informática.* Patría.

Vivas, T., Huerta, M., Zambrano, A., Clotet, R., & Satizábal, C. (2015). Aplicación de mecanismos de seguridad en una red de telemedicina basados en certificados digitales. *IFMBE Proceedings*(18), 971–974. doi:https://doi.org/10.1007/978-3-540-74471-9_225

ANEXOS

ANEXO 1. Organigrama general del Gobierno Autónomo Descentralizado San Miguel de Ibarra.



ANEXO 2. Activos del GAD-Ibarra, clasificados mediante la Metodología Magerit v3.

Tabla 34 Tabla de activos denominado Servicios del GAD-Ibarra

SERVICIOS	
1	Administración De Servidores
2	Administración Réplica De Datos Del Sri
3	Alfresco Community
4	Aplicación Web De Reportes Del Sri
5	App Móvil
6	Aulas Virtuales
7	Avalúos Y Catastros
8	Bases De Datos
9	Capacitación
10	Compra Y Venta
11	Consola De Administración Dinners
12	Control Urbano
13	Control Vehicular
14	Firmador Sri
15	Geoportal
16	Informe De Compatibilidad Y Uso De Suelo
17	Informe De Reglamentación Cantonal (IRC)
18	Integración GADI-MOVIDELNOR
19	Kiosco Electrónico
20	Módulo De Bioseguridad
21	Módulo De Fichas Médicas
22	Módulo Teletón
23	Participación Ciudadana
24	Portal Académico Educativo
25	Portal Ciudadano
26	Portal De Documentos Electrónicos
27	Portales Web
28	Procesos Administrativos Unidad De Desarrollo
29	Procesos Batch
30	Registro Ciudadano
31	Reservas Espacios Culturales
32	RPI & GADI
33	Servicios En Línea
34	SIGET
35	SIGM
36	Simulador De Impuesto Predial Masivo

37	SISMERT
38	Sistema ERP OLYMPO ODOO
39	Sistema Académico Educativo
40	Sistema AS400 (IESS)
41	Sistema De Archivo Documental
42	Sistema De Concejo Municipal
43	Sistema De Fauna Urbana
44	Sistema De Gestión Documental Quipux
45	Sistema De Información Geográfica
46	Registro De Obras
47	Sistema De Parquímetros
48	Sistema De Partes Policiales
49	Sistema Transaccional Pagos En Línea
50	Sitios Web
51	Tasa De Turismo (LUAF)
52	Internet
53	Seguridad Perimetral
54	Video Seguridad
55	Antivirus/Antispam
56	Hosting De Servidores
57	Virtualización De Servidores
59	Help Desk
60	Mail
61	Telefonía IP
62	Control De Accesos
63	Energía
64	Biométricos

Tabla 35 Tabla de activos denominado Datos del GAD-Ibarra

	DATOS
1	Bases de datos de **Producción**: Alfanumérica, Espacial y Binaria (Master y Replica)
2	Base de Datos **Quipux** (Master y Replica)
3	Base de Datos **Firma Electrónica** (Master y Replica)
4	Bases de Datos **fotos** de Avalúos y Catastros y Tareas **activiti** (Master y Replica)
5	Base de datos **ODOO** (Master y Replica)
6	Base de datos Portal Web (Hosting)

7	Base de Datos SQL SERVER OLYMPO (Histórico)
8	Base de Datos de Correo Electrónico
9	Servidor de Desarrollo SCRIPTCASE V8
10	Servidor de Desarrollo SCRIPTCASE V9
11	Sistema réplica de Base de datos Oracle (SRI)
12	Servidor FREENAS almacenamiento de archivos de backups de bases de datos
13	Servidores de Aplicaciones GADI: ()
14	Archivos de configuración (equipos, aplicaciones, servicios)
15	Registros de Actividad (LOG) (equipos, servicios, antivirus)

Tabla 36 Tabla de activos denominado Aplicaciones del GAD-Ibarra

1	Sistema de información geográfica del GAD Ibarra
2	Portal ciudadano
3	Comprobantes electrónicos
4	Sistema de participación ciudadana
5	Portal web del Cantón Ibarra
6	Sistema de control urbano
7	Sistema de Talento Humano
8	Sistema de Gestión Municipal
9	Aplicación web de reportes servicio de rentas internas.
10	Sistema Moodle
11	Sistema de parquímetros
12	Aplicación web de reportes de parquímetros
13	Sistema de registro de obras
14	Módulo de consulta de impuestos y predios
15	Sistema Administrador TIC´s
16	Botón de pagos diners
17	Módulo de partes policiales
18	Sistema de Notificación y Multas
19	Sistema de Tránsito y transporte
20	Sistema SISMERT
21	Sistema de SIG IMI (web)
22	Sistema de Ventanilla Única
23	Sistema de Transferencias de Dominio
24	Sistemas de Control Vehicular
25	Sistema Control de turnos (GOIA Turnos)
26	Sistema SITAC (SRI)
	SISTEMAS OPERATIVOS

27	Centos
28	Windows
29	Ubuntu
30	Debian
31	Mac OS
	OTROS
32	Mozilla Firefox
33	Internet Explorer
34	Safari
35	Apache Tompcat
36	Pandora FMS
37	Map Server
38	Geo Server
39	Tile Cache
40	Web Mind
41	ARC SDE
42	Mozilla Thunderbird
43	Postgres SQL
44	My SQL
45	Post GIS
46	Microsoft Office
47	Open Office
48	Autocad
49	Autocad Map 3D
50	Topografía MDT 6
51	Eset Nod 32

Tabla 37 Tabla de activos denominado Equipos Informáticos del GAD-Ibarra

APLICACIONES	
1	Firewall Check Point 4600
2	Smart Event
3	Switch Core Chasis
4	Router Borde
5	Switch Administración
6	Switch Distribución
7	Switch De Acceso
8	Chasis Blade
9	Almacenamiento
10	Onboard Administrator
11	Onboard Administrator Backup

12	Blade Switch
13	Blade Switch Bay 2
14	San Switch
15	Swichlan1 DELL HYPERCONVERGENCIA
16	Swichlan2 DELL HYPERCONVERGENCIA
17	Swich SAN DELL
18	Servidor De Almacenamiento Storage (I)
19	Servidor Sigad Hp Bl 460 G8 (Proyecto Caf) Bay 3
20	Servidor Sigad Hp Bl 460 G8 (Proyecto Caf) Bay 4
21	Servidor de BDD Prueba
22	Servidor Portal Ciudadano (Migrar Disco)
23	Servidor INTERPRO
24	Servidor Aplicación Web Ligas Barriales
25	Servidor SCRIPCASE
26	Servidor De Aplicación De Firma Electrónica Clon
27	Servidor Aplicaciones Móviles Desarrollo
28	SERVIDOR DE CORREO VIRSAP (Migrar Disco)
29	Servidor HP BL 460 G6 Bay 5
30	Free NAS Almacenamiento
31	Servidor Control De Personal
32	Servidor Administración
33	Servidor Firma Electrónica Sri Clon
34	Servidor Hp Bl 460 G6 Bay1
35	Servidor Servicios De Red DNS Y DHCP
36	Servidor Read Mine
37	Servidor NTP
38	Servidor Sri
39	Servidor Promox (Srv5)
40	Servidor Moodle
41	Servidor De Balanced Scord Card
42	Servidor De Streaming
43	Servidor Hp BL 460 G8 Bay 8
44	Servidor Contoller Unifi
45	Servidor De OCS
46	Servidor Carpetas De Planificación
47	Servidor Monitoreo Cámaras GAD Ibarra
48	Servidor Voz IP
49	Servidor Parqueo Tarifado
50	Servidor Parroquias

51	Servidor DNS
52	Servidor Dude Monitoreo De Red
53	Servidor OLYMPO 2012
54	Servidor Hp Blade Gen 9 Bay 2
55	Servidor SIGM Desarrollo Nueva Versión
56	Servidor UGPC IREKIA
57	Servidor ERP ODOO
58	Servidor ERP ODOO Desarrollo
59	Servidor Moodle
60	Servidor Aplicaciones SIG Producción
61	Servidor Aplicaciones SIG Producción Nueva Versión
62	Servidor Aplicaciones SIG Producción Nueva Falla
63	Servidor Zoom
64	Servidor Quipux Pruebas
65	Servidor Quipux BDD Clon
66	Servidor Hp Dl Gen9
67	Servidor Base De Datos Espejo Avalúos
68	Servidor Base De Datos Espejo ODOO
69	Servidor De Balanceo De Aplicaciones
70	Servidor De Balanceo De Aplicaciones Web
71	Servidor Portal Ciudadano Nueva Versión
72	Servidor Pruebas
73	PROLIANT BL460c Gen9 (Bay 7)
74	Servidor Virtual FREENAS 11.0
75	Servidor Antivirus
76	Servidor Replica BDD Producción
77	Servidor Replica BDD Quipux Producción
78	Servidor Quipux Prueba
79	Servidor Quipux Firma Electrónica Pr
80	Servidor BDD Producción
81	Servidor BDD GADI Antiguo Producción
82	Servidor Respaldo Bomberos
83	Servidor Respaldo Bomberos
84	Servidor Monitoreo Pandora
85	Servidor Documental Alfresco Clon
86	Servidor Pruebas GADI
87	Servidor BDD ACTIVITY Replica
88	Servidor SCRIP Case Nueva Versión
89	Servidor Dell Host 1

90	Servidor Dell Host 2
91	Servidor Dell Host 3
92	VCENTER
93	Servidor Clon BDD Firma Electrónica
94	Servidor Aplicación Firma Electrónica
95	Servidor Aplicación Quipux
96	Base De Datos Geo Espacial
97	Servidor De Aplicaciones De Quipux 2
98	Servidor De Repositorio Alfresco
99	Servidor De Aplicaciones Web1
100	Servidor De Aplicaciones Web2
101	Servidor GPR
102	Servidor PG Pool
103	Servidor Correo NV
104	Servidor Firma Electrónica BDD
105	Servidor BDD Odo Replica,
106	Servidor BDD Quipux
107	Servidor BDD Produccion0
108	Servidor Heldeskp
109	Servidor De BDD Activity
110	Servidor De Avalúos Y Catastros APPL
111	Servidor De Avalúos Y Catastros APPL 2
112	Servidor File Server
113	Servidor Moodle
114	Servidor WIN Sr1 1
115	Servidor WIN Sr1 2
116	Servidor De Active Directory
117	Servidor Firma Electrónica SRI
118	Veam BEACOUP
119	VMWARE One
120	Servidor De Monitoreo
121	Servidor Smart Event

Tabla 38 Tabla de activos denominado Redes de Comunicación del GAD-Ibarra

REDES DE COMUNICACIÓN	
1	RED LAN
2	RED WLAN
3	RED MAN
4	RED WAN (ENLACES EXTERNOS)
5	CONECTATE IBARRA

Tabla 39 Tabla de activos denominado Soporte de Información del GAD-Ibarra

SOPORTE DE INFORMACION	
1	Discos externos de respaldos de información (Sistema y Datos)
2	CD
3	DVD
4	Storage Blade
5	Proyectos, Planes, Evaluaciones, Informes de TIC
6	USB

Tabla 40 Tabla de activos denominado Equipamiento Auxiliar del GAD-Ibarra

EQUIPAMINTO AUXILIAR	
1	Fuentes de Alimentación (servers)
2	Fuentes de Alimentación (PCs)
3	Equipos de Climatización
4	Cableado Estructurado
5	Fibra Óptica
6	Sistemas de Alimentación Ininterrumpida (Servers)
7	Sistemas de Alimentación Ininterrumpida (PCs)
8	UPS
9	Generador eléctrico

Tabla 41 Tabla de activos denominado Instalaciones del GAD-Ibarra

	INSTALACIONES
1	Data Center
2	Oficinas TIC
3	Sala de reuniones
4	**Nodo 1** Cuartel Antiguo (García Moreno y Olmedo)
5	**Nodo 2** Casa de la Ibarreñidad (Bolívar y Flores)
6	**Nodo 3** Dirección de Turismo (Esquina del Coco, Oviedo y Sucre)
7	**Nodo 4** Dirección de Planificación (García Moreno)
8	**Nodo 5** Dirección de Comunicación (García Moreno)
9	**Nodo 6** Administración de mercados (Obispo Mosquera y Eugenio Espejo)
10	**Nodo 7** Centro de educación Inicial María Olimpia Gudiño (Eugenio Espejo y Teodoro Gómez)
11	**Nodo 8** Unidad Educativa Alfredo Albuja Galindo (Av. Tobar y Tobar y Luis Jaramillo Pérez)
12	**Nodo 9** Casa de la Justicia (Av. Mariano Acosta)
13	**Nodo 10** Unidad de Activos Fijos (Victoria Castello Chiriboga y German Granja)
14	**Nodo 11** Unidad de Comisaria de Construcciones (Manuela Cañizares y Laura Jaramillo)
15	**Nodo 12** Teatro Gran Colombia (Flores y Sucre)
16	**Nodo 13** Bodega Municipal (Víctor Manuel Guzmán y Uruguay)
17	**Nodo 14** Centro Mis Abuelitos (Tobías Mena y Gral. Julio Andrade)
18	**Nodo 15** Mercado Santo Domingo (Rafael Troya y Chica Narváez)
19	**Nodo 16** EMAPA (Sucre y Pedro Moncayo)
20	**Nodo 17** Cuerpo de Bomberos X1 (Luis Fernando Villamar y Olmedo)

Tabla 42 Tabla de activos denominado Personal del GAD-Ibarra

PERSONAL	
1	Usuarios externos
2	Usuarios Internos
3	Administrados de BDD
4	Administrador de redes y comunicaciones

5	Analistas de Sistemas
6	Técnicos de Soporte
7	Proveedores Olympo
8	Proveedores Fiel Web
9	Proveedor de ordenador de colas GOIA
10	Proveedor de Internet
11	Proveedor de Equipos

ANEXO 3. Valoración de activos del GAD-Ibarra

Ver en el siguiente link.

https://1drv.ms/b/s!AmZvMg8oum26hPQ52SNlVxpcD7ZEgQ?e=WaxcBU

ANEXO 4: Amenazas

- [N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen: Natural (accidental)

- [N.1] Fuego

Tabla 43 Daños por Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema.	
Ver: EBIOS: 01- INCENDIO	

- [N.2] Daños por agua

Tabla 44 Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad

Descripción:
inundaciones: posibilidad de que el agua acabe con recursos del sistema.
Ver:
EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA

- [N.*] Desastres Naturales

Tabla 45 Daños por Desastres Naturales

[N.*] Desastres naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ... Se excluyen desastres específicos tales como incendios e inundaciones Se excluye al personal por cuanto se ha previsto una amenaza específica para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Ver:** EBIOS: 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 – INUNDACIÓN	

- **[I] De origen industrial**

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

- [I.1] Fuego

Tabla 46 Daños por fuego de Origen Industrial

[I.1] Fuego

Tipos de activos:

- [HW] equipos informáticos (hardware)
- [Media] soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones

Dimensiones:

1. [D] disponibilidad

Descripción:

incendio: posibilidad de que el fuego acabe con los recursos del sistema.

Origen:

Entorno (accidental)
Humano (accidental o deliberado)

Ver:

EBIOS: 01- INCENDIO

- [I.2] Daños por agua

Tabla 47 Daño por agua de Origen Industrial

[I.2] Daños por agua

Tipos de activos:

- [HW] equipos informáticos (hardware)
- [Media] soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones

Dimensiones:

1. [D] disponibilidad

Descripción:

escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Origen:

Entorno (accidental)
Humano (accidental o deliberado)

Ver:

EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA

- [I.*] Desastres industriales

Tabla 48 Daño por Desastres Industriales

[I.*] Desastres industriales

Tipos de activos:

- [HW] equipos informáticos (hardware)
- [Media] soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones

Dimensiones:

1. [D] disponibilidad

Descripción:

Otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ...

sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ...

Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]).

Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.

Origen:

Entorno (accidental)

Humano (accidental o deliberado)

Ver:

EBIOS: 04 - SINIESTRO MAYOR

- [I.3] Contaminación mecánica

Tabla 49 Daños por Contaminación Mecánica

[I.3] Contaminación mecánica	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad

Descripción:

vibraciones, polvo, suciedad, ...

Origen:

Entorno (accidental)

Humano (accidental o deliberado)

Ver:

EBIOS: 03 – CONTAMINACIÓN

- [I.4] Contaminación Electromagnética

Tabla 50 Daños por Contaminación Electromagnética

[I.4] Contaminación electromagnética	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad

Descripción:
interferencias de radio, campos magnéticos, luz ultravioleta, ...
Origen:
Entorno (accidental)
Humano (accidental o deliberado)
Ver:
EBIOS:
14 - EMISIONES ELECTROMAGNÉTICAS
15- RADIACIONES TÉRMICAS
16 - IMPULSOS ELECTROMAGNÉTICOS

- [I.5] Avería de Origen Físico o Lógico

Tabla 51 Daño por avería Físico o Lógico

[I.5] Avería de origen físico o lógico
Tipos de activos:
- [SW] aplicaciones (software)
- [HW] equipos informáticos (hardware)
- [Media] soportes de información
- [AUX] equipamiento auxiliar

Dimensiones:
1. [D] disponibilidad

Descripción:
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
Origen:
Entorno (accidental)
Humano (accidental o deliberado)
Ver:
EBIOS:
28 - AVERÍA DEL HARDWARE
29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE

- [I.6] Corte del suministro eléctrico

Tabla 52 Corte del suministro eléctrico

[I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la alimentación de potencia **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA	

- **[I.7] Condiciones inadecuadas de temperatura o humedad**

Tabla 53 Condiciones inadecuadas de temperatura o humedad

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN	

[I.8] Fallo de servicios de comunicaciones

Tabla 54 Fallo de servicios de comunicaciones

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos:	**Dimensiones:**
• [COM] redes de comunicaciones	1. [D] disponibilidad
Descripción: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	
Origen: Entorno (accidental) Humano (accidental o deliberado)	
Ver: EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN	

[I.9] Interrupción de otros servicios y suministros esenciales

Tabla 55 Interrupción de otros servicios y suministros esenciales

[I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos:	**Dimensiones:**
• [AUX] equipamiento auxiliar	1. [D] disponibilidad
Descripción: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ...	
Origen: Entorno (accidental) Humano (accidental o deliberado)	
Ver: EBIOS: no disponible	

- **[I.10] Degradación de los soportes de almacenamiento de la información**

Tabla 56 Degradación de los soportes de almacenamiento de la información

[I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad
Descripción: como consecuencia del paso del tiempo	
Origen: Entorno (accidental) Humano (accidental o deliberado)	
Ver: EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

- **[I.11] Emanaciones electromagnéticas**

Tabla 57 Daños por Emanaciones electromagnéticas

[I.11] Emanaciones electromagnéticas	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] media • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés "Transient Electromagnetic Pulse Standard"). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "TEMPEST protection", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.	

Origen:
Entorno (accidental)
Humano (accidental o deliberado)
Ver:
EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS

- **[E] Errores y fallos no intencionados**

Fallos no intencionales causados por las personas. - La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Origen:

Humano (accidental)

[E.1] Errores de los usuarios

Tabla 58 Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. **Ver:** EBIOS: 38 - ERROR DE USO	

- **[E.2] Errores del administrador**

Tabla 59 Errores del administrador

[E.2] Errores del administrador

Tipos de activos:

- [D] datos / información
- [keys] claves criptográficas
- [S] servicios
- [SW] aplicaciones (software)
- [HW] equipos informáticos (hardware)
- [COM] redes de comunicaciones
- [Media] soportes de información

Dimensiones:

1. [D] disponibilidad
2. [I] integridad
3. [C] confidencialidad

Descripción:

equivocaciones de personas con responsabilidades de instalación y operación

Ver:

EBIOS: 38 - ERROR DE USO

- **[E.3] Errores de monitorización *(log)***

Tabla 60 Errores de monitorización (log)

[E.3] Errores de monitorización *(log)*

Tipos de activos:

- [D.log] registros de actividad

Dimensiones:

1. [I] integridad (trazabilidad)

Descripción:

inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...

Ver:

EBIOS: no disponible

- **[E.4] Errores de configuración**

Tabla 61 Errores de configuración

[E.4] Errores de configuración

Tipos de activos:

- [D.conf] datos de configuración

Dimensiones:

1. [I] integridad

Descripción:

introducción de datos de configuración erróneos.

Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad- ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

Ver:

EBIOS: no disponible

- **[E.7] Deficiencias en la organización**

Tabla 62 Deficiencias en la organización

[E.7] Deficiencias en la organización	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] disponibilidad
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc. **Ver:** EBIOS: no disponible	

- **[E.8] Difusión de software dañino**

Tabla 63 Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

- **[E.9] Errores de [re-]encaminamiento**

Tabla 64 Errores de [re-]encaminamiento

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad

Descripción:

envío de información a través de un sistema o una red usando, accidentalmente, una ruta in- correcta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.

Ver:

EBIOS: no disponible

- **[E.10] Errores de secuencia**

Tabla 65 Errores de secuencia

[E.10] Errores de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental del orden de los mensajes transmitidos.	
Ver: EBIOS: no disponible	

- **[E.14] Escapes de información**

Obsoleta: use E.19.

Tabla 66 Escapes de información

[E.14] Escapes de información	
Tipos de activos: 	**Dimensiones:** 1. [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

- **[E.15] Alteración accidental de la información**

Tabla 67 Alteración accidental de la información

[E.15] Alteración accidental de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

- **[E.18] Destrucción de información**

Tabla 68 Destrucción de información

[E.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

- **[E.19] Fugas de información**

Tabla 69 Fugas de información

[E.19] Fugas de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. **Ver:** EBIOS: no disponible	

- **[E.20] Vulnerabilidades de los programas (software)**

Tabla 70 Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. **Ver:** EBIOS: no disponible	

- **[E.21] Errores de mantenimiento / actualización de programas (software)**

Tabla 71 Errores de mantenimiento / actualización de programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. **Ver:** EBIOS: 31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

- **[E.23] Errores de mantenimiento / actualización de equipos (hardware)**

Tabla 72 Errores de mantenimiento / actualización de equipos (hardware)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes electrónicos • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. **Ver:** EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

- **[E.24] Caída del sistema por agotamiento de recursos**

Tabla 73 Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos

Tipos de activos:
- [S] servicios
- [HW] equipos informáticos (hardware)
- [COM] redes de comunicaciones

Dimensiones:
1. [D] disponibilidad

Descripción:
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Ver:
EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO

- **[E.25] Pérdida de equipos**

Tabla 74 Pérdida de equipos

[E.25] Robo

Tipos de activos:
- [HW] equipos informáticos (hardware)
- [Media] soportes de información
- [AUX] equipamiento auxiliar

Dimensiones:
1. [D] disponibilidad
2. [C] confidencialidad

Descripción:
la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.
En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

Ver:
EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS

- **[E.28] Indisponibilidad del personal**

Tabla 75 Indisponibilidad del personal

[E.28] Indisponibilidad del personal

Tipos de activos:
- [P] personal interno

Dimensiones:
1. [D] disponibilidad

Descripción:
ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ...
Ver:
EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL

[A] Ataques intencionados

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas ve- ces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen:

Humano (deliberado)

- **[A.3] Manipulación de los registros de actividad (log)**

Tabla 76 Manipulación de los registros de actividad (log)

[A.4] Manipulación de los registros de actividad (log)	
Tipos de activos:	**Dimensiones:**
• [D.log] registros de actividad	1. [I] integridad (trazabilidad)
Descripción:	
Ver: EBIOS: no disponible	

- **[A.4] Manipulación de la configuración**

Tabla 77 Manipulación de la configuración

[A.4] Manipulación de la configuración	
Tipos de activos:	**Dimensiones:**
• [D.log] registros de actividad	1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad

Descripción:

prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

Ver:

EBIOS: no disponible

- **[A.5] Suplantación de la identidad del usuario**

Tabla 78 Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. **Ver:** EBIOS: 40 - USURPACIÓN DE DERECHO	

- **[A.6] Abuso de privilegios de acceso**

Tabla 79 Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad

Descripción:

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

Ver:

EBIOS: 39 - ABUSO DE DERECHO

- **[A.7] Uso no previsto**

Tabla 80 Uso no previsto

[A.7] Uso no previsto	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad 3. [I] integridad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. **Ver:** EBIOS: no disponible	

- **[A.8] Difusión de software dañino**

Tabla 81 Difusión de software dañino

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad

Descripción:

propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.

Ver:

EBIOS: no disponible

- **[A.9] Re-]encaminamiento de mensajes**

Tabla 82 Re-]encaminamiento de mensajes

[A.9] [Re-]encaminamiento de mensajes

Tipos de activos:

- [S] servicios
- [SW] aplicaciones (software)
- [COM] redes de comunicaciones

Dimensiones:

1. [C] confidencialidad

Descripción:

envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.

Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado.

Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.

Ver:

EBIOS: no disponible

- **[A.10] Alteración de secuencia**

Tabla 83 Daño Alteración de secuencia

[A.10] Alteración de secuencia

Tipos de activos:

- [S] servicios
- [SW] aplicaciones (software)
- [COM] redes de comunicaciones

Dimensiones:

1. [I] integridad

Descripción:

alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.

Ver:

EBIOS: 36 - ALTERACIÓN DE DATOS

- **[A.11] Acceso no autorizado**

Tabla 84 Daño por Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos:	**Dimensiones:**
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [C] confidencialidad 2. [I] integridad

Descripción:

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

Ver:

EBIOS: 33 - USO ILÍCITO DEL HARDWARE

- **[A.12] Análisis de tráfico**

Tabla 85 Daño por Análisis de tráfico

[A.12] Análisis de tráfico	
Tipos de activos:	**Dimensiones:**
• [COM] redes de comunicaciones	1. [C] confidencialidad

Descripción:

el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.

A veces se denomina “monitorización de tráfico”.

Ver:

EBIOS: no disponible

- **[A.13] Repudio**

Tabla 86 Daño por Repudio

[A.13] Repudio

Tipos de activos:

- [S] servicios
- [D.log] registros de actividad

Dimensiones:

1. [I] integridad (trazabilidad)

Descripción:

negación a posteriori de actuaciones o compromisos adquiridos en el pasado.

Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación.

Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.

Ver:

EBIOS: 41 - NEGACIÓN DE ACCIONES

- **[A.14] Interceptación de información (escucha)**

Tabla 87 Daño por Interceptación de información (escucha)

[A.14] Interceptación de información (escucha)

Tipos de activos:

- [COM] redes de comunicaciones

Dimensiones:

1. [C] confidencialidad

Descripción:

el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.

Ver:

EBIOS: 19 - ESCUCHA PASIVA

- **[A.15] Modificación deliberada de la información**

Tabla 88 Daño por Modificación deliberada de la información

[A.15] Modificación deliberada de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

- **[A.18] Destrucción de información**

Tabla 89 Daño por Destrucción de información

[A.18] Destrucción de información

Tipos de activos:

- [D] datos / información
- [keys] claves criptográficas
- [S] servicios (acceso)
- [SW] aplicaciones (SW)
- [Media] soportes de información
- [L] instalaciones

Dimensiones:

1. [D] disponibilidad

Descripción:

eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

Ver:

EBIOS: no disponible

- **[A.19] Divulgación de información**

Tabla 90 Daño por Divulgación de información

[A.19] Revelación de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación de información. **Ver:** EBIOS: 23 – DIVULGACIÓN 27 – GEOLOCALIZACIÓN 34 - COPIA ILEGAL DE SOFTWARE	

- **[A.22] Manipulación de programas**

Tabla 91 Daño por Manipulación de programas

[A.22] Manipulación de programas

Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad

Descripción:
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

Ver:
EBIOS: 26 - ALTERACIÓN DE PROGRAMAS

- **[A.23] Manipulación de los equipos**

Tabla 92 Daño por Manipulación de los equipos

[A.22] Manipulación de los equipos	
Tipos de activos: • [HW] equipos • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [C] confidencialidad 2. [D] disponibilidad

Descripción:
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

Ver:
EBIOS: 25 - SABOTAJE DEL HARDWARE

- **[A.24] Denegación de servicio**

Tabla 93 Daño por Denegación de servicio

[A.24] Denegación de servicio	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad

Descripción:

la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Ver:

EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO

- **[A.25] Robo**

Tabla 94 Daño por robo

[A.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 3. [D] disponibilidad 4. [C] confidencialidad
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. **Ver:** EBIOS: 20 - ROBO DE SOPORTES O DOCUMENTOS 21 - ROBO DE HARDWARE	

- **[A.26] Ataque destructivo**

Tabla 95 Daño por Ataque destructivo

[A.26] Ataque destructivo

Tipos de activos:

- [HW] equipos informáticos (hardware)
- [Media] soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones

Dimensiones:

1. [D] disponibilidad

Descripción:

vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

Ver:

EBIOS: 05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES

- **[A.27] Ocupación enemiga**

Tabla 96 Daño por Ocupación enemiga

[A.27] Ocupación enemiga

Tipos de activos:

- [L] instalaciones

Dimensiones:

1. [D] disponibilidad
2. [C] confidencialidad

Descripción:

cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

Ver:

EBIOS: no disponible

- **[A.28] Indisponibilidad del personal**

Tabla 97 Daño por Indisponibilidad del personal

[A.28] Indisponibilidad del personal

Tipos de activos:

- [P] personal interno

Dimensiones:

1. [D] disponibilidad

Descripción:

ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ...

Ver:

EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL

- **[A.29] Extorsión**

Tabla 98 Daño por Extorsión

[A.29] Extorsión	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. **Ver:** EBIOS: no disponible	

- **[A.30] Ingeniería social (picaresca)**

Tabla 99 Daño por Ingeniería social (picaresca)

[A.30] Ingeniería social (picaresca)	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. **Ver:** EBIOS: no disponible	

ANEXO 5: Encuestas realizadas al personal de la Dirección de TICS

SERVICIOS		DISPONIBILIDAD					
		LARA	EOCHOA	ALVAREZ	BUCHELI	MESA	RESULTADO
1	Administración De Servidores	10	10	10	10	10	10
2	Administración Réplica De Datos Del Sri	10	10	8	4	5	7
3	Alfresco Community	7	10	6	5	4	6
4	Aplicación Web De Reportes Del Sri	7	10	6	5	5	7
5	App Móvil	3	9	3	7	7	6
6	Aulas Virtuales	3	10	4	5	5	5
7	Avalúos Y Catastros	10	10	10	10	10	10
8	Bases De Datos	10	10	10	10	10	10
9	Capacitación	3	10	2	5	4	5
10	Compra Y Venta	8	10	2	5	4	6
11	Consola De Administración Dinners	0	10	10	5	5	6
12	Control Urbano	10	10	10	5	5	8
13	Control Vehicular	10	10	9	5	5	8
14	Firmador Sri	10	10	9	5	5	8
15	Geoportal	7	10	8	5	6	7
16	Informe De Compatibilidad Y Uso De Suelo	9	10	8	5	8	8
17	Informe De Reglamentación Cantonal (IRC)	9	10	8	5	8	8
18	Integración GADI-MOVIDELNOR	0	10	10	5	7	6
19	Kiosco Electrónico	7	10	8	5	5	7
20	Módulo De Bioseguridad	1	10	3	5	5	5
21	Módulo De Fichas Médicas	0	10	3	5	5	5
22	Módulo Teletón	0	9	5	5	5	5
23	Participación Ciudadana	8	10	9	5	5	7
24	Portal Académico Educativo	8	10	6	5	5	7
25	Portal Ciudadano	10	10	10	10	10	10
26	Portal De Documentos Electrónicos	8	10	10	5	5	8
27	Portales Web	10	10	10	5	5	8
28	Procesos Administrativos Unidad De Desarrollo	0	10	8	5	5	6
29	Procesos Batch	10	10	10	5	5	8
30	Registro Ciudadano	10	10	8	5	5	8

31	Reservas Espacios Culturales	10	9	8	5	5	**7**
32	RPI & GADI	10	10	10	5	5	**8**
33	Servicios En Línea	10	10	10	5	5	**8**
34	SIGET	10	10	10	5	6	**8**
35	SIGM	10	10	10	10	10	**10**
36	Simulador De Impuesto Predial Masivo	6	10	10	5	5	**7**
37	SISMERT	10	10	10	5	5	**8**
38	Sistema ERP OLYMPO ODOO	10	10	10	10	10	**10**
39	Sistema Académico Educativo	8	10	8	5	5	**7**
40	Sistema AS400 (IESS)	8	10	8	5	5	**7**
41	Sistema De Archivo Documental	8	10	8	5	5	**7**
42	Sistema De Concejo Municipal	10	10	10	5	5	**8**
43	Sistema De Fauna Urbana	7	10	7	5	5	**7**
44	Sistema De Gestión Documental Quipux	10	10	10	10	10	**10**
45	Sistema De Información Geográfica	8	10	10	5	5	**8**
46	Sistema De Información Geográfica De	8	10	10	5	5	**8**
47	Registro De Obras	0	10	8	5	5	**6**
48	Sistema De Parquímetros	10	10	6	5	5	**7**
49	Sistema De Partes Policiales	0	10	4	5	5	**5**
50	Sistema Transaccional Pagos En Línea	10	10	10	5	5	**8**
51	Sitios Web	10	10	10	5	5	**8**
52	Tasa De Turismo (LUAF)	7	10	8	5	5	**7**
53	Internet	10	10	10	10	10	**10**
54	Seguridad Perimetral	10	10	8	10	10	**10**
55	Video Seguridad	8	9	9	5	6	**7**
56	Antivirus/Antispam	10	10	10	5	6	**8**
57	Hosting De Servidores	10	10	10	10	10	**10**
58	Virtualización De Servidores	10	10	10	10	10	**10**
59	Quipux	10	10	10	10	10	**10**
60	Help Desk	10	10	8	10	10	**10**
61	Mail	10	10	10	7	7	**9**
62	Telefonía IP	10	10	10	5	5	**8**
63	Control De Accesos	10	10	7	5	6	**8**
64	Energía	10	10	10	5	5	**8**
65	Biométricos	10	10	10	5	5	**8**

SERVICIOS		INTEGRIDAD					
		LARA	EOCHOA	ALVAREZ	BUCHELI	MESA	RESULTADO
1	Administración De Servidores	10	10	10	10	10	10
2	Administración Réplica De Datos Del Sri	10	10	10	10	10	10
3	Alfresco Community	10	10	8	5	5	7,6
4	Aplicación Web De Reportes Del Sri	10	10	6	5	5	7,2
5	App Móvil	9	10	6	7	7	7,8
6	Aulas Virtuales	9	10	6	5	5	7
7	Avalúos Y Catastros	10	10	10	10	10	10
8	Bases De Datos	10	10	10	10	10	10
9	Capacitación	9	10	5	5	5	6,8
10	Compra Y Venta	9	10	3	5	5	6,4
11	Consola De Administración Dinners	0	10	10	10	10	8
12	Control Urbano	10	10	10	10	10	10
13	Control Vehicular	10	10	10	10	10	10
14	Firmador Sri	10	10	10	10	10	10
15	Geoportal	10	10	10	10	10	10
16	Informe De Compatibilidad Y Uso De Suelo	10	10	10	10	10	10
17	Informe De Reglamentación Cantonal (IRC)	10	10	10	10	10	10
18	Integración GADI-MOVIDELNOR	0	10	10	10	10	8
19	Kiosco Electrónico	7	10	8	10	10	9
20	Módulo De Bioseguridad	9	10	5	10	10	8,8
21	Módulo De Fichas Médicas	0	10	8	10	10	7,6
22	Módulo Teletón	0	10	6	10	10	7,2
23	Participación Ciudadana	10	10	10	10	10	10
24	Portal Académico Educativo	10	10	10	10	10	10
25	Portal Ciudadano	10	10	10	10	10	10
26	Portal De Documentos Electrónicos	10	10	10	10	10	10
27	Portales Web	10	10	10	10	10	10
28	Procesos Administrativos Unidad De Desarrollo	0	10	10	10	10	8
29	Procesos Batch	10	10	10	10	10	10
30	Registro Ciudadano	10	10	10	10	10	10
31	Reservas Espacios Culturales	10	10	8	10	10	9,6

32	RPI & GADI	10	10	10	10	10	**10**
33	Servicios En Línea	10	10	10	10	10	**10**
34	SIGET	10	10	10	10	10	**10**
35	SIGM	10	10	10	10	10	**10**
36	Simulador De Impuesto Predial Masivo	10	10	10	10	10	**10**
37	SISMERT	10	10	10	10	10	**10**
38	Sistema ERP OLYMPO ODOO	10	10	10	10	10	**10**
39	Sistema Académico Educativo	10	10	10	10	10	**10**
40	Sistema AS400 (IESS)	10	10	10	10	10	**10**
41	Sistema De Archivo Documental	10	10	10	10	10	**10**
42	Sistema De Concejo Municipal	10	10	10	10	10	**10**
43	Sistema De Fauna Urbana	10	10	10	10	10	**10**
44	Sistema De Gestión Documental Quipux	10	10	10	10	10	**10**
45	Sistema De Información Geográfica	10	10	10	10	10	**10**
46	Sistema De Información Geográfica De	10	10	10	10	10	**10**
47	Registro De Obras	0	10	10	10	10	**8**
48	Sistema De Parquímetros	10	10	10	10	10	**10**
49	Sistema De Partes Policiales	0	10	6	10	10	**7,2**
50	Sistema Transaccional Pagos En Línea	10	10	10	10	10	**10**
51	Sitios Web	10	10	10	10	10	**10**
52	Tasa De Turismo (LUAF)	10	10	10	10	10	**10**
53	Internet	10	10	10	10	10	**10**
54	Seguridad Perimetral	10	10	10	10	10	**10**
55	Video Seguridad	10	10	10	10	10	**10**
56	Antivirus/Antispam	10	10	10	10	10	**10**
57	Hosting De Servidores	10	10	10	10	10	**10**
58	Virtualización De Servidores	10	10	10	10	10	**10**
59	Quipux	10	10	10	10	10	**10**
60	Help Desk	10	10	8	10	10	**9,6**
61	Mail	10	10	10	10	10	**10**
62	Telefonía IP	10	10	10	10	10	**10**
63	Control De Accesos	10	10	10	10	10	**10**
64	Energía	1	10	5	10	10	**7,2**
65	Biométricos	10	10	10	10	10	**10**

SERVICIOS		CONFIDENCIALIDAD					
		LARA	EOCHOA	ALVAREZ	BUCHELI	MESA	RESULTADO
1	Administración De Servidores	10	10	10	10	10	10
2	Administración Réplica De Datos Del Sri	10	10	10	10	10	10
3	Alfresco Community	7	10	7	5	5	6,8
4	Aplicación Web De Reportes Del Sri	7	10	10	5	5	7,4
5	App Móvil	9	10	8	7	7	8,2
6	Aulas Virtuales	9	10	6	5	5	7
7	Avalúos Y Catastros	10	10	10	10	10	10
8	Bases De Datos	10	10	10	10	10	10
9	Capacitación	9	10	2	5	5	6,2
10	Compra Y Venta	9	10	3	5	5	6,4
11	Consola De Administración Dinners	0	10	7	10	10	7,4
12	Control Urbano	10	10	10	10	10	10
13	Control Vehicular	10	10	10	10	10	10
14	Firmador Sri	10	10	10	10	10	10
15	Geoportal	10	10	10	10	10	10
16	Informe De Compatibilidad Y Uso De Suelo	10	10	10	10	10	10
17	Informe De Reglamentación Cantonal (IRC)	10	10	10	10	10	10
18	Integración GADI-MOVIDELNOR	0	10	10	10	10	8
19	Kiosco Electrónico	7	10	8	10	10	9
20	Módulo De Bioseguridad	5	10	5	10	10	8
21	Módulo De Fichas Médicas	0	10	8	10	10	7,6
22	Módulo Teletón	0	10	6	10	10	7,2
23	Participación Ciudadana	10	10	8	10	10	9,6
24	Portal Académico Educativo	10	10	9	10	10	9,8
25	Portal Ciudadano	10	10	10	10	10	10
26	Portal De Documentos Electrónicos	10	10	10	10	10	10
27	Portales Web	10	10	8	10	10	9,6
28	Procesos Administrativos Unidad De Desarrollo	0	10	9	10	10	7,8
29	Procesos Batch	10	10	10	10	10	10
30	Registro Ciudadano	10	10	10	10	10	10

31	Reservas Espacios Culturales	10	10	8	10	10	**9,6**
32	RPI & GADI	10	10	10	10	10	**10**
33	Servicios En Línea	10	10	10	10	10	**10**
34	SIGET	10	10	10	10	10	**10**
35	SIGM	10	10	10	10	10	**10**
36	Simulador De Impuesto Predial Masivo	10	10	10	10	10	**10**
37	SISMERT	10	10	10	10	10	**10**
38	Sistema ERP OLYMPO ODOO	10	10	10	10	10	**10**
39	Sistema Académico Educativo	10	10	10	10	10	**10**
40	Sistema AS400 (IESS)	10	10	10	10	10	**10**
41	Sistema De Archivo Documental	8	10	10	10	10	**9,6**
42	Sistema De Concejo Municipal	10	10	10	10	10	**10**
43	Sistema De Fauna Urbana	10	10	8	10	10	**9,6**
44	Sistema De Gestión Documental Quipux	10	10	10	10	10	**10**
45	Sistema De Información Geográfica	10	10	10	10	10	**10**
46	Sistema De Información Geográfica De	10	10	10	10	10	**10**
47	Registro De Obras	0	10	10	10	10	**8**
48	Sistema De Parquímetros	10	10	8	10	10	**9,6**
49	Sistema De Partes Policiales	0	10	6	10	10	**7,2**
50	Sistema Transaccional Pagos En Línea	10	10	10	10	10	**10**
51	Sitios Web	10	10	8	10	10	**9,6**
52	Tasa De Turismo (LUAF)	10	10	10	10	10	**10**
53	Internet	10	10	10	10	10	**10**
54	Seguridad Perimetral	10	10	8	10	10	**9,6**
55	Video Seguridad	10	10	8	10	10	**9,6**
56	Antivirus/Antispam	10	10	10	10	10	**10**
57	Hosting De Servidores	10	10	10	10	10	**10**
58	Virtualización De Servidores	10	10	10	10	10	**10**
59	Quipux	10	10	10	10	10	**10**
60	Help Desk	10	10	8	10	10	**9,6**
61	Mail	10	10	10	10	10	**10**
62	Telefonía IP	10	10	10	10	10	**10**
63	Control De Accesos	10	10	10	10	10	**10**
64	Energía	1	10	5	10	10	**7,2**
65	Biométricos	10	10	10	10	10	**10**

ANEXO 6: PLAN DE CONTINGENCIA DE BASE DE DATOS

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PLAN DE CONTINGENCIA BASE DE DATOS DEL GADMI

VERSIÓN 1.0

JULIO, 2023

Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra	**Instructivo**	**Fecha de creación:**	2023-05-15
	Plan de Contingencia BDD	**Fecha de revisión:**	2023-07-13
Código:	**Idioma:** Castellano	**Versión:**	1.0
Elaborado por:	**Revisado por:**	**Aprobado por:**	
Fernanda Farinango **Tesista**	Ing. Gabriel Bucheli **Analista de Sistemas**		

4.4 OBJETIVO

Garantizar la continuidad del servicio de los servidores de producción de bases de datos sobre los cuáles se almacenan la información de todos los aplicativos internos y externos del Gobierno Autónomo descentralizado Municipal de San Miguel de Ibarra, con la finalidad de garantizar la disponibilidad, integridad y confidencialidad de la información institucional y salvaguardar la información alojada en la infraestructura tecnológica de hardware.

4.5 ALCANCE

El plan de contingencia para el fallo en el funcionamiento del servidor y las bases de datos, se encuentran consideradas dentro del Plan de Contingencia tecnológica y tiene como alcance la

recuperación de la continuidad de los servicios informáticos de la institución que brindan el motor de las bases de datos al igual que los servidores en los cuales están instalados, que tengan impacto en el funcionamiento de los aplicativos del GAD-IBARRA ; y que aumentan el riesgo de la disponibilidad de la información institucional alojada en los equipos de la institución.

El presente plan contiene las acciones específicas a desarrollar por parte del personal técnico de la Dirección de Tecnologías de la Información del GAD-IBARRA. Detallando cada una de las acciones a seguir en caso de caída de las bases de datos y por ende los aplicativos que en él alojadas de los servicios que presta el GAD-IBARRA.

Este instructivo aplica para todos los procesos del GAD Municipal Ibarra y cubre todos los documentos del Sistema de Gestión de Seguridad de la Información.

4.6 DEFINICIONES

Documento: Es la información detallada y registrada en algún medio de soporte.

Plan: Conjunto de acciones en el que se detalla el modo y medios necesarios para llevar a cabo un propósito.

Contingencia: Suceso que puede suceder o no, especialmente un problema que se presenta de forma imprevista.

Política: Es una declaración de alto nivel requerida por algún estándar de certificación, es el conjunto de decisiones y medidas tomadas por determinados grupos que detentan el poder, en pos de organizar una sociedad.

Procedimiento: La forma específica de llevar a cabo una actividad o un proceso.

Instructivo: Documentos que describen de la forma más precisa y específica cómo se deben realizar ciertas tareas incluidas en los procedimientos.

ITILV3: Biblioteca de Infraestructura de Tecnologías de Información.

GADMI: Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra

4.7 BASE LEGAL

- Constitución de la Republica de Ecuador Art 91
- Leyes Orgánicas (COIP Art 190, 191, 192)
- Ordenanzas Municipales.
- ISO 27001 – Sistema de seguridad de la Información.
- ITIL V3 – Catalogo Diseño del servicio.
- Normas de control interno de la contraloría general del Estado Art.410 y 411.

4.8 RESPONSABILIDADES

Dependiendo del tipo de desastre presentado, el responsable del área afectada será el encargado de autorizar la ejecución del contingente presentado en este documento.

4.9 EJECUCION / CONTENIDO

En la Tabla 1 se detalla las BDD del GAD I, se describe cada uno de sus aplicativos.

Tabla 1 Estructura de Base de Datos del GAD - IBARRA

NOMBRE	VERSION	NOMBRE DE BDD	APLICACIONES
PRODUCCION	POSTGRESQL V13	BDDIMI	SIGM, AVALUOS Y CATASTROS, ALFANUMERICA Y GRAFICA, PORTAL CIUDADANO
		BDDI BIN	FOTOS (AVALUOS Y CATASTROS HISTORICO)
		MOODLE	CURSOS
QUIPUX	POSTGRESQL V13	GXIBARRA	SISTEMA QUIPUX
		FIRMA DIGITAL	FIRMA DIGITAL
ACTIVITY	POSTGRESQL V13	FOTOS (CATASTROS)	FOTOS AVALUOS Y CATASTROS ACTUAL
		ACTIVITY	TAREAS O PROCESOS DE AVALUOS Y CATASTROS
ODOO	POSTGRESQL V9.6	IMI	SISTEMA ODOO
REPLICA SRI	ORACLE	BDD SRI	INFORMACION SRI

4.9.1 BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN ITIL V3.

ITIL es una guía que se encarga de fomentar buenas prácticas dentro de la gestión de servicios TI, la cual propone organizar los procesos TI y ser una guía para los profesionales del área para que realicen sus tareas de manera más eficiente. ITIL abarca tres áreas como son: Infraestructura del área, el mantenimiento y operación de los servicios TI.

Su objetivo principal es garantizar una gestión adecuada de los procesos, asi como también la experiencia de los clientes al hacer uso de un servicio TI. Este marco de trabajo esta ligado a la satisfacción del cliente.

ITIL trabaja mediante procesos, en la versión 3, son 5 procesos que plantea esta normativa, los cuales se describen a continuación:

- Estrategia del servicio
- Diseño del servicio.
- Transición del servicio.
- Operación del servicio.
- Mejora continua del servicio.

Siendo el Catálogo del diseño del servicio el cual se enfoca este trabajo, ya que es la que se encarga de dar continuidad al negocio, en este caso de los servicios TI. Es una de los procesos más importantes ya que se encarga de identificar posibles fallos, determinar maneras de corregirlos y mejorar el servicio.

4.9.2 GESTIÓN DE LA CONTINUIDAD DEL SERVICIO TI.

La gestión de la continuidad del servicio TI, es una clave esencial de la prestación de servicios que plantea ITIL, esta gestión se centra principalmente en la planificación de la prevención, predicción y gestión de incidentes, con el principal objetivo de mantener operativos los servicios TI en los niveles más altos, antes, durante y después de ocurrido el incidente.

Su objetivo es reducir el tiempo de inactividad, costes y el impacto empresarial que tendría en caso que un incidente llegase a materializarse, mediante procesos eficaces y estandarizados que deben aplicarse cuando suceden accidentes inevitables.

La gestión de la continuidad empresarial (BCM) abarca ITSCM y otros procesos de mitigación de riesgos. Por lo que los equipos de TI deben colaborar para crear lo siguiente:

- **Un plan de continuidad empresarial (BCP):** En este se incluyen planes para la prevención y recuperación de incidentes TI a nivel de desastre.
- **Análisis de Impacto empresarial (BIA):** Identifican el posible impacto de un desastre TI en el negocio.

Por consiguiente, se muestra el proceso a seguir dentro de un plan de continuidad empresarial (BCP). La cual consta de 4 fases que se describen a continuación:

- **Fase 1:** Se toma en cuenta el alcance y las políticas de ITSCM.
- **Fase 2**: Indica los procesos que se debe seguir como es el análisis del impacto del negocio, identificación y análisis de activos, evaluación de riesgos, estrategia de continuidad. Revisar los Anexos 2 y3.
- **Fase 3**: Indica el despliegue de la estrategia, desarrollo de procedimientos de continuidad y la puesta en marcha de la estrategia. (Revisar plan de acción)
- **Fase 4**: Mejora continua del servicio. (Recomendaciones)

4.9.3 PLAN DE CONTINGENCIA

Un plan de contingencia es un proceso que se encarga de dar continuidad a los procesos en el caso que se presenten riesgos que puedan afectarlos, organizando a las personas responsables de cada área, actividades que ayuden a mitigar o evitar el impacto. Esta información será documentada en un texto totalmente claro y entendible con las medidas y normas a seguir de forma estratégica para su implementación. El objetivo principal de un plan de contingencia es mejorar la capacidad de respuesta frente a diversos eventos que afecten el buen funcionamiento del sistema. A más de ello el plan de contingencia pretende ayudar a las organizaciones empleando los recursos disponibles para poder enfrentar el escenario de riesgo.

4.9.4 OBJETIVO DE UN PLAN DE CONTINGENCIA

Según la NTE INEN-ISO /IEC 27002 y el registro oficial Nro. 039 GG, (2009) menciona que un plan de contingencia informático debe contar con los siguientes objetivos:

- Debe mantener a la medida de lo posible la continuidad de los servicios proporcionados por la organización denominados críticos en un nivel aceptable en caso de un plan de contingencia.

- Establecer acciones y procesos que permitan mantener la operatividad de los sistemas de información en caso de una emergencia.

4.9.5 IMPORTANCIA DE UN PLAN DE CONTINGENCIA

- Garantizar la seguridad física, la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos.
- Permitir realizar un conjunto de acciones con el fin de evitar el fallo, o en su caso, disminuir las consecuencias que en él se puedan derivar.
- Permite realizar un análisis de riesgos por servicio, respaldo de los datos y su posterior Recuperación de los datos. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal funcionamiento de una Institución. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la institución.

4.9.6 CICLO DE PLAN DE CONTINGENCIA

- **Identificar los riesgos potenciales:** el primer paso es identificar los posibles riesgos que pueden afectar la disponibilidad del servicio de base de datos. Esto puede incluir fallas de hardware, errores de software, ataques cibernéticos, desastres naturales, errores humanos, entre otros.
- **Crear un plan de respaldo**: es importante tener una copia de seguridad actualizada de la base de datos en un lugar seguro y fuera del sitio, preferiblemente en una ubicación geográfica diferente a la principal. El plan de respaldo debe incluir detalles sobre cómo se realiza el respaldo, con qué frecuencia se realiza y cómo se verifica su integridad.

- **Establecer procedimientos de recuperación**: en caso de una falla o interrupción, es necesario contar con procedimientos claros de recuperación. Esto debe incluir instrucciones sobre cómo restaurar la base de datos desde una copia de seguridad, cómo verificar la integridad de los datos y cómo garantizar la continuidad del servicio.
- **Definir roles y responsabilidades:** es importante asignar roles y responsabilidades claras a las personas encargadas de ejecutar el plan de contingencia. Esto debe incluir un equipo de respuesta de emergencia que tenga la capacidad de responder rápidamente y tomar medidas para minimizar el impacto de una falla.
- **Realizar pruebas periódicas:** es importante realizar pruebas periódicas del plan de contingencia para asegurarse de que esté actualizado y sea efectivo. Las pruebas deben incluir simulaciones de situaciones de emergencia para evaluar la capacidad del plan de contingencia para responder y recuperar el servicio de base de datos.
- **Comunicar el plan:** finalmente, es importante comunicar el plan de contingencia a todos los miembros del equipo y partes interesadas relevantes. Esto debe incluir información sobre los riesgos potenciales, los procedimientos de respaldo y recuperación, los roles y responsabilidades, y las pruebas periódicas del plan.

4.9.7 IDENTIFICACION DE RIESGOS

Dentro del GADMI existen 5 BDD principales, las cuales se dividen para cada una de las aplicaciones habilitadas dentro de la institución. El administrador de base de datos de la institución es el responsable de identificar posibles daños físicos o lógicos que puedan

interrumpir su buen funcionamiento. Una vez identificado el daño la persona responsable levantará el servicio dependiendo del tipo de afectación, para lo cual nos referimos al plan de acción. Ver en el Anexo 4 los posibles riesgos que pueden presentarse dentro de la Dirección de Tecnologías de la Información

4.9.8 CREACION DE PLAN DE RESPALDOS

La Dirección de Tecnologías de la Información trabaja en base a las Políticas de seguridad detalladas en el documento denominado ***Memoria Técnica - Marzo 2023 - GAD IBARRA v2.***

4.9.9 PROCEDIMIENTOS DE RECUPERACIÓN

Dentro del procedimiento de recuperación, se detalla el plan de acción que el responsable asignado de cada servicio deberá seguir en el caso de presentarse algún tipo de afectación en el servicio.

4.9.10 PLAN DE ACCION

A continuación, se muestra un plan de acción a seguir, cuando ocurra algún inconveniente en el buen funcionamiento de las BDD y se deba implementar un contingente para que las aplicaciones en él alojadas sigan en funcionando. En la Tabla 2 se muestra los pasos a seguir.

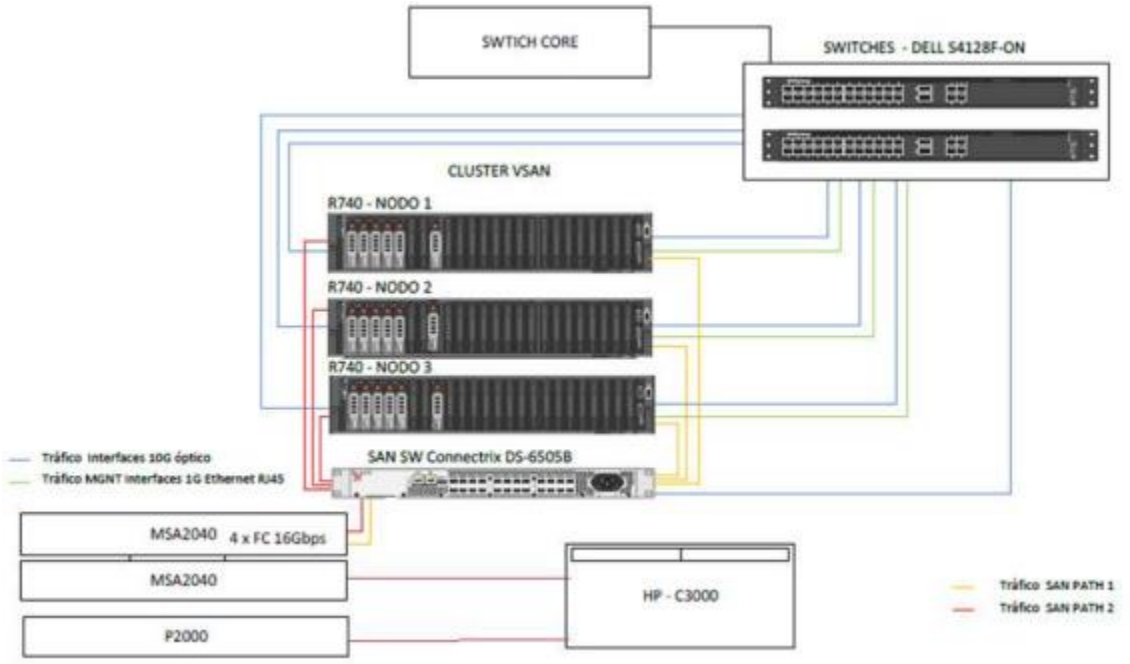
Para poder determinar el tiempo de recuperación del servicio, se ha tomado en cuenta dos conceptos el Objetivo de punto de recuperación (RPO), que es el punto en el que la copia de seguridad va a restaurar los datos. Por ejemplo, si se tiene un respaldo de hace una semana, el RPO será de hace una semana o 168 horas. Y el tiempo objetivo de recuperación (RTO), es el tiempo que el servicio estará fuera de funcionamiento. Por ejemplo: si se tarda cargar el backup 2 horas el RTO será de 2 horas.

Para conocer el RPO de las copias de seguridad, ver el documento denominado ***Memoria Técnica - Marzo 2023 - GAD IBARRA v2.***

El RTO se ha obtenido mediante entrevistas al personal encargado de la restauración de las BDD del GAD-Ibarra.

Cabe mencionar que el presente plan de acción esta desarrollado en el caso que el servicio de Base de Datos deje de funcionar en su totalidad. Es necesario detallar que este caso es poco probable, ya que la municipalidad cuenta con Hiperconvergencia en sus servicios TI, haciendo uso de servidores alternos que sirven para reemplazar al principal automáticamente en el caso que éste tenga una caída. En la Figura 1 se detalla la estructura física y lógica de cómo se encuentra conectados los equipos para poner en marcha la Hiperconvergencia formar la Como se muestra en la Figura 1.

Figura 1 Estructura física de conexión de los equipos de Hiperconvergencia.



Nota: Estructura física de conexión de equipos de Hiperconvergencia para servicios TI implementada por la Dirección de TIC´s del GA-Ibarra.

Tabla 2

ITEM	ACTIVIDAD	DAÑO	DESCRIPCION DEL INCONVENIENTE	REQUERIMIENTO	INSTRUCTIVO	PLAN DE ACCION	RESPONSABLE	TIEMPO ESTIMADO
	Realizar el diagnóstico del problema reportado	Físico	Equipo apagado	Energía eléctrica	Revisar fuente de energía. Revisar cableado de la fuente de poder. Encender equipo. Revisar el servicio este activo.	Instructivo x Sección	Ing. Gabriel Bucheli	5 min
			Equipo quemado	Reporte al responsable de hardware, para cambio de equipo.	Remplazar equipo Hardware prepara equipo. Instalación y configuración de servicio de BDD Restaurar o recuperación de BDD.	Instructivo x Sección	Ing. Gabriel Bucheli	10 min
			Fallas del hardware del servidor (procesador, discos de memoria, RAM, placa base hardware de red, etc.)	Reporte al responsable de hardware, para cambio o reparación del elemento afectado.	Remplazar equipo Hardware prepara equipo. Instalación y configuración de servicio de BDD Restaurar o recuperación de BDD	Instructivo x Sección	Ing. Gabriel Bucheli	10 min
		Lógico	Daño del Sistema Operativo	Imagen ISO	Instalación del sistema operativo, configuración de accesos, instalación del motor de base de datos.	Instructivo x Sección	Ing. Gabriel Bucheli	40 min
			Servicio de BDD Inactivo	Comandos para levantar el servicio.	Levantar el servicio.	Instructivo x Sección	Ing. Manuel Lara	2 min
			Fallas en la red de datos.	Software de monitoreo de la red.	Escaneo de la red, identificación de problemas	Instructivo x Sección	Ing. Gabriel Bucheli	5 min
			Daño en el motor de base de datos o falla en el sistema operativo.	Respaldo de BDD	Se elige el archivo ISO de copia de respaldo más reciente.	Instructivo x Sección	Ing. Manuel Lara	10 min

			Saturación en espacio de disco		Eliminar los archivos temporales o logs de fechas de anteriores	Instructivo x Sección	Ing. Manuel Lara	3 min
			Servidor de réplica se promueva a ser Master		Reportar la falla a la empresa contratada.	Instructivo x Sección	Ing. Manuel Lara	20 min
			Procesos con tiempo de respuesta elevados y con tiempos de espera altos.		Revisar y mejorar los procesos de BDD Eliminar los procesos que no se han ejecutados	Instructivo x Sección	Ing. Manuel Lara	15 min

4.9.11 PRUEBAS DE FUNCIONAMIENTO

Una vez que se ha identificado la falla de total o parcial de una base de datos, el administrador procederá a realizar una auditoria para determinar la causa del inconveniente determinando el tipo de amenaza materializada.

Como primer paso se determina la alerta emitida por el software de monitoreo implementado en el GAD-Ibarra, una vez identificado el daño se procede a seguir el instructivo planteado según el Plan de Contingencia dependiendo del tipo de inconveniente, en este caso se tomará como referencia los fallos más comunes que se pueden presentar. La demostración de las pruebas del Plan de Contingencia se la realizan mediante un Check List en el cual se detalla los daños físicos y lógicos y si éstos fueron solventados o no. Cabe mencionar que el análisis de daños tanto físicos como lógicos están enfocados únicamente al servicio de Base de Datos. como se muestra a continuación:

Check List Plan de Contingencia Base de Datos del GAD - IBARRA

El presente documento detalla un Check List de las pruebas realizadas en la Dirección de Tecnologías de la Información, aplicado al Plan de Contingencia de las Bases de Datos que cuenta el GAD - Ibarra. La demostración de los resultados se dividirá en dos partes, Daños Físicos y Daños Lógicos, como se muestra a continuación:

1. **Daños Físicos**

Dentro de los daños físicos la Dirección de Tecnologías de la Información debe tener equipos de respaldo, para poder solventar los daños físicos descritos en el Plan de Contingencia.

Tabla 100 Equipos de Respaldo de manejados por TICs.

EQUIPOS	RESPALDO	
	SI	NO
Generador Electrico	☑	☐
UPS	☑	☐
Inversores	☑	☐
Baterias	☑	☐
Reguladores de voltaje	☑	☐
Regletas	☑	☐
Cable Eléctrico	☑	☐
Toma Corriente	☑	☐
Servidores	☑	☐
CPU	☑	☐
Discos de memoria	☑	☐
Extintores	☑	☐
Sensores de Humo	☑	☐
Cable Fibra Óptica	☑	☐
Cable UTP Cat6a	☑	☐

Check List de las Pruebas de Funcionamiento del Plan de Contingencia.

Las pruebas de funcionamiento se realizaron en conjunto con las personas responsables de la administración y gestión de las Bases de Datos. Por motivos de seguridad de la información se optó por la demostración de las pruebas de funcionamiento del Documento denominado Plan de Contingencia de servicio de Base de Datos, por la creación de un check list, en el cual se muestra los daños ocasionados al servicio dependiendo del tipo y si éste fue solventado o no. Como se muestra en la tabla 2 y 4.

Tabla 101 Check List de Pruebas de Funcionamiento Daños Físicos.

TIPO DE DAÑO	DESCRIPCION	EVENTO SOLVENTADO		RESPONSABLE	TIEMPO ESTIMADO	TIEMPO DURADO
		SI	NO			
Físico	Equipo quemado, se revisa y se determina que el equipo esta quemado por descargas de energía. Reemplazo del equipo.	☑		Ing. Gabriel Bucheli	15 min	12 min
Físico	Equipo apagado, se revisa conexiones eléctricas, se mide niveles de voltaje.	☑		Ing. Gabriel Bucheli	10 min	7 min
Físico	Fallos de hardware de servidor. Disco de memoria saturado	☑		Ing. Gabriel Bucheli	12 min	10 min

2. Daños Lógicos

Dentro de los daños lógicos, la Dirección de Tecnologías de la Información cuenta con políticas de seguridad de la información, las cuales establecen normas para resguardar la información de la Municipalidad y por ende de los servicios que esta ofrece y con ello dar una continuidad a la prestación de servicios. Para ello se ha realizado un check list de las herramientas esenciales que la Dirección de TIC´S necesita cumplir con lo antes descrito. Como se muestra en la Tabla 3 que se presenta a continuación:

Tabla 102 Herramientas de respaldo para solventar Daños Lógicos.

HERRAMIENTAS	RESPALDO		OBSERVACIONES
	SI	NO	
Respaldo de BDD de Producción	☑		
Respaldo de BDD Quipux	☑		
Respaldo de BDD Activity	☑		
Respaldo de BDD ODOO	☑		
Respaldo de BDD Replica de SRI.	☑		
Sistemas Operativos	☑		
Imágenes ISO	☑		
Respaldo proveedor Internet	☑		
Respaldo de Soporte Técnico	☑		

Pruebas de Funcionamiento

En la Tabla 4 se detalla un check List de las pruebas de funcionamiento simuladas en la parte lógica del servicio de Base de Datos.

Pruebas de Funcionamiento

Tabla 103 Check List de Pruebas de Funcionamiento Daños Lógicos.

TIPO DE DAÑO	DESCRIPCIÓN	SOLVENTADO		RESPONSABLE	TIEMPO ESTIMADO	TIEMPO DURADO
		SI	NO			
Lógico	Daño del Sistema Operativo	☑		Ing. Gabriel Bucheli	5 min	7 min
Lógico	Servicio de BDD Inactivo. Ingreso de comando para levantar el servicio.	☑		Ing. Manuel Lara	2 min	2 min
Lógico	Fallas en la red de datos. Reemplazo de Patch Cord.	☑		Ing. Gabriel Bucheli	5 min	4 min
Lógico	Daño en el motor de base de datos. Se elige el archivo ISO de copia de respaldo más reciente.	☑		Ing. Manuel Lara	10 min	13 min
Lógico	Saturación en espacio de disco	☑		Ing. Manuel Lara	5 min	6 min
Lógico	Procesos con tiempo de respuesta elevados y con tiempos de espera altos	☑		Ing. Manuel Lara	15 min	13 min

4.9.12 INFORME DE IMPLEMENTACION DEL PLAN DE CONTINGENCIA

A continuación, se especifica el contenido que debe tener el Informe una vez aplicado el contingente en el Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra.

- **Portada**: En ella se incluye el titulo y nombre de la Institución involucrada.
- **Índice**: Orden de los temas o partes de las páginas.
- **Introducción:** Establece un foco o idea central del inconveniente presentado. También indica la dirección e ideas principales que cubrirán dicho inconveniente. En ella generalmente se detallan hipótesis y objetivos.
- **Materiales y métodos**: Objetos utilizados. Se incluye el nombre del material o dispositivo y se describe el uso que se le dio, además se escriben las formas o métodos que se usaron para tener resultados.
- **Contenido:** En esta parte dar a conocer los resultados obtenidos, Estos son el fruto de los objetivos planteados en la Introducción. Se incluyen tablas o gráficos con los datos y una breve descripción.
- **Conclusiones:** Se incluyen los resultados más importantes que permitan responder las interrogantes planteadas en la introducción y que están de acuerdo con los objetivos planteados.
- **Bibliografía:** Ordenamiento alfabético y por fechas de la literatura ocupada para responder las inquietudes presentadas a lo largo de trabajo.

4.9.13 CONCLUSIONES

- La realización de copias de seguridad regulares de la base de datos es crucial para asegurarse de que se puedan restaurar los datos en caso de pérdida, daño o corrupción. Es importante asegurarse de que las copias de seguridad se almacenen en un lugar seguro y protegido.
- Un plan de recuperación de desastres detallado y específico debe estar disponible para todos los miembros del equipo de seguridad de la base de datos. El plan debe incluir procedimientos para la recuperación de datos en caso de pérdida, así como una lista de los recursos necesarios para llevar a cabo la recuperación.
- Las pruebas y simulaciones regulares del plan de contingencia de la base de datos pueden ayudar a identificar y abordar posibles brechas o problemas en el plan antes de que ocurra un desastre real. Las pruebas también pueden ayudar a mejorar la eficacia del plan y asegurarse de que los procedimientos estén en su lugar para abordar cualquier problema de seguridad.
- Un equipo de respuesta a incidentes bien entrenado puede ayudar a minimizar el impacto de cualquier pérdida de datos y acelerar la recuperación de la base de datos. Es importante que el equipo esté compuesto por miembros con habilidades y experiencia relevantes, y que se realicen simulaciones y ejercicios regulares para mantener sus habilidades actualizadas.

4.10 REFERENCIAS

Resumen de Referencias

Nombre	**Formato (Físico/Electrónico)**
GERI-DI-PR-001 Plan de contingencia BDD	Electrónico/Físico

4.11 ANEXOS

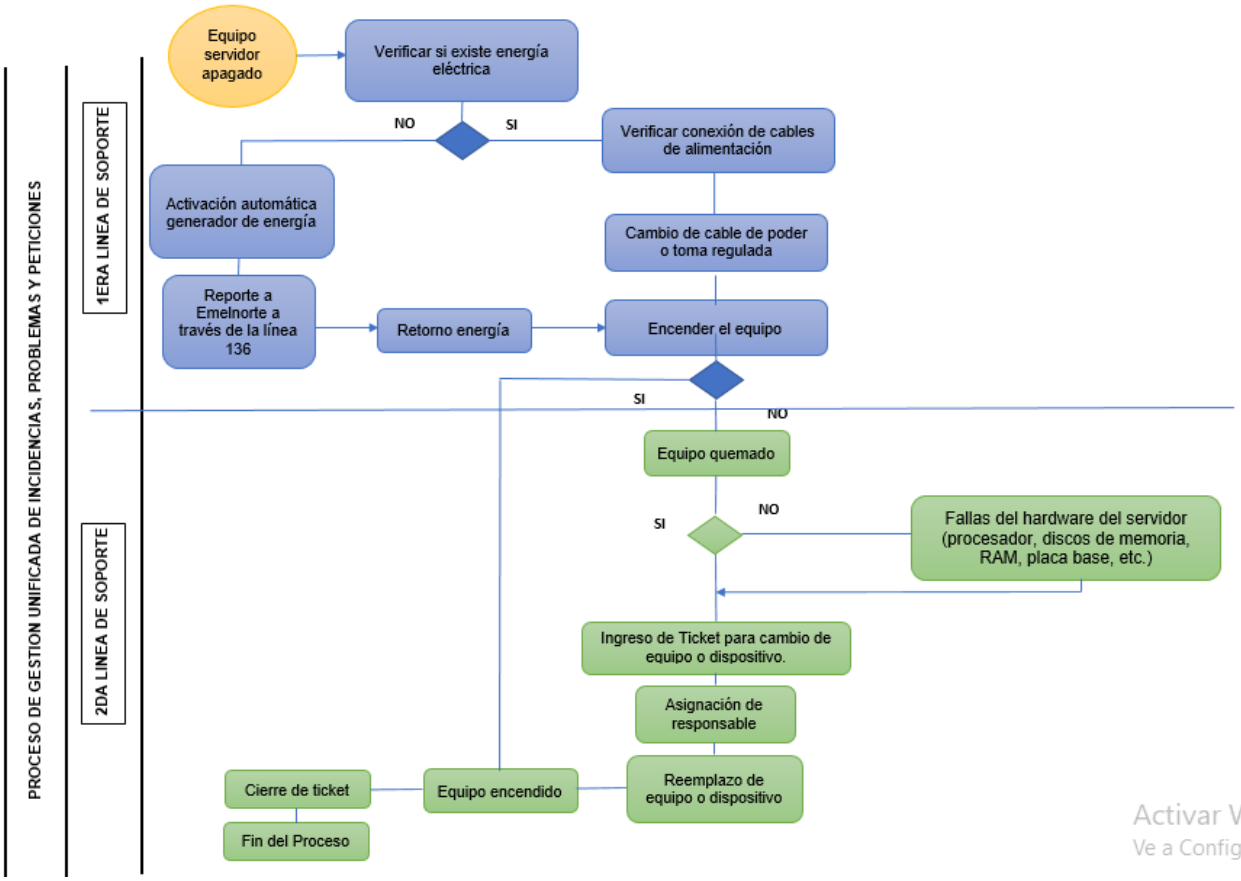
Resumen de Anexos			
Código	**Nombre del Formato**	**Formato (Físico/ Electrónico)**	**Ubicación**
TIC-XX-RE-001	Plan de Contingencia BDD	Electrónico/Físico	Oficina / Cloud

ANEXO 1 Asignación de personal designado para dar solución al inconveniente presentado dependiendo del tipo de Fallo.

SERVICIOS	SUBSERVICIOS	CÓDIGO	PROPIETARIO/OPERADOR	BACKUP	CÓDIGO
RED	MAN	SRV-RED-MAN	gbucheli	etaez	SRV-RED
	WAN (ENLACES EXTERNOS)	SRV-RED-WAN	gbucheli	etaez	
	LAN	SRV-RED-LAN	mtobar	gbucheli	
	WLAN	SRV-RED-WLAN	gbucheli	etaez	
	CONECTATE IBARRA	SERV-RED-CI	etaez	gbucheli	
	INTERNET	SRV-RED-INTERNET	gbucheli	etaez	
SEGURIDAD	SEGURIDAD PERIMETRAL	SRV-SEG-PER	gbucheli	etaez	SRV-SEG
	VIDEO SEGURIDAD	SRV-DC-CCTVV	etaez	mtobar	
	ANTIVIRUS/ANTISPAM	SRV-SEG-AV	mtobar	etaez	
INFRAESTRUCTURA	HOSTING DE SERVIDORES	SRV-INF-HS	gbucheli	mtobar	SRV-INF
	VIRTUALIZACIÓN DE SERVIDORES	SRV-INF-KVM	gbucheli	mtobar	
WEB	QUIPUX	SRV-WEB-QUIPUX	etaez	etaez	SRV-WEB
	HELP DESK	SERV-WEB-OTRS	vdavila	etaez	SRV-OTRS
DATACENTER	CONTROL DE ACCESOS	SRV-DC-CCAA	mtobar	etaez	SRV-DC
	INCENDIOS	SRV-DC-FIRE	mtobar	vdavila	
	VENTILACIÓN Y AIRE ACONDICIONADO	SRV-DC-HVAC	mtobar	vdavila	
	ENERGIA	SRV-DC-POWER	mtobar	vdavila	
REGISTRO Y CONTROL	BIOMETRICOS	SRV-RYC-BIOM	mtobar	etaez	SRV-RYC
SOPORTE	EQUIPOS	SRV-SOP-EQP	vdavila	etaez	SRV-SOPORTE
	IMPRESORAS	SRV-SOP-IMP	vdavila	etaez	

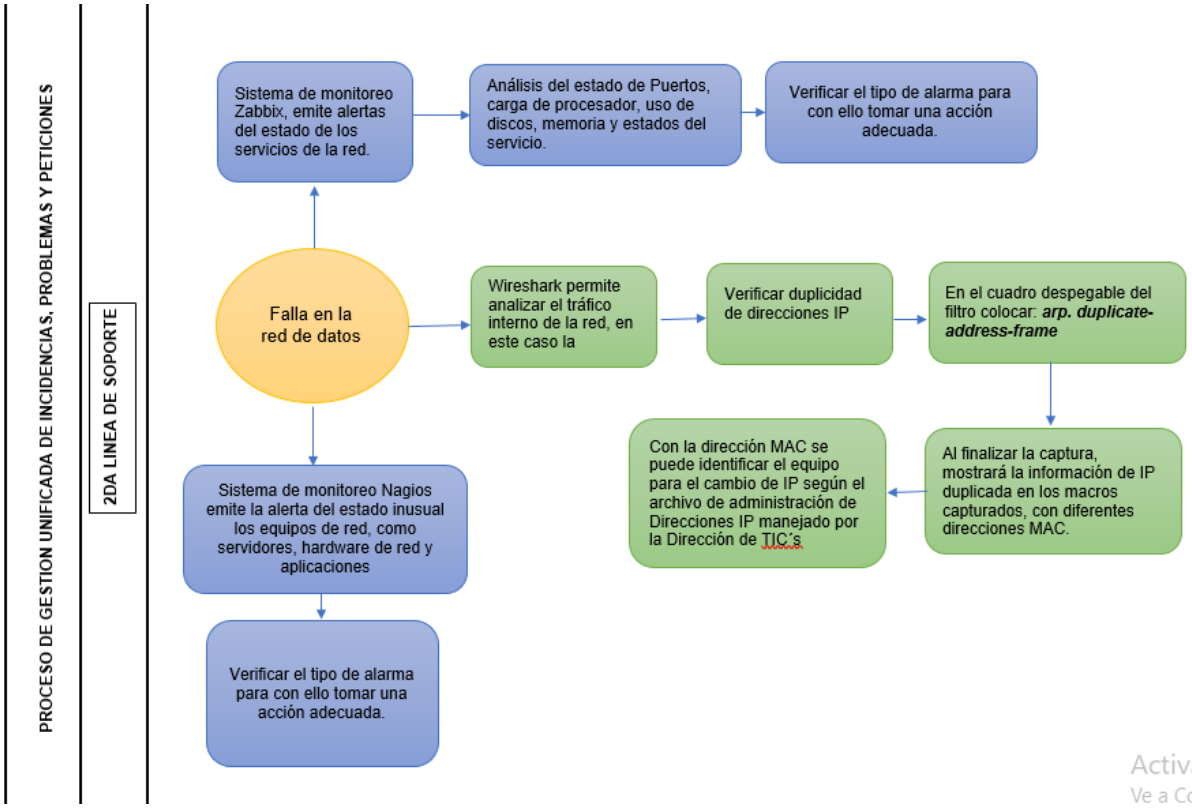
ANEXO 2 Diagramas de Flujo de procesos de las pruebas de funcionamiento del Plan de Contingencia.

Figura 8 *Diagrama de Flujo de procesos de Fallos Físicos del servicio de Base de Datos.*



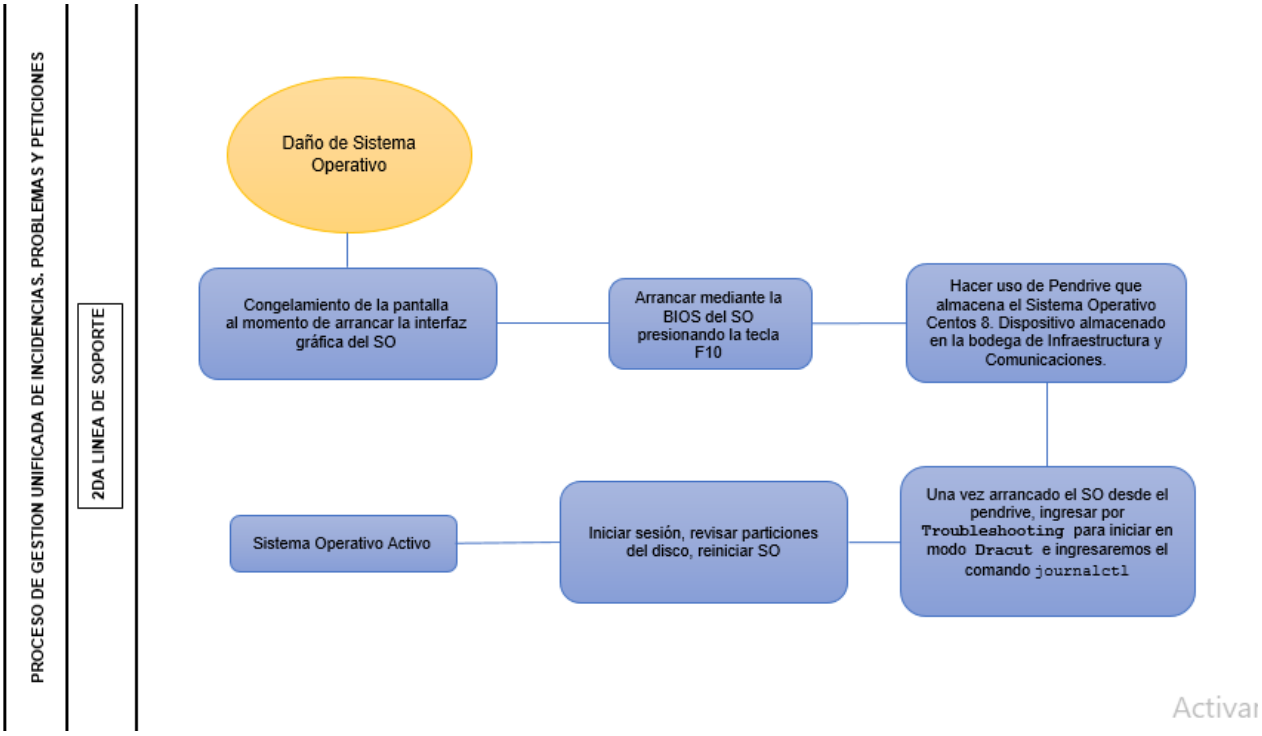
Nota: El presente diagrama se muestra el proceso a seguir en caso de una falla física del equipo que afecte el buen funcionamiento del sistema. Cada uno de los procesos tiene una línea de soporte responsable, la cual se encargará de tomas las acciones necesarias para levantar el equipo y por ende el servicio. Cabe mencionar que para el cambio de equipos la Dirección de Tecnologías de la Información cuenta con un manual de procedimientos ya que, al momento de cambio de un equipo o dispositivo, éste se vuelve un activo que debe pasar a la bodega de la persona responsable de Hardware, justificando el reemplazo del mismo.

Figura 9 Fallo en la red de Datos del servicio de Bases de Datos.



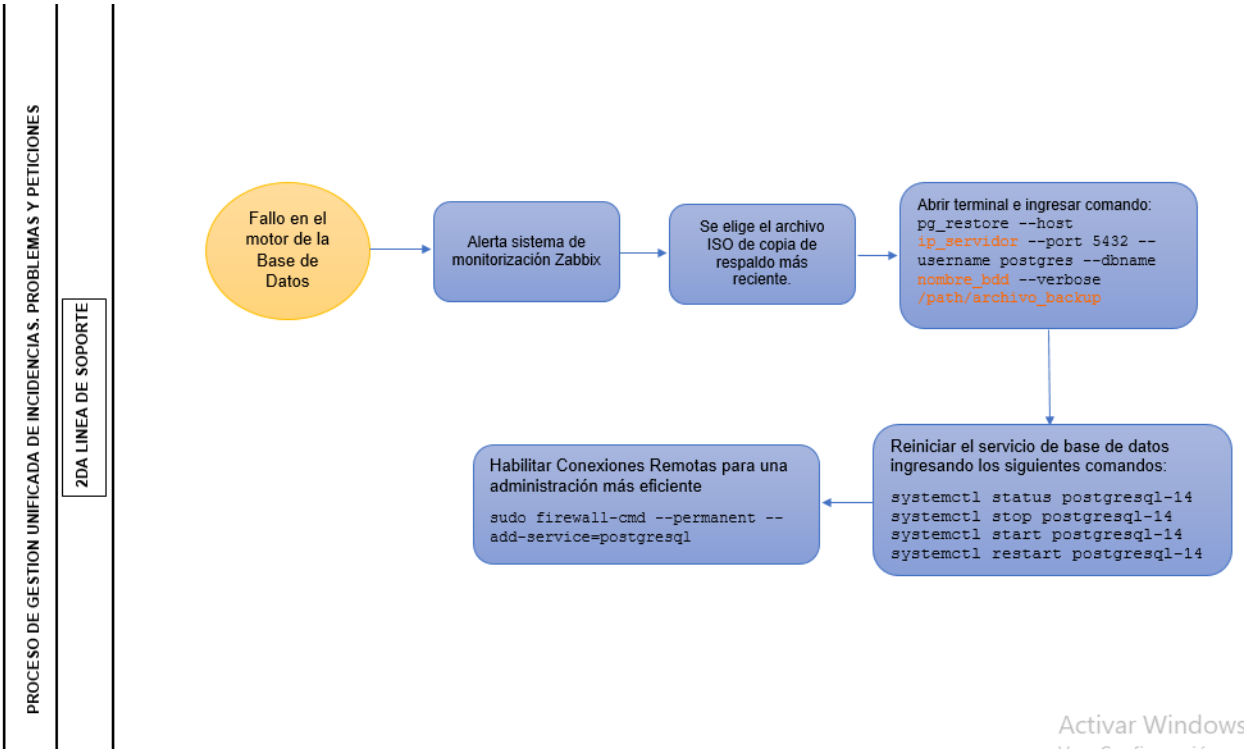
Nota: Dentro de los fallos lógicos que pueden ocurrir en la red de datos se tiene como principal a la duplicidad de direcciones IP, por ello la Dirección de TIC´s del GAD-Ibarra ha implementado la herramienta Wireshark, la cual permite filtrar mediante comandos las direcciones IP asignadas a un equipo con sus respectivas direcciones MAC´s. Adicional, la dirección cuenta también con sistemas de monitoreo como son Zabbix y Nagios, los cuales permiten tener un control de toda la infraestructura de la municipalidad.

Figura 10 Diagrama de Flujo de procesos en caso de Falla del Sistema Operativo Centos 8.



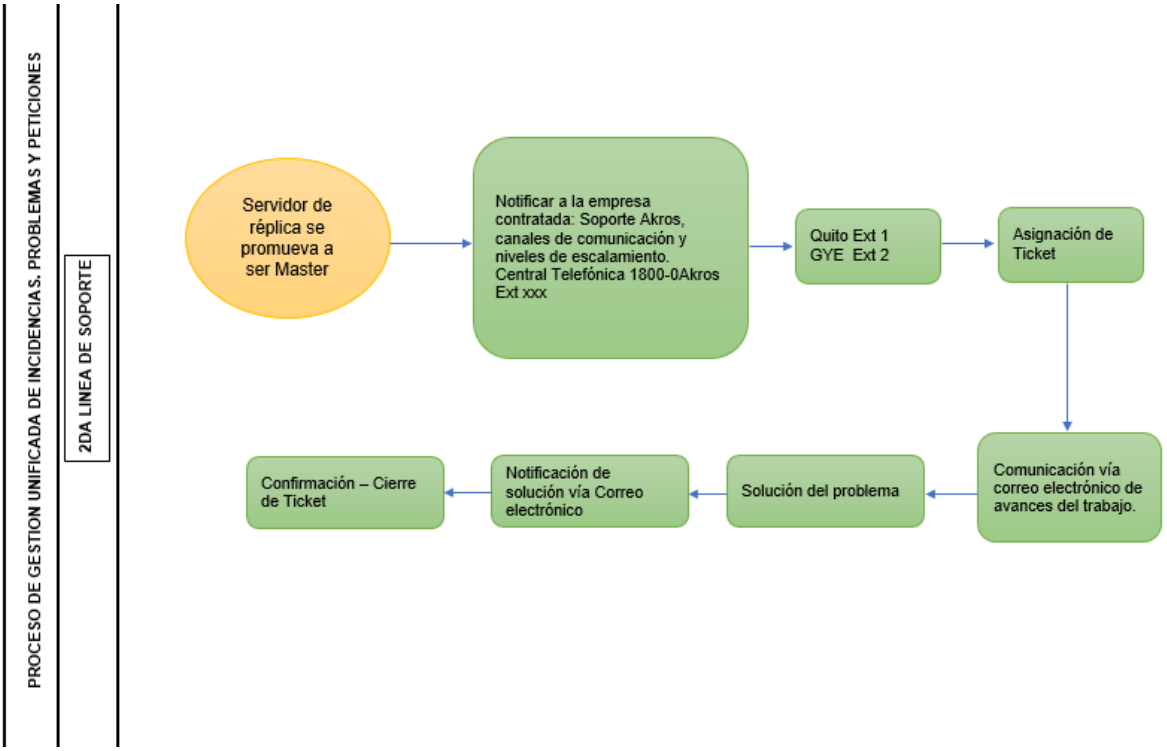
Nota: El presente diagrama se muestra el proceso a seguir en caso de una falla en el sistema operativo Centos 8.

Figura 11 Fallo en el Motor de la Base de Datos



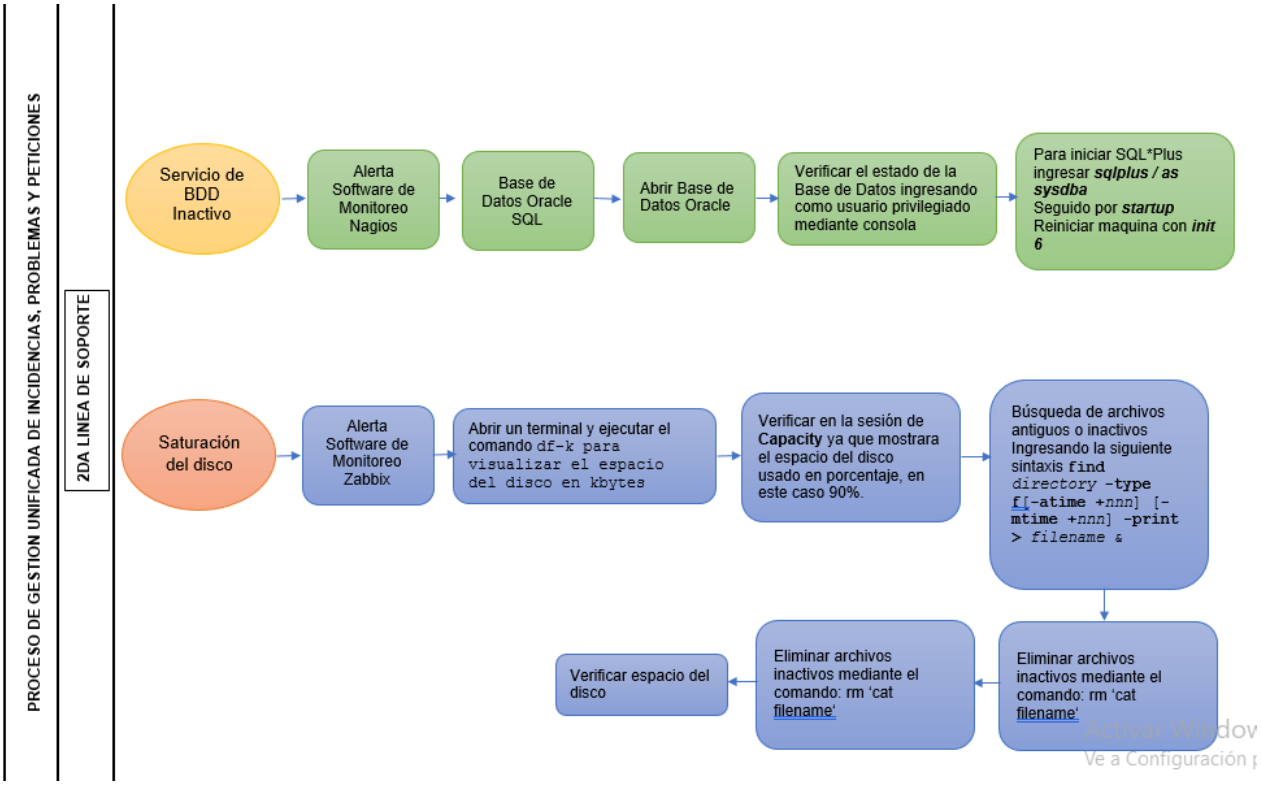
Nota: Proceso a seguir en caso del fallo en el motor de la Bases de Datos. Dependiendo del tipo de base de datos Oracle o POSTGRESQL

Figura 12 Diagrama de flujo de procesos, en caso de Fallo de servidor de Base de Datos Réplica se promueva a Master



Nota: La Dirección de TIC´s del GAD-Ibarra contrajo un contrato con la empresa Akros, la cual es la encargada de los respaldos de la red, al igual que el mantenimiento y funcionamiento de la Hiperconvergencia de los datos, entre otros.

Figura 13 Diagrama de Flujo de procesos en caso de Inactividad de las BDD o Saturación del disco.



Nota: El presente diagrama se muestra el proceso a seguir en caso de una falla en el Servicio de BDD Inactivo, saturación del disco e Inyección de código malicioso. Fallos que serán emitidos a través de un sistema de monitorización constante a la red de datos.

4.12 CONTROL DE CAMBIOS

Resumen de Modificaciones con relación a la versión anterior:			
Nro. Versión	**Fecha Rev.**	**Descripción de modificación**	**Aprobado por:**
1.0	10-03-2023		

ANEXO 7: PLAN DE CONTINGENCIA SIGM

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PLAN DE CONTINGENCIA DE SIGM DEL GADMI

VERSIÓN 1.0

JULIO, 2023

Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra	**Instructivo**	**Fecha de creación:**	2023-05-15
	Plan de Contingencia SIGM	**Fecha de revisión:**	2023-07-13
Código:	**Idioma:** Castellano	**Versión:**	1.0
Elaborado por:	**Revisado por:**	**Aprobado por:**	
Fernanda Farinango **Tesista**	Ing. Gabriel Bucheli **Analista de Sistemas**		

4.13 OBJETIVO

Garantizar la continuidad del servicio del Sistema Integrado de Gestión del Gobierno Autónomo descentralizado Municipal de San Miguel de Ibarra, con la finalidad de garantizar la disponibilidad, integridad y confidencialidad de la información institucional hacia los usuarios de la institución.

4.14 ALCANCE

El plan de contingencia del Sistema integrado de gestión del GAD Municipal de Ibarra está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA, tiene como alcance la recuperación de la normalidad de la plataforma del Sistema integrado de gestión Municipal SIGM.

El presente plan contiene las acciones específicas a desarrollar por parte del personal técnico de la Dirección de Tecnologías de la Información del GAD-IBARRA.

El servicio del Sistema Integrado de Gestión del Municipio de Ibarra, de forma general contiene los siguientes módulos principales:

a) CORE Empresarial
b) Módulo de administración del ciudadano.
c) Módulo de recaudación.
d) Módulo de coactivas.
e) Módulo de emisión de impuestos, tasas y contribuciones.
f) Módulo de Gestión de Trámites
g) Módulo de transferencias de dominio.
h) Sistema de la Unidad Educativa Municipal
i) Módulo de SISMERT
j) Módulo de Participación Ciudadana.
k) Declaraciones de Impuestos y fiscalización.
l) Módulo de actividades económicas.
m) Otros

4.15 DEFINICIONES

Documento: Es la información detallada y registrada en algún medio de soporte.

Plan: Conjunto de acciones en el que se detalla el modo y medios necesarios para llevar a cabo un propósito.

Contingencia: Suceso que puede suceder o no, especialmente un problema que se presenta de forma imprevista.

Política: Es una declaración de alto nivel requerida por algún estándar de certificación, es el conjunto de decisiones y medidas tomadas por determinados grupos que detentan el poder, en pos de organizar una sociedad.

Procedimiento: La forma específica de llevar a cabo una actividad o un proceso.

Instructivos: Son documentos que describen de la forma más precisa y específica cómo se deben realizar ciertas tareas incluidas en los procedimientos.

ITILV3: Biblioteca de Infraestructura de Tecnologías de Información.

GADMI: Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra.

SIGM: Sistema Integrado de Gestión Municipal.

4.16 BASE LEGAL

- Constitución de la Republica de Ecuador Art 91
- Leyes Orgánicas (COIP Art 190, 191, 192)
- Ordenanzas Municipales.
- ISO 27001 – Sistema de seguridad de la Información.
- ITIL V3 – Catalogo Diseño del servicio.
- Normas de control interno de la contraloría general del Estado Art.410 y 411.

4.17 EJECUCION / CONTENIDO

Cada módulo del Sistema Integrado de Gestión requiere de una base de datos para almacenar la información correspondiente, por lo cual en la Tabla 1 se citan las bases de datos que intervienen en el funcionamiento:

Tabla 1: Base de datos

N°.	ACTIVO - DATOS
1	Base de datos IMI
2	Sistema réplica de base de datos Oracle del servicio de rentas internas

4.17.1 BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN ITIL V3.

ITIL es una guía que se encarga de fomentar buenas prácticas dentro de la gestión de servicios TI, la cual propone organizar los procesos TI y ser una guía para los profesionales del área para que realicen sus tareas de manera más eficiente. ITIL abarca tres áreas como son: Infraestructura del área, el mantenimiento y operación de los servicios TI.

Su objetivo principal es garantizar una gestión adecuada de los procesos, así como también la experiencia de los clientes al hacer uso de un servicio TI. Este marco de trabajo está ligado a la satisfacción del cliente.

ITIL trabaja mediante procesos, en la versión 3, son 5 procesos que plantea esta normativa, los cuales se describen a continuación:

- Estrategia del servicio
- Diseño del servicio.
- Transición del servicio.

- Operación del servicio.
- Mejora continua del servicio.

Siendo este último en el cual se enfoca este trabajo, ya que es la que se encarga de monitorear y revisar el buen funcionamiento de los servicios TI. Es uno de los procesos más importantes ya que se encarga de identificar posibles fallos, determinar maneras de corregirlos y mejorar el servicio.

4.17.2 GESTIÓN DE LA CONTINUIDAD DEL SERVICIO TI.

La gestión de la continuidad del servicio TI, es una clave esencial de la prestación de servicios que plantea ITIL, esta gestión se centra principalmente en la planificación de la prevención, predicción y gestión de incidentes, con el principal objetivo de mantener operativos los servicios TI en los niveles más altos, antes, durante y después de ocurrido el incidente.

Su objetivo es reducir el tiempo de inactividad, costes y el impacto empresarial que tendría en caso que un incidente llegase a materializarse, mediante procesos eficaces y estandarizados que deben aplicarse cuando suceden accidentes inevitables.

La gestión de la continuidad empresarial (BCM) abarca ITSCM y otros procesos de mitigación de riesgos. Por lo que los equipos de TI deben colaborar para crear lo siguiente:

- **Un plan de continuidad empresarial (BCP):** En este se incluyen planes para la prevención y recuperación de incidentes TI a nivel de desastre.
- **Análisis de Impacto empresarial (BIA):** Identifican el posible impacto de un desastre TI en el negocio.

Por consiguiente, se muestra el proceso a seguir dentro de un plan de continuidad empresarial (BCP). La cual consta de 4 fases que se describen a continuación:

- **Fase 1:** Se toma en cuenta el alcance y las políticas de ITSCM.

- **Fase 2**: Indica los procesos que se debe seguir como es el análisis del impacto del negocio, identificación y análisis de activos, evaluación de riesgos, estrategia de continuidad. Revisar los Anexos 2 y 3.
- **Fase 3**: Indica el despliegue de la estrategia, desarrollo de procedimientos de continuidad y la puesta en marcha de la estrategia. (Revisar plan de acción)
- **Fase 4**: Mejora continua del servicio. (Conclusiones)

4.17.3 PLAN DE CONTINGENCIA

Un plan de contingencia es un proceso que se encarga de dar continuidad a los procesos en el caso que se presenten riesgos que puedan afectarlos, organizando a las personas responsables de cada área, actividades que ayuden a mitigar o evitar el impacto. Esta información será documentada en un texto totalmente claro y entendible con las medidas y normas a seguir de forma estratégica para su implementación. El objetivo principal de un plan de contingencia es mejorar la capacidad de respuesta frente a diversos eventos que afecten el buen funcionamiento del sistema. A más de ello el plan de contingencia pretende ayudar a las organizaciones empleando los recursos disponibles para poder enfrentar el escenario de riesgo.

4.17.4 OBJETIVO DE UN PLAN DE CONTINGENCIA

Según la NTE INEN-ISO /IEC 27002 y el registro oficial Nro. 039 GG, (2009) menciona que un plan de contingencia informático debe contar con los siguientes objetivos:

- Debe mantener a la medida de lo posible la continuidad de los servicios proporcionados por la organización denominados críticos en un nivel aceptable en caso de un plan de contingencia.

- Establecer acciones y procesos que permitan mantener la operatividad de los sistemas de información en caso de una emergencia.

4.17.5 IMPORTANCIA DE UN PLAN DE CONTINGENCIA

- Garantizar la seguridad física, la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos.
- Permitir realizar un conjunto de acciones con el fin de evitar el fallo, o en su caso, disminuir las consecuencias que en él se puedan derivar.
- Permite realizar un análisis de riesgos por servicio, respaldo de los datos y su posterior Recuperación de los datos. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal funcionamiento de una Institución. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la institución.

4.17.6 CICLO DE PLAN DE CONTINGENCIA

- **Identificar los riesgos potenciales:** el primer paso es identificar los posibles riesgos que pueden afectar la disponibilidad del servicio de base de datos. Esto puede incluir fallas

de hardware, errores de software, ataques cibernéticos, desastres naturales, errores humanos, entre otros.

- **Crear un plan de respaldo**: es importante tener una copia de seguridad actualizada de la base de datos en un lugar seguro y fuera del sitio, preferiblemente en una ubicación geográfica diferente a la principal. El plan de respaldo debe incluir detalles sobre cómo se realiza el respaldo, con qué frecuencia se realiza y cómo se verifica su integridad.
- **Establecer procedimientos de recuperación**: en caso de una falla o interrupción, es necesario contar con procedimientos claros de recuperación. Esto debe incluir instrucciones sobre cómo restaurar la base de datos desde una copia de seguridad, cómo verificar la integridad de los datos y cómo garantizar la continuidad del servicio.
- **Definir roles y responsabilidades:** es importante asignar roles y responsabilidades claras a las personas encargadas de ejecutar el plan de contingencia. Esto debe incluir un equipo de respuesta de emergencia que tenga la capacidad de responder rápidamente y tomar medidas para minimizar el impacto de una falla.
- **Realizar pruebas periódicas:** es importante realizar pruebas periódicas del plan de contingencia para asegurarse de que esté actualizado y sea efectivo. Las pruebas deben incluir simulaciones de situaciones de emergencia para evaluar la capacidad del plan de contingencia para responder y recuperar el servicio de base de datos.
- **Comunicar el plan:** finalmente, es importante comunicar el plan de contingencia a todos los miembros del equipo y partes interesadas relevantes. Esto debe incluir información sobre los riesgos potenciales, los procedimientos de respaldo y recuperación, los roles y responsabilidades, y las pruebas periódicas del plan.

4.17.7 IDENTIFICACION DE DAÑOS

Dentro del servicio de SIGM trabajan 2 BDD importantes, las cuales se dividen para cada una de los módulos habilitados para realizar las funciones diarias de la institución. El administrador del servicio del Sistema Integrado de Gestión Municipal es el encargado de identificar posibles daños físicos o lógicos que puedan interrumpir su buen funcionamiento. Una vez identificado el daño la persona responsable levantara el servicio dependiendo del tipo de afectación, para lo cual nos referimos al plan de acción. Ver en el Anexo X los posibles riesgos que pueden presentarse dentro de la Dirección de Tecnologías de la Información.

4.17.8 CREACION DE PLAN DE RESPALDOS

La Dirección de Tecnologías de la Información trabaja en base a las Políticas de seguridad detalladas en el documento denominado ***Memoria Técnica - Marzo 2023 - GAD IBARRA v2.***

4.17.9 PROCEDIMIENTOS DE RECUPERACIÓN

Dentro el procedimiento de recuperación, se detalla el plan de acción que el responsable asignado de cada servicio deberá seguir en el caso de presentarse algún tipo de afectación en el servicio.

4.17.10 PLAN DE ACCION

A continuación, se muestra un plan de acción a seguir, cuando ocurra algún inconveniente en el buen funcionamiento del Sistema Integrado de Gestión Municipal

(SIGM), y se deba implementar un contingente para que los módulos alojados en él, sigan en funcionando adecuadamente. En la Tabla 2 se muestra los pasos a seguir.

Tabla 2: Plan de acción en caso de caída del Sistema Integrado de Gestión Municipal.

ITEM	ACTIVIDAD	DESCRIPCION DEL REPORTE	IDENTIFICACION DEL DAÑO (FISICO O LOGICO)	DESCRIPCION DEL INCONVENIENTE	REQUERIMIENTO	INSTRUCTIVO	PLAN DE ACCION	RESPONSABLE	TIEMPO ESTIMADO
1	Realizar el diagnóstico del problema reportado	Reporte de usuarios	FÍSICO	Equipo apagado	Energía eléctrica	Revisar fuente de energía. Revisar cableado de la fuente de poder. Encender equipo. Revisar el servicio este activo.	Ver instructivo sección x	Ing. Gabriel Bucheli	
				Equipo quemado	Reporte al responsable de hardware, para cambio de equipo.	Remplazar equipo Hardware prepara equipo. Instalación y configuración de servicio de BDD Restaurar o recuperación de BDD.	Ver instructivo sección x	Ing. Gabriel Bucheli	
				Fallas del hardware del servidor (procesador, discos de memoria, RAM, placa base hardware de red, etc.)	Reporte al responsable de hardware, para cambio o reparación del elemento afectado.	Remplazar equipo Hardware prepara equipo. Instalación y configuración de servicio de BDD Restaurar o recuperación de BDD	Ver instructivo sección x	Ing. Gabriel Bucheli	

			LÓGICO	Falla en los servicios (HTML, Replica de BDD de SRI, Conexión BDD EMAPA, DINARDAP)	Comandos para levantar el servicio.	Encender equipo. Revisar el servicio este activo.	Ver instructivo sección x	Ing. Verónica Rosero Ing. Jairo Álvarez	
				Daño del Sistema Operativo	Imagen ISO	Instalación del sistema operativo, configuración de accesos, instalación del motor de base de datos.	Ver instructivo sección x	Ing. Gabriel Bucheli	
				Servicio de BDD Inactivo	Comandos para levantar el servicio.	Levantar el servicio.	Ver instructivo sección x	Ing. Manuel Lara	
				Fallas en la red de datos.	Software de monitoreo de la red.	Escaneo de la red, identificación de problemas	Ver instructivo sección x	Ing. Gabriel Bucheli	
				Saturación en espacio de disco		Eliminar los archivos temporales o logs de fechas de anteriores	Ver instructivo sección x	Ing. Gabriel Bucheli	
				Inyección de código malicioso	Restauración de aplicaciones	Levantar el servicio mediante la última imagen de respaldo del SO. Publicar todas las aplicaciones desde Script case.	Ver instructivo sección x	Ing. Verónica Rosero Ing. Jairo Álvarez	

4.17.11 PRUEBAS DE FUNCIONAMIENTO

Una vez que se ha identificado la falla de total o parcial de una base de datos, el administrador procederá a realizar una auditoria para determinar la causa del inconveniente determinando el tipo de amenaza materializada.

Como primer paso se determina la alerta emitida por el software de monitoreo implementado en el GAD-Ibarra, una vez identificado el daño se procede a seguir el instructivo planteado según el Plan de Contingencia dependiendo del tipo de inconveniente, en este caso se tomará como referencia los fallos más comunes que se pueden presentar. La demostración de las pruebas del Plan de Contingencia se la realizan mediante un Check List en el cual se detalla los daños físicos y lógicos y si éstos fueron solventados o no. Cabe mencionar que el análisis de daños tanto físicos como lógicos están enfocados únicamente al servicio de SIGM, como se muestra a continuación:

- **Daños Físicos**

Dentro de los daños físicos la Dirección de Tecnologías de la Información debe tener equipos de respaldo, para poder solventar los daños físicos descritos en el Plan de Contingencia.

Tabla 104 Equipos de Respaldo de manejados por TICs.

EQUIPOS	RESPALDO	
	SI	NO
Generador Electrico	☑	☐
UPS	☑	☐
Inversores	☑	☐
Baterias	☑	☐
Reguladores de voltaje	☑	☐
Regletas	☑	☐
Cable Eléctrico	☑	☐
Toma Corriente	☑	☐
Servidores	☑	☐
CPU	☑	☐
Discos de memoria	☑	☐
Extintores	☑	☐
Sensores de Humo	☑	☐
Cable Fibra Óptica	☑	☐
Cable UTP Cat6a	☑	☐

Check List de las Pruebas de Funcionamiento del Plan de Contingencia.

Las pruebas de funcionamiento se realizaron en conjunto con las personas responsables de la administración y gestión del Sistema Integrado de Gestión Municipal. Por motivos de seguridad de la información se optó por la demostración de las pruebas de funcionamiento del Documento denominado Plan de Contingencia SIGM mediante la creación de un check list, en el cual se muestra

los daños ocasionados al servicio dependiendo del tipo y si éste fue solventado o no. Como se muestra en la tabla 2 y 4.

Tabla 105 Check List de Pruebas de Funcionamiento Daños Físicos.

TIPO DE DAÑO	DESCRIPCION	EVENTO SOLVENTADO		RESPONSABLE	TIEMPO ESTIMADO	TIEMPO DURADO
		SI	NO			
Físico	Equipo quemado, se revisa y se determina que el equipo esta quemado por descargas de energía. Reemplazo del equipo.	☑		Ing. Gabriel Bucheli	15 min	12 min
Físico	Equipo apagado, se revisa conexiones eléctricas, se mide niveles de voltaje.	☑		Ing. Gabriel Bucheli	10 min	7 min
Físico	Fallos de hardware de servidor. Disco de memoria saturado	☑		Ing. Gabriel Bucheli	12 min	**10 in**

- **Daños Lógicos**

Dentro de los daños lógicos, la Dirección de Tecnologías de la Información cuenta con políticas de seguridad de la información, las cuales establecen normas para resguardar la información de la Municipalidad y por ende de los servicios que esta ofrece y con ello dar una continuidad a la prestación de servicios. Para ello se ha realizado un check list de las herramientas esenciales que la Dirección de TIC´S necesita cumplir con lo antes descrito. Como se muestra en la Tabla 3 que se presenta a continuación:

Tabla 106 Herramientas de respaldo para solventar Daños Lógicos.

HERRAMIENTAS	**RESPALDO**		**OBSERVACIONES**
	SI	**NO**	
Respaldo de BDD IMI	☑		
Respaldo de Sistema réplica de base de datos Oracle del SRI	☑		
Imágenes ISO	☑		
Respaldo proveedor Internet	☑		
Respaldo de Soporte Técnico	☑		

Pruebas de Funcionamiento

En la Tabla 4 se detalla un check List de las pruebas de funcionamiento simuladas en la parte lógica del servicio SIGM.

Pruebas de Funcionamiento

Tabla 107 Check List de Pruebas de Funcionamiento Daños Lógicos.

TIPO DE DAÑO	DESCRIPCIÓN	SOLVENTADO		RESPONSABLE	TIEMPO ESTIMADO	TIEMPO DURADO
		SI	NO			
Lógico	Falla en los servicios (HTML, Replica de BDD de SRI, Conexión BDD EMAPA, DINARDAP)	☑		Ing. Verónica Rosero Ing. Jairo Álvarez	5 min	7 min
Lógico	Daño del Sistema Operativo	☑		Ing. Gabriel Bucheli	2 min	2 min
Lógico	Servicio de BDD Inactivo	☑		Ing. Gabriel Bucheli	5 min	4 min
Lógico	Fallas en la red de datos.	☑		Ing. Gabriel Bucheli	10 min	13 min
Lógico	Saturación en espacio de disco	☑		Ing. Gabriel Bucheli	5 min	6 min
Lógico	Inyección de código malicioso	☑		Ing. Verónica Rosero Ing. Jairo Álvarez	15 min	13 min

10.1.1 INFORME DE IMPLEMENTACION DEL PLAN DE CONTINGENCIA

A continuación, se especifica el contenido que debe tener el Informe una vez aplicado el contingente en el Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra.

- **Portada**: En ella se incluye el titulo y nombre de la Institución involucrada.
- **Índice**: Orden de los temas o partes de las páginas.
- **Introducción:** Establece un foco o idea central del inconveniente presentado. También indica la dirección e ideas principales que cubrirán dicho inconveniente. En ella generalmente se detallan hipótesis y objetivos.
- **Materiales y métodos**: Objetos utilizados. Se incluye el nombre del material o dispositivo y se describe el uso que se le dio, además se escriben las formas o métodos que se usaron para tener resultados.
- **Contenido:** En esta parte dar a conocer los resultados obtenidos, Estos son el fruto de los objetivos planteados en la Introducción. Se incluyen tablas o gráficos con los datos y una breve descripción.
- **Conclusiones:** Se incluyen los resultados más importantes que permitan responder las interrogantes planteadas en la introducción y que están de acuerdo con los objetivos planteados.
- **Bibliografía:** Ordenamiento alfabético y por fechas de la literatura ocupada para responder las inquietudes presentadas a lo largo de trabajo.

10.2 CONCLUSIONES

- ✓ Un plan de contingencia efectivo debe ser detallado, específico y estar disponible para todos los miembros del equipo encargado del Sistema Integrado de Gestión. Es importante que el plan se mantenga actualizado y se revise regularmente para asegurarse de que sigue siendo efectivo en la protección de las operaciones de la organización.
- ✓ Es importante identificar y evaluar los riesgos potenciales que pueden afectar el funcionamiento del Sistema Integrado de Gestión. Esto ayudará a establecer medidas preventivas y de respuesta adecuadas.
- ✓ Las pruebas y simulaciones regulares pueden ayudar a identificar posibles debilidades en el plan de contingencia y permitir que el equipo encargado del Sistema Integrado de Gestión practique los procedimientos de respuesta en caso de interrupción.
- ✓ Un equipo de respuesta a incidentes bien entrenado puede ayudar a minimizar el impacto de cualquier interrupción del Sistema Integrado de Gestión y acelerar la recuperación del sistema. Es importante que el equipo esté compuesto por miembros con habilidades y experiencia relevantes, y que se realicen simulaciones y ejercicios regulares para mantener sus habilidades actualizadas.

10.3 REFERENCIAS

Resumen de Referencias	
Nombre	**Formato (Físico/ Electrónico)**
GERI-DI-PR-001 Plan de contingencia SIGM	Electrónico/Físico

10.4 ANEXOS

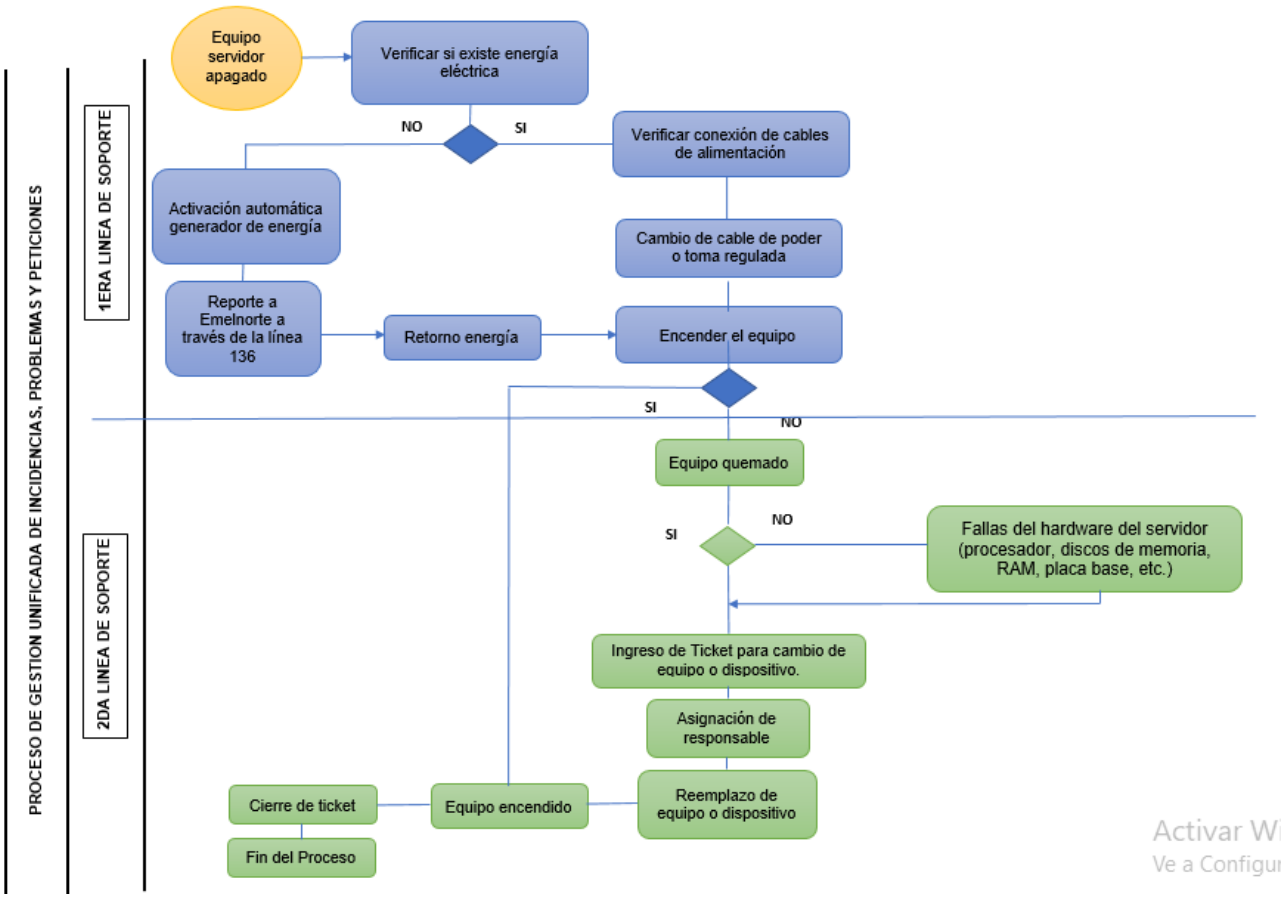
Resumen de Anexos			
Código	**Nombre del Formato**	**Formato (Físico/ Electrónico)**	**Ubicación**
Xxxxxx	Tipos de amenazas	Electrónico/Físico	Oficina / Cloud

ANEXO 1 Asignación de personal designado para dar solución al inconveniente presentado dependiendo del tipo de Fallo.

SERVICIOS	SUBSERVICIOS	CÓDIGO	PROPIETARIO/OPERADOR	BACKUP	CÓDIGO
RED	MAN	SRV-RED-MAN	gbucheli	etaez	SRV-RED
	WAN (ENLACES EXTERNOS)	SRV-RED-WAN	gbucheli	etaez	
	LAN	SRV-RED-LAN	mtobar	gbucheli	
	WLAN	SRV-RED-WLAN	gbucheli	etaez	
	CONECTATE IBARRA	SERV-RED-CI	etaez	gbucheli	
	INTERNET	SRV-RED-INTERNET	gbucheli	etaez	
SEGURIDAD	SEGURIDAD PERIMETRAL	SRV-SEG-PER	gbucheli	etaez	SRV-SEG
	VIDEO SEGURIDAD	SRV-DC-CCTVV	etaez	mtobar	
	ANTIVIRUS/ANTISPAM	SRV-SEG-AV	mtobar	etaez	
INFRAESTRUCTURA	HOSTING DE SERVIDORES	SRV-INF-HS	gbucheli	mtobar	SRV-INF
	VIRTUALIZACIÓN DE SERVIDORES	SRV-INF-KVM	gbucheli	mtobar	
WEB	QUIPUX	SRV-WEB-QUIPUX	etaez	etaez	SRV-WEB
	HELP DESK	SERV-WEB-OTRS	vdavila	etaez	SRV-OTRS
DATACENTER	CONTROL DE ACCESOS	SRV-DC-CCAA	mtobar	etaez	SRV-DC
	INCENDIOS	SRV-DC-FIRE	mtobar	vdavila	
	VENTILACIÓN Y AIRE ACONDICIONADO	SRV-DC-HVAC	mtobar	vdavila	
	ENERGIA	SRV-DC-POWER	mtobar	vdavila	
REGISTRO Y CONTROL	BIOMETRICOS	SRV-RYC-BIOM	mtobar	etaez	SRV-RYC
SOPORTE	EQUIPOS	SRV-SOP-EQP	vdavila	etaez	SRV-SOPORTE
	IMPRESORAS	SRV-SOP-IMP	vdavila	etaez	

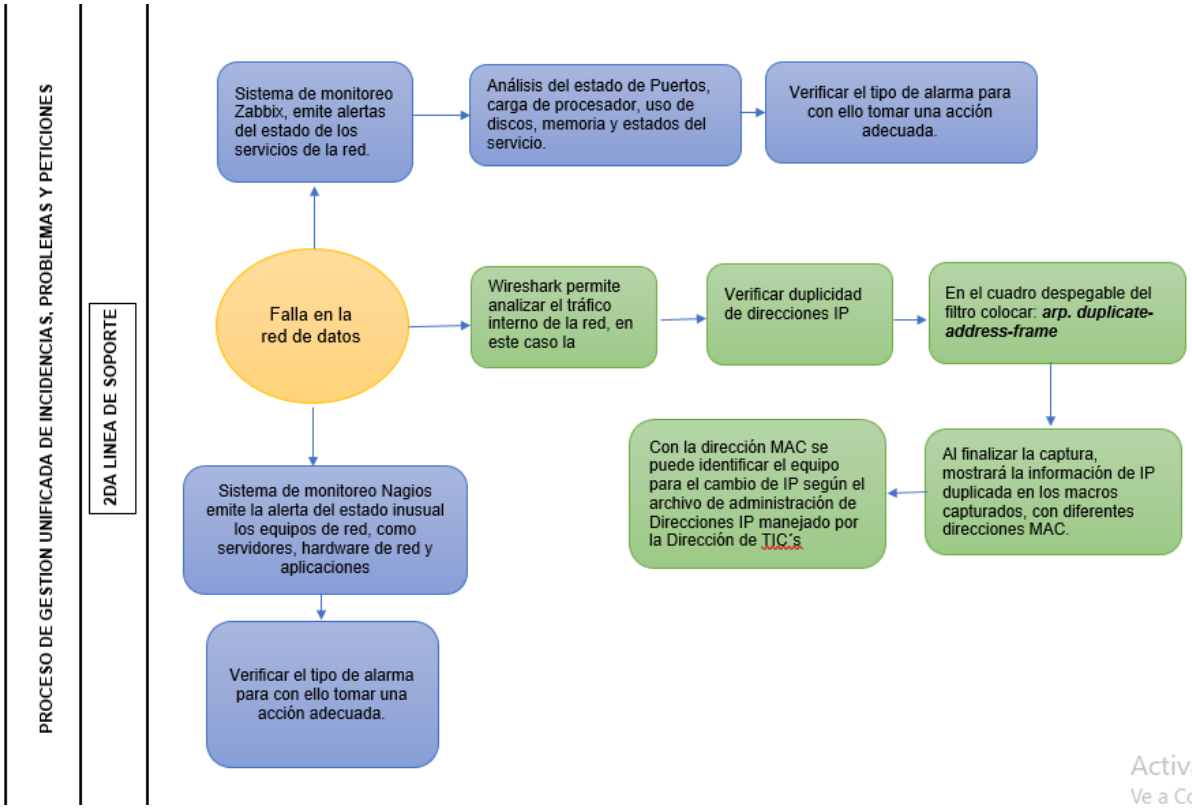
ANEXO 2 Diagramas de Flujo de las pruebas de funcionamiento del Plan de Contingencia.

Figura 14 Diagrama de Flujo del proceso de Fallos Físicos en el servicio de SIGM.



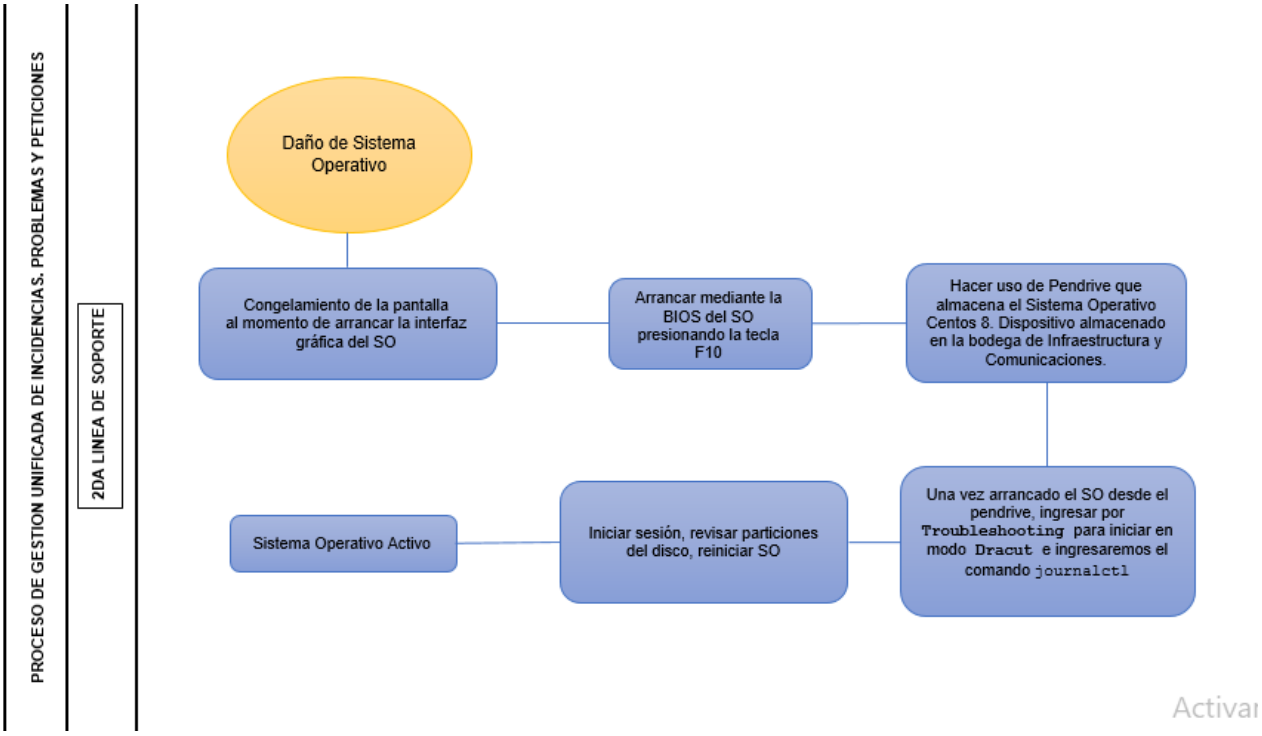
Nota: El presente diagrama se muestra el proceso a seguir en caso de una falla física del equipo que afecte el buen funcionamiento del sistema. Cada uno de los procesos tiene una línea de soporte responsable, la cual se encargará de tomas las acciones necesarias para levantar el equipo y por ende el servicio. Cabe mencionar que para el cambio de equipos la Dirección de Tecnologías de la Información cuenta con un manual de procedimientos ya que, al momento de cambio de un equipo o dispositivo, éste se vuelve un activo que debe pasar a la bodega de la persona responsable de Hardware, justificando el reemplazo del mismo.

Figura 15 Diagrama de Flujo del proceso de Fallas lógicas en el funcionamiento de la red de datos del servicio SIGM.



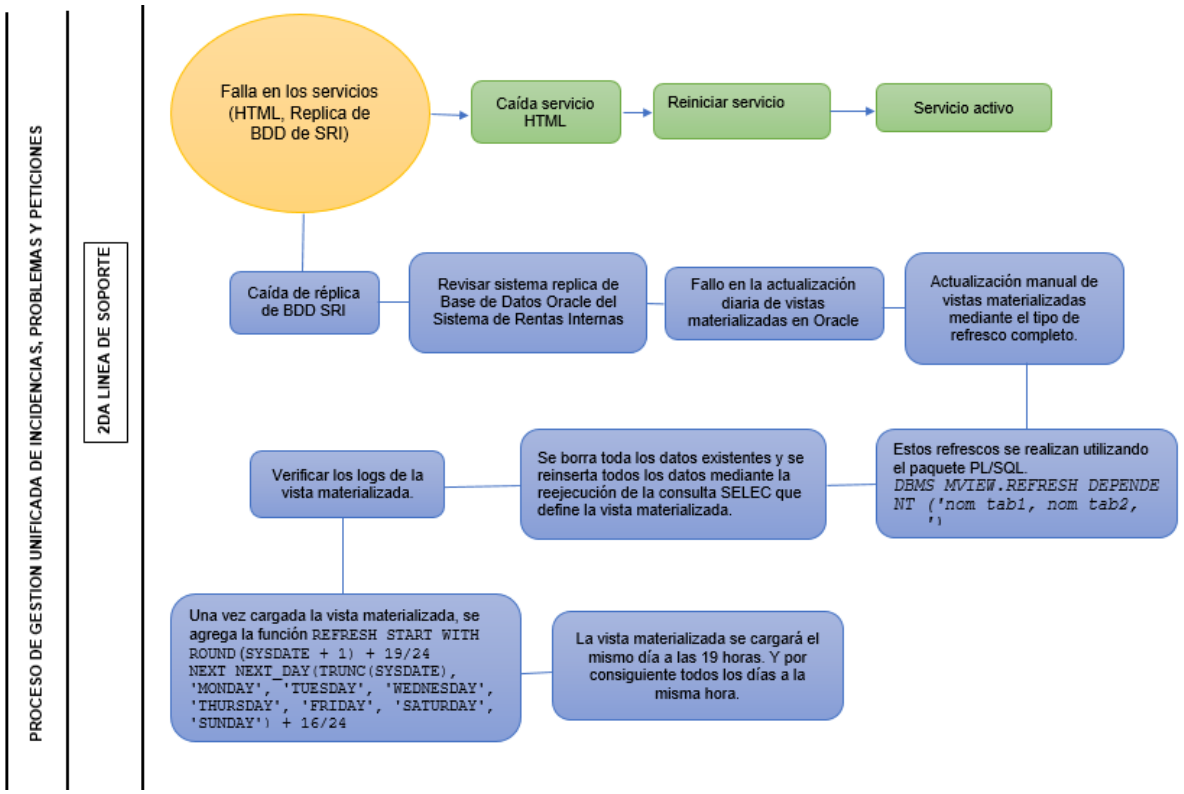
Nota: Dentro de los fallos lógicos que pueden ocurrir en la red de datos se tiene como principal a la duplicidad de direcciones IP, por ello la Dirección de TIC´s del GAD-Ibarra ha implementado la herramienta Wireshark, la cual permite filtrar mediante comandos las direcciones IP asignadas a un equipo con sus respectivas direcciones MAC´s. Adicional, la dirección cuenta también con sistemas de monitoreo como son Zabbix y Nagios, los cuales permiten tener un control de toda la infraestructura de la municipalidad.

Figura 16 Diagrama de flujo de procesos en caso de Falla del Sistema Operativo



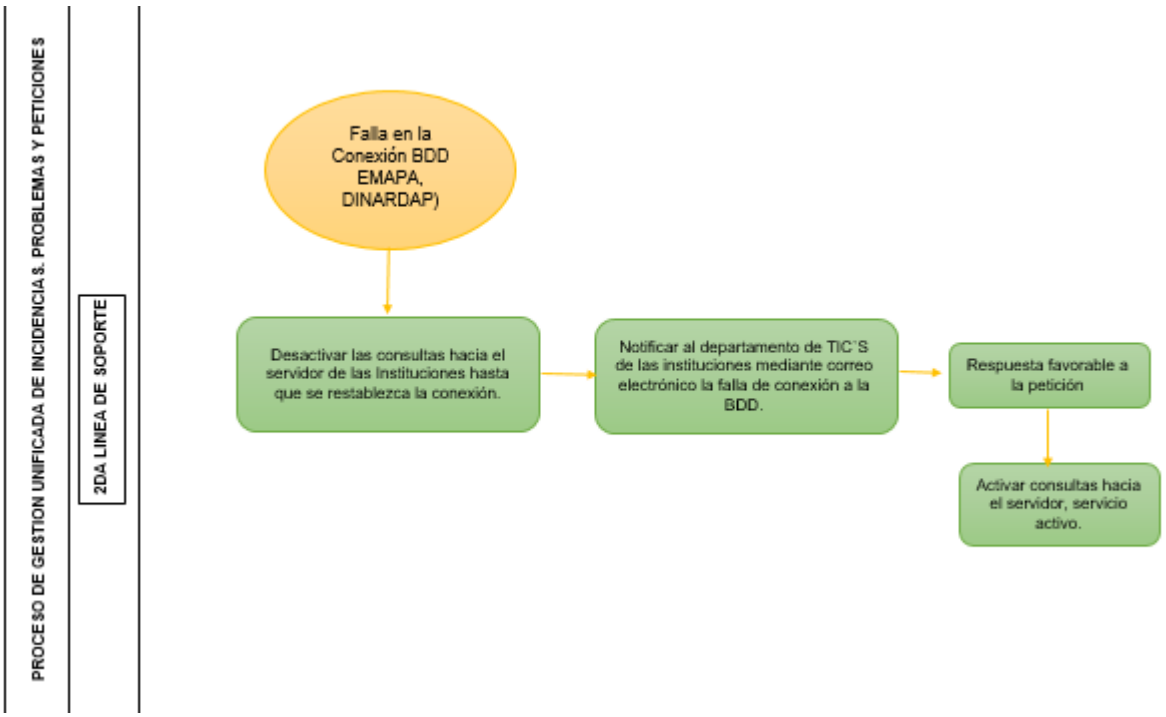
Nota: El presente diagrama se muestra el proceso a seguir en caso de una falla del sistema operativo Centos 8.

Figura 17 Diagrama de Flujo al encontrar una falla en los servicios de HTML y BDD de SRI.



Nota: El presente diagrama se muestra el proceso a seguir en caso de una falla lógica en los servicios de HTML y BDD del Servicio de Rentas Internas. El cual será revisado y reparado por un especialista en el área.

Figura 18 Diagrama de Flujo de procesos Daños Lógicos del servicio SIGM.



Nota: El presente diagrama se muestra el proceso a seguir en caso de una falla lógica en la conexión a la BDD de las instituciones de EMAPA y DINARDAP. Cabe mencionar que al momento de existir la desconexión de las Bases de Datos no habrá mayor afectación al brindar el servicio al cliente, ya que son bases de datos de lectura.

10.5 CONTROL DE CAMBIOS

Resumen de Modificaciones con relación a la versión anterior:			
Nro. Versión	**Fecha Rev.**	**Descripción de modificación**	**Aprobado por:**
1.0	10-07-2023		