# UNIVERSIDAD TÉCNICA DEL NORTE

## FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

## CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

### TRABAJO DE INTEGRACIÓN CURRICULAR

**TEMA:**

"PLAN DE SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA DEL DATA CENTER, BASADO EN MARCO REFERENCIAL COBIT 2019, PARA EL GAD MUNICIPAL DEL CANTÓN BOLÍVAR."

Trabajo de titulación previo a la obtención del título de Ingeniero en Tecnologías de la Información.

**Línea de investigación:** Desarrollo, aplicación de software y cyber security (seguridad cibernética).


**AUTOR:**

Byron Andres Angulo Patiño.

**DIRECTOR:**

Ing. Marco Remigio Pusdá Chulde, PhD.


**Ibarra – Ecuador 2026.**

# 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:** | 0401573175 | | |
| **APELLIDOS Y NOMBRES:** | Angulo Patiño Byron Andres | | |
| **DIRECCIÓN:** | Bolívar - Carchi | | |
| **EMAIL:** | baangulop1@utn.edu.ec | | |
| **TELÉFONO FIJO:** | 062-287-092 | **TELÉFONO MÓVIL:** | 0939141325 |

| DATOS DE LA OBRA | |
|---|---|
| **TÍTULO:** | PLAN DE SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA DEL DATA CENTER, BASADO EN MARCO REFERENCIAL COBIT 2019, PARA EL GAD MUNICIPAL DEL CANTÓN BOLÍVAR. |
| **AUTOR (ES):** | Angulo Patiño Byron Andres. |
| **FECHA: DD/MM/AAAA** | 05/03/2026 |
| SOLO PARA TRABAJOS DE GRADO | |
| **PROGRAMA:** | [X] **PREGRADO** [ ] **POSGRADO** |
| **TITULO POR EL QUE OPTA:** | Ingeniero en Tecnologías de la Información. |
| **ASESOR /DIRECTOR:** | Ing. Marco Remigio Pusdá Chulde, PhD. |

### 2. CONSTANCIAS

El autor (es) manifiesta (n) 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 (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 05 días del mes de marzo de 2026

**EL AUTOR:**

Firmado electrónicamente por:
BYRON ANDRES ANGULO PATIÑO
Validar únicamente con FirmaEC

.....
Angulo Patiño Byron Andres.

# CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

**Ibarra, 05 de marzo de 2026**

Ing. Marco R. Pusdá, PhD
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR
CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.


*Ing. Marco R. Pusdá, PhD*

*C.C: 0401200951*

# APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificado del trabajo de Integración Curricular “ Plan de seguridad informática de la infraestructura del data center, basado en marco referencial COBIT 2019, para el GAD Municipal del Cantón Bolívar. ” elaborado por Angulo Patiño Byron Andres , previo a la obtención del título del Ingeniero en Tecnologías de la Información , aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

Firmado electrónicamente por:
MARCO REMIGIO PUSDA CHULDE
Validar únicamente con FirmaEC

*Ing. Marco R. Pusdá, PhD*

*C.C: 0401200951*

Firmado electrónicamente por:
DAISY ELIZABETH IMBAQUINGO ESPARZA
Validar únicamente con FirmaEC

*Ing. Daisy Imbaquingo, PhD*

*C.C: 1002873048*

# DEDICATORIA

Esta tesis está dedicada con todo mi cariño y admiración a mis hijas, con la esperanza de que comprendan que no existen límites cuando se tiene un propósito claro en la vida. Que aprendan que el éxito radica en el esfuerzo constante, la perseverancia, la disciplina y la responsabilidad, y que, con estos valores, todo lo demás llegará por añadidura.

A mi esposa, por su amor incondicional, apoyo constante y por ser mi pilar fundamental en cada paso de este camino.

A mis padres, por su incansable apoyo, confianza y por inculcarme siempre la convicción de que los sueños están hechos para ser cumplidos, y que la verdadera fuerza reside en la fe y el trabajo arduo.

Angulo Patiño Byron Andres

## AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento al Msc. Marco Pusdá y Msc. Daysi Imbaquingo, distinguidos docentes de la Universidad Técnica del Norte, quienes desde el inicio de este proceso académico han brindado su invaluable guía y orientación en el desarrollo de esta investigación, contribuyendo con su experiencia y conocimientos para el éxito de este trabajo.

Asimismo, agradezco profundamente al Ing. Libardo Benalcázar, Alcalde del Cantón Bolívar, y al Ing. Andrés Villarruel, jefe del Departamento de Tecnologías de la Información del GAD Municipal del Cantón Bolívar, por su predisposición, apoyo y confianza para llevar a cabo esta investigación, que tiene como objetivo mejorar los servicios tecnológicos en beneficio de la ciudadanía.

Finalmente, extiendo mi agradecimiento al personal directivo y técnico operativo de la Unidad Especial Móvil Antinarcóticos San Gerónimo, por su apoyo incondicional durante los momentos difíciles, demostrando siempre una actitud colaborativa que me permitió equilibrar el ámbito profesional con los estudios académicos, contribuyendo al desarrollo integral de este proyecto.

Angulo Patiño Byron Andres

# ÍNDICE DE CONTENIDOS

## ÍNDICE DE FIGURAS

## ÍNDICE DE TABLAS

## RESUMEN

El GAD Municipal del Cantón Bolívar enfrenta desafíos importantes debido a las vulnerabilidades en su Data Center, lo que pone en riesgo la disponibilidad, integridad y confidencialidad de los datos vitales para la administración pública, este trabajo tiene como objetivo diseñar un plan de seguridad informática que, basándose en el marco normativo COBIT 2019, busque proteger los datos e infraestructura tecnológica del GAD, garantizando su integridad y continuidad operativa, para lograr este objetivo, se adoptó un enfoque de investigación mixta, que se dividió en varias etapas, desde el diagnóstico inicial del estado actual de la infraestructura, pasando por el diseño y validación de herramientas de evaluación, hasta la aplicación de COBIT 2019 para identificar las brechas de seguridad y realizar un análisis de riesgos, los primeros resultados evidenciaron brechas significativas en la seguridad del Data Center, especialmente en las áreas relacionadas con el acceso físico y lógico, el manejo del cableado estructurado y la falta de redundancia en los sistemas críticos, estas deficiencias reflejaron un nivel de madurez en seguridad de 1.22, por debajo del nivel objetivo de 4 establecido por COBIT 2019, lo que subrayó la necesidad urgente de implementar mejoras en la infraestructura tecnológica, para validar las recomendaciones y el plan de seguridad propuesto, se aplicó la metodología Delphi en dos rondas sucesivas con la participación de siete expertos, En la primera ronda, los resultados mostraron un índice de aceptación del 87.2 %, lo que reflejó un alto grado de acuerdo sobre la necesidad de implementar las mejoras sugeridas, sin embargo, durante esta primera ronda también se identificaron áreas que requerían mayor claridad, como los indicadores de desempeño y algunos procedimientos operativos, tras realizar los ajustes necesarios, en la segunda ronda se alcanzó un consenso total (100 %) con puntuaciones de 5 en todos los dominios evaluados, lo que validó la efectividad del plan y demostró su viabilidad para mejorar la seguridad y eficiencia del Data Center, el impacto de esta investigación no solo se limita a la mejora de la infraestructura tecnológica del GAD Municipal, sino que también establece un modelo de gobernanza tecnológica replicable, que puede ser adoptado por otras entidades públicas y privadas, a través de este plan, se fortalece la seguridad informática, se optimiza la gestión de riesgos y se sientan las bases para un desarrollo sostenible en la administración pública, mejorando la confianza de los ciudadanos en los servicios digitales que ofrece el municipio.



**Palabras clave:** COBIT 2019, Seguridad informática, Data Center, Gobernanza de TI, Evaluación de madurez

## ABSTRACT

The Municipal Autonomous Government (GAD) of Bolívar Canton faces significant challenges due to vulnerabilities in its Data Center, which jeopardise the availability, integrity, and confidentiality of critical data for public administration. This study aims to design an IT security plan based on the COBIT 2019 framework, with the goal of protecting the data and technological infrastructure of the GAD, ensuring its integrity and operational continuity. To achieve this objective, a mixed-methods research approach was adopted, structured in several phases: from the initial diagnosis of the current state of the infrastructure, through the design and validation of evaluation tools, to the application of COBIT 2019 to identify security gaps and conduct a risk analysis. The initial results revealed significant security gaps in the Data Center, particularly in areas related to physical and logical access, structured cabling management, and the lack of redundancy in critical systems. These deficiencies reflected a security maturity level of 1.22, which is below the target level of 4 established by COBIT 2019, highlighting the urgent need to implement improvements in the technological infrastructure. To validate the recommendations and the proposed security plan, the Delphi methodology was applied in two successive rounds with the participation of seven experts. In the first round, the results showed an acceptance index of 87.2 %, reflecting a high degree of agreement on the need to implement the suggested improvements. However, during this first round, areas requiring greater clarity were also identified, such as performance indicators and certain operational procedures. After making the necessary adjustments, in the second round, a total consensus (100 %) was reached with scores of 5 in all evaluated domains, thereby validating the effectiveness of the plan and demonstrating its viability to improve the security and efficiency of the Data Center. The impact of this research extends beyond improving the technological infrastructure of the GAD Municipal; it also establishes a replicable IT governance model that can be adopted by other public and private entities. Through this plan, IT security is strengthened, risk management is optimised, and the foundations for sustainable development in public administration are laid, enhancing the trust of citizens in the digital services provided by the municipality.



**Keywords:** COBIT 2019, IT security, Data Center, IT Governance, Maturity Assessment

# CAPÍTULO I
# INTRODUCCIÓN

## 1.1 Planteamiento del Problema

En la actualidad, el Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Bolívar, tiene un Data Center que presenta diversas vulnerabilidades relacionadas con la seguridad de la infraestructura, lo que pone en riesgo la disponibilidad, integridad y confidencialidad de los datos, como también los servicios que brinda a la ciudadanía.

El centro de datos del GAD no cuenta con las medidas de seguridad necesarias, y en la actualidad se han detectado varios problemas que comprometen la integridad de la infraestructura tecnológica. y afectan al sistema de control de seguridad de acceso, interrupciones operativas por ausencia de sistemas de refrigeración, uso inapropiado de espacios, deficiencias en la organización y gestión del cableado estructurado [1].

Estas deficiencias pueden generar interrupciones en los servicios digitales, pérdida de datos sensibles, aumento en el tiempo de recuperación ante fallos y exposición a amenazas cibernéticas o físicas, afectando la operatividad de la entidad y comprometiendo la confianza de la ciudadanía en la administración municipal [2].

La Fig. 1 muestra un diagrama de los problemas encontrados en el GAD municipal del cantón Bolívar. Este diagrama no solo describe las causas, sino también sus efectos, además permite visualizar los roles de quienes contribuyen a la situación de crisis, la necesidad de mejorar la gestión y seguridad del data center.

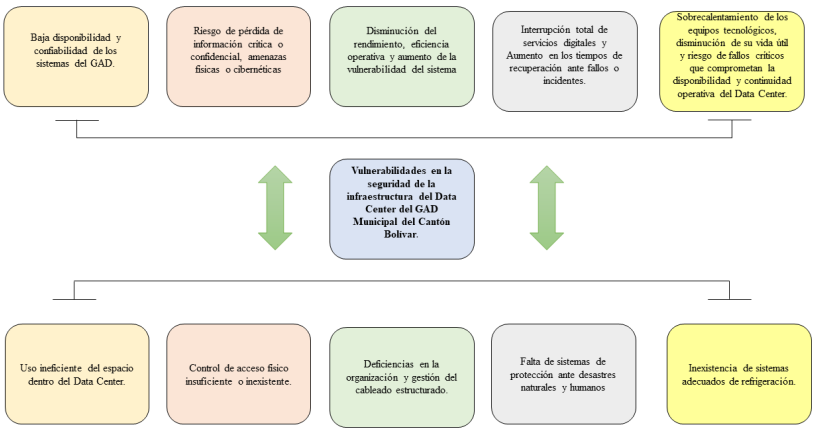


**Fig. 1**. Árbol de problemas

Desde un enfoque tecnológico, COBIT 2019 se presenta como el marco de trabajo reconocido mundialmente, diseñado para garantizar el Gobierno Corporativo de la Información y la Tecnología (GEIT). Este marco facilita la evaluación técnica de la seguridad en la infraestructura del data center, empleando una metodología que se basa en el análisis de riesgos y el cumplimiento de estándares internacionales, de esta forma, se podrán identificar vulnerabilidades específicas que requieren atención.

Con base en el diagnóstico realizado sobre el estado actual de la infraestructura y la seguridad del Data Center del GAD Municipal del Cantón Bolívar, la arquitectura de seguridad alineada al marco COBIT 2019, incluye un conjunto de recomendaciones que puedan servir como base para la toma de decisiones y la implementación de mejoras que garanticen el cumplimiento de estándares para datacenters seguros, confiables y eficientes [3].

## 1.2 Objetivos

### 1.2.1 Objetivo General

Desarrollar un plan de seguridad informática de la infraestructura del Data Center, basado en Marco Referencial COBIT 2019, para el GAD Municipal del Cantón Bolívar.

### 1.2.2 Objetivos Específicos

- Documentar el estado actual de la infraestructura del Data Center del GAD Municipal del Cantón Bolívar, considerando aspectos físicos, de cableado estructurado y seguridad de acceso.

- Aplicar Marco referencial COBIT 2019, identificando dominios y principios relacionados a la seguridad de la infraestructura del Data Center con la finalidad de verificar el cumplimiento de estándares y gestión de riesgos.

- Evaluar el plan propuesto en función de los hallazgos obtenidos sobre la seguridad de la infraestructura del Data Center, proponer recomendaciones y buenas prácticas de gestión que contribuyan a mejorar su nivel de seguridad, confiabilidad y eficiencia operativa.

## 1.3 Alcance y delimitación

El presente estudio se enfoca en la evaluación y diagnóstico de la seguridad de la infraestructura del Data Center del GAD Municipal del Cantón Bolívar, tomando en cuenta los siguientes aspectos: infraestructura física, cableado estructurado y controles de acceso, con la finalidad de identificar vulnerabilidades y riesgos que afecten el correcto funcionamiento del Data Center.

Para cumplir con el objetivo de diagnosticar la seguridad de la infraestructura del Data Center, se lleva a cabo una revisión bibliográfica de los principios y dominios COBIT 2019, como también estándares internacionales relacionados con la seguridad de la infraestructura de TI.

Como resultado final, se desarrolla un plan de seguridad informática que abarca los hallazgos obtenidos, incluyendo la evaluación del estado actual, la identificación de riesgos y vulnerabilidades en la infraestructura, como también las recomendaciones basadas en estándares internacionales. Todo esto con el objetivo de mejorar la seguridad y la confiabilidad del data center.

Es importante aclarar, que el presente estudio no contempla la implementación de las mejores propuestas, solo se limita a la evaluación, diagnóstico y generación de recomendaciones que sirvan como base para futuras decisiones de adecuación y mejora por parte del GAD Municipal del Cantón Bolívar

## 1.4 Justificación

Un centro de datos o Data Center (DC), es el lugar más crítico para las empresas u organizaciones, debido a que alberga los activos más importantes en infraestructura, redundancia y protección, garantizando así la confidencialidad, disponibilidad e integridad de la información [4].

Esta investigación ofrece al GAD Municipal del Cantón Bolívar un informe detallado sobre el estado actual de la infraestructura del Data Center, en él, se identifican las principales vulnerabilidades y riesgos en cuanto a seguridad, utilizando el marco COBIT 2019 como referencia, en línea con las normas y estándares internacionales.

Además, se alinea con el Objetivo de Desarrollo Sostenible (ODS) 9: Industria, Innovación e Infraestructura, que busca fortalecer la resiliencia de las infraestructuras tecnológicas para garantizar un desarrollo sostenible e inclusivo, asegurando que la administración municipal pueda ofrecer soluciones tecnológicas confiables a la ciudadanía [5].

Los principales beneficiarios son:

- El GAD Municipal del Cantón Bolívar, quien tendrá un documento de valor para tomar decisiones estratégicas para mejorar su infraestructura y garantizar la seguridad y continuidad de los servicios digitales.
- Los funcionarios municipales, quienes tendrán un entorno tecnológico más confiable seguro y eficiente.
- La ciudadanía, tendrán un servicio de calidad, sin interrupciones o perdidas de información.

La propuesta ayuda a documentar las deficiencias y vulnerabilidades que tiene el Data Center y como estos riesgos pueden comprometer significativamente a la operatividad del Municipio, como también fomenta la mejora continua en la seguridad de la administración pública, frente a cualquier evento adverso.

La aplicación del marco referencial COBIT 2019,facilita la identificación y gestión eficaz de los riesgos y vulnerabilidades asociados con la seguridad del Data Center, solucionando problemas específicos encontrados en la evaluación inicial, que posiblemente fueron ocasionados por las malas administraciones o la falta de conocimiento en la gestión tecnológica.

Desde el punto de vista de la ingeniería esta investigación aporta con beneficios técnicos, teóricos y prácticos en el conocimiento de estándares internacionales para la implementación de Data Center como COBIT 2019.

La importancia de contar con un Data Center que disponga de una infraestructura tecnológica certificada, segura y confiable, radica en establecer una metodología de evaluación de tecnológica en instituciones públicas, sirviendo como referencia para futuras auditorias y planificación de inversiones tecnologías.

Con este estudio, se espera fortalecer la seguridad de la infraestructura del Data Center del GAD Municipal del Cantón Bolívar, esto contribuirá a mejorar la protección de los datos, el almacenamiento de la información, el manejo adecuado del cableado estructurado, la comunicación entre los usuarios y, en general, la confianza en los servicios que se ofrecen a la comunidad.

# CAPÍTULO II
# MARCO TEÓRICO

## 2.1 Antecedentes

El gobierno autónomo descentralizado Municipal del Cantón Bolívar, se encuentra ubicado en la Provincia del Carchi, como cabecera cantonal la parroquia con el mismo nombre y una vida política institucional de 40 años, dentro de la estructura organizacional del GAD, existe el departamento de Tecnologías de la información que tiene como objetivo administrar y gestionar eficientemente los recursos informáticos y de comunicación, mediante la utilización de aplicaciones y servicios en beneficio de la comunidad.

Esto favorece una gestión pública eficiente y significativa para la comunidad, funcionando de manera integrada con la información accesible a los diversos niveles de toma de decisiones del GAD Municipal del Cantón Bolívar, en cumplimiento con las disposiciones legales actuales [6].

Eito-Brun et al. (2020) llevaron a cabo un estudio en Madrid, España, donde analizaron cómo se aplica el marco COBIT 2019 en los modelos de Gobernanza de TI, para ello, combinaron revisiones de documentos y entrevistas con partes interesadas [7]. Emplearon una metodología de codificación cualitativa que les permitió establecer una conexión clara entre los principios de COBIT y las normas ISO, los resultados mostraron una alta compatibilidad entre ambos marcos, aunque también se identificaron algunas áreas que requieren mejora, sobre todo en la gestión de la información, el estudio destacó la falta de visibilidad y de aplicación práctica de las normas de gobernanza, lo que subraya la necesidad de fortalecer su integración en los procesos organizacionales para mejorar su efectividad.

Tuabanda J. (2023) realizó un diagnóstico de la infraestructura tecnológica del Colegio Nacional Cutulagua, en Ecuador, empleando el marco referencial COBIT 2019 para evaluar la eficacia de los procesos de gestión de TI y la seguridad de la información [8]. La investigación integró encuestas, entrevistas con docentes y personal técnico, así como un análisis comparativo con los estándares COBIT, y observación directa de la infraestructura del Data Center, entre los principales hallazgos se identificaron deficiencias en la gestión de la seguridad y el control de

accesos. Como resultado, se propusieron estrategias de mejora basadas en COBIT 2019, incluyendo políticas de control de acceso y capacitación del personal, lo que permitió formular un plan de acción enfocado en la modernización de la infraestructura, la optimización de recursos tecnológicos y el fortalecimiento de la seguridad de la información.

Arana J. (2020) realizó un estudio sobre la infraestructura tecnológica del Centro de Procesamiento de Datos de la Municipalidad Provincial de Ilo, en Perú, aplicando el marco COBIT 2019 para evaluar la seguridad y eficiencia operativa [9]. Se emplearon entrevistas, recopilación de datos sobre hardware y software, y un análisis comparativo con los estándares del marco. El diagnóstico evidenció deficiencias en la gestión de seguridad informática y en la configuración de la red estructurada. A partir de estos hallazgos, se propusieron mejoras como la implementación de controles específicos, optimización de procesos y capacitación del personal. La aplicación de estas recomendaciones permitió fortalecer la infraestructura tecnológica, Mejorar la seguridad de la información y alinear las operaciones del Data Center con los estándares internacionales.

Lema C. (2020) desarrolló un plan de gestión de seguridad de la información para el Gobierno Provincial del Cañar, con el propósito de identificar y reducir los riesgos en la infraestructura tecnológica de la institución, utilizó un enfoque inductivo-deductivo respaldado por investigación bibliográfica y técnica [10]. Se realizaron encuestas, listas de verificación y entrevistas con el personal del área de TIC, para el análisis, se aplicaron las normativas ISO/IEC 27001, MAGERIT y COBIT 2019, los resultados identificaron riesgos críticos, como la falta de procedimientos formales de seguridad, con base en estos hallazgos, se propusieron medidas para mejorar la protección de la información, destacando el valor del marco COBIT 2019 para alinear la gestión de seguridad con los estándares internacionales, en un contexto de digitalización pública.

De acuerdo con Panimboza A. (2020), se realizó un diagnóstico en el departamento de Tecnologías de la Información y Comunicación (TIC) de la Universidad Estatal Península de Santa Elena (UPSE), en Ecuador, Enfocado en la seguridad de la información y la infraestructura del Data Center, se tomaron como referencia la norma ISO/IEC 27002 y el marco COBIT 2019 [11]. A través de observación directa y entrevistas con el personal, se evaluaron aspectos clave como el control de acceso y la seguridad física, el estudio reveló la falta de documentos esenciales, como análisis de riesgos y protocolos de acceso, lo que generaba vulnerabilidades en la

infraestructura, como resultado, se diseñó un plan de acción con mejoras basadas en buenas prácticas internacionales, orientadas a mitigar los riesgos, fortalecer la seguridad de la información y establecer una base para futuras evaluaciones en entornos similares.

Según el reporte de ISACA.[12], en 2022, el 65 % de las organizaciones que implementan COBIT 2019 mejoran sus métricas de seguridad en un 40 % durante el primer año. Por otro lado, Cedeño R. [13], en 2022 reportó que el 30 % de los ataques a entidades públicas en Ecuador se deben a vulnerabilidades en Data Centers.

## 2.2 Institución: misión, visión y estructura organizacional

El Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Bolívar es la entidad responsable de administrar los recursos públicos y de garantizar el desarrollo social, económico y tecnológico de la comunidad, Dentro de su estructura, el área de Tecnologías de la Información cumple un papel estratégico al gestionar los recursos tecnológicos que sustentan los procesos administrativos y de atención a la ciudadanía [14].

### 2.2.1 Misión

El GAD Municipal del Cantón Bolívar como una institución autónoma tiene la misión fundamental de promover e incentivar las fortalezas de la ciudadanía y sus organizaciones para que conjuntamente con el Gobierno Municipal, eje coordinador, mejore su calidad de vida en el marco del desarrollo humano y socio económico integral, cuidando su ambiente, privilegiando satisfacer las necesidades intelectuales, físicas y espirituales, garantizando la Continuidad en el tiempo, con ciudadanos constructores de su propio bienestar, enmarcados en el Plan de Desarrollo y Ordenamiento Territorial del Cantón Bolívar [14].

### 2.2.2 Visión

El GAD tiene una visión orientada al desarrollo y progreso de sus moradores, en la que busca trabajar de manera sostenida para mejorar la calidad de vida de sus habitantes, mediante la aplicación de políticas participativas de desarrollo, aprovechando sus potencialidades y oportunidades, en el marco de la interculturalidad, la solidaridad, la tolerancia, la reciprocidad y la transparencia [14].

### 2.2.3 Estructura organizacional

El Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Bolívar organiza sus recursos en cuatro áreas clave: procesos gubernamentales, procesos de asesoría y apoyo, procesos de valor agregado y empresas adscritas, lo que permite optimizar la administración pública [14].

En la parte superior de la estructura están la alcaldía, que tiene funciones ejecutivas, y el concejo municipal, encargado de la fiscalización y la legislación, conjuntamente con las unidades de asesoría, como la Procuraduría Síndica, así como las de comunicación y fiscalización, se encargan de garantizar el control y la transparencia.

La Dirección Administrativa y Financiera coordina varias unidades clave, como la Unidad de Tecnologías de la Información, que se encarga de gestionar los sistemas informáticos, garantizar la seguridad de la información y brindar soporte tecnológico, esta unidad juega un papel crucial en la implementación del plan de seguridad del Data Center, asegurando que los servicios digitales se mantengan operativos.

El GAD también incluye otras direcciones importantes, como Obras Públicas, Desarrollo Económico y Cultural, Planificación y Ordenamiento Territorial, y el Registro de la Propiedad, que son responsables de llevar a cabo proyectos y promover el desarrollo local, además, varias empresas adscritas, como la Empresa Municipal de Agua Potable, la Empresa de Tránsito y Transporte, y el Cuerpo de Bomberos, refuerzan la seguridad y los servicios básicos en la comunidad.

La Fig. 2 se muestra el diagrama de la estrucutura organizacional del GAD, con sus respectivos niveles jerárquicos y las áreas clave relacionadas con el plan de seguridad informática.

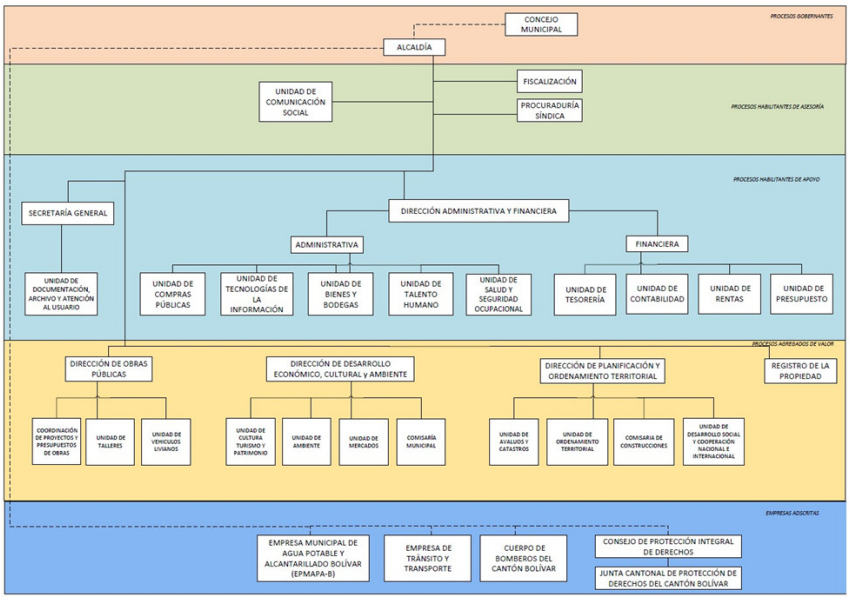


**Fig. 2**. Estructura organizacional GAD adaptado de [14]

## 2.3 ¿Qué es un plan de seguridad?

Un plan de seguridad informática es un documento estratégico que establece políticas, procedimientos y medidas destinadas a proteger los activos tecnológicos y la información crítica de una organización. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de los datos, así como la continuidad operativa de los servicios frente a riesgos internos y externos [15].

En el caso del GAD municipal del cantón Bolívar, el plan de seguridad está diseñado para proteger la infraestructura del data center, este plan abarca controles físicos y lógicos, gestión de riesgos, respaldo de la información y planes de contingencia, que son fundamentales para mejorar la resiliencia tecnológica, cumplir con estándares internacionales y generar confianza en los servicios digitales que ofrece el municipio.

## 2.4 Fundamentos de seguridad informática en Data Center

La información es la base para la toma de decisiones. La seguridad informática en los centros de datos es importante para proteger la información con el fin de mantener su confidencialidad e integridad. El COBIT 2019 proporciona un conjunto completo de principios y prácticas para la gobernanza y gestión de TI y puede ayudar a proteger infraestructuras críticas como los data centers.

En el marco normativo ecuatoriano que regula la seguridad de la información, la gobernanza tecnológica y la gestión de riesgos informáticos, se consideran las disposiciones establecidas en la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) y el Código Orgánico de la Economía Social de los Conocimientos (COESCCI), las cuales promueven el acceso abierto, la protección y la integridad de la información pública [16].

A nivel técnico y operativo, el estudio se basa en el marco de referencia COBIT 2019, el cual proporciona una estructura integral para la gobernanza y gestión de Tecnologías de la Información, orientada a la alineación entre los objetivos institucionales y los de TI, garantizando la confidencialidad, integridad y disponibilidad de la información [17]. Este marco fue complementado con principios de las normas ISO/IEC 27001 y ISO/IEC 27002, que orientan las buenas prácticas en seguridad de la información, y con la metodología PILAR, utilizada para la evaluación de riesgos y salvaguardas en la infraestructura tecnológica [18].

De esta manera, La propuesta se enmarca en un contexto legal y técnico que avala la creación de políticas y procedimientos de seguridad informática aplicables al Data Center del GAD Municipal del Cantón Bolívar, garantizando la trazabilidad, el control y la mejora continua de los procesos institucionales de TI [17].

### 2.4.1 ¿Qué es un Data Center?

Un Data Center es una instalación especializada en el procesamiento, almacenamiento y gestión de grandes volúmenes de datos de forma segura, según la International Data Center Authority (IDCA), debe contar con infraestructura física adecuada, energía redundante, climatización y sistemas de seguridad que aseguren su operación continua frente a amenazas internas y externas [19].

La Fig. 3 muestra la estructura de un Data Center, destacando sus componentes esenciales, este modelo ilustra la de infraestructura tecnológica, donde los servidores están interconectados para centralizar el procesamiento y almacenamiento de datos, facilitando el acceso remoto y mejorando la escalabilidad y la gestión de recursos.

**Fig. 3**. Representación gráfica de un Data Center adaptado de [20]

De acuerdo con COBIT 2019, el Data Center es un activo clave que debe gestionarse dentro del dominio APO03 - Gestión de la Arquitectura Empresarial, alineando la infraestructura con los objetivos estratégicos del negocio, garantizando la seguridad de la información.

Los Data Centers modernos incorporan tecnologías avanzadas de gestión de recursos, monitoreo en tiempo real y automatización, mejorando la seguridad y eficiencia operativa [21].

En el marco de la gobernanza de TI, COBIT 2019 considera al Data Center como un componente crucial de la arquitectura empresarial, garantizando la disponibilidad, confiabilidad y seguridad de la infraestructura [22].

### 2.4.2 Componentes Críticos

Los componentes críticos de un Data Center son aquellos elementos fundamentales que aseguran su funcionamiento seguro, confiable y eficiente, por lo tanto, deben ser gestionados de manera cuidadosa para minimizar riesgos y garantizar la continuidad de los servicios tecnológicos que respaldan las operaciones del GAD Municipal del Cantón Bolívar.

A continuación, se describen los principales componentes que conforman la infraestructura de un Data Center:

- **Infraestructura tecnológica**

La infraestructura tecnológica comprende todos los componentes físicos y lógicos que soportan el funcionamiento del Data Center incluyendo hardware (servidores, sistemas de almacenamiento, dispositivos de red), software, sistemas eléctricos, climatización, sistemas de respaldo energético y mecanismos de monitoreo. Una infraestructura bien diseñada permite maximizar la eficiencia energética, minimizar el riesgo de fallos y facilitar la gestión operativa [23].

- **Infraestructura física**

La infraestructura física de un Data Center incluye el espacio donde se alojan los equipos tecnológicos, junto con los sistemas eléctricos, de climatización y de seguridad física necesarios para su funcionamiento. A continuación, se detallan los principales componentes que forman parte de esta infraestructura.

- **Sistemas de energía eléctrica redundantes:** fuentes de alimentación ininterrumpida (UPS), generadores de respaldo y sistemas de distribución eléctrica diseñados para evitar interrupciones de energía que puedan afectar la operación de los servidores y equipos [24].

- **Sistemas de climatización y refrigeración:** para mantener la temperatura y humedad adecuadas, evitando el sobrecalentamiento que puede causar fallos en los equipos. El monitoreo constante y la automatización son claves para optimizar el consumo energético y prevenir riesgos térmicos [25].

- **Seguridad física:** controles de acceso biométricos, cámaras de videovigilancia, sistemas de detección y supresión de incendios y otras medidas para proteger el centro contra intrusiones o desastres naturales [26].

- **Sistemas de respaldo y recuperación**

Para asegurar la integridad y disponibilidad de los datos, los Data Centers deben implementar medidas integrales de protección y recuperación, entre las cuales destacan las copias de seguridad periódicas, almacenadas en ubicaciones separadas para evitar la pérdida de información ante incidentes críticos. Asimismo, es esencial contar con planes de recuperación ante desastres que definan procedimientos claros para restablecer las operaciones en caso de fallos mayores o amenazas a la seguridad. Además, la incorporación de sistemas de alta disponibilidad, como

clústeres de servidores y balanceadores de carga, permite reducir al mínimo el impacto de interrupciones, asegurando que los servicios tecnológicos permanezcan activos y accesibles para los usuarios en todo momento [27].

- **Monitoreo y gestión**

Los sistemas de monitoreo y gestión son esenciales para supervisar el estado del Data Center, identificar posibles incidentes y optimizar el uso de los recursos tecnológicos, entre las herramientas más utilizadas se encuentran las plataformas de gestión unificada, las cuales integran la supervisión de la infraestructura física, los aspectos de seguridad y el rendimiento de los sistemas.

Además, el análisis de datos combinado con inteligencia artificial permite anticipar posibles fallos y automatizar las respuestas ante incidentes, mejorando así la eficiencia operativa y la seguridad del Data Center. De igual manera, la realización de auditorías periódicas es necesaria para evaluar el cumplimiento de las políticas de seguridad establecidas y asegurar la conformidad con normas internacionales reconocidas [28].

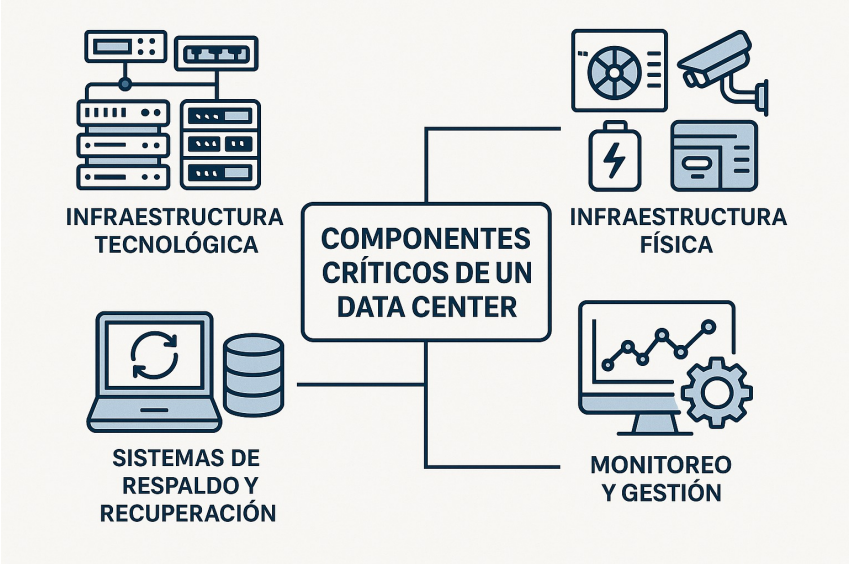


**Fig. 4**. Componentes críticos de un Data Center basada en [23]-[28].

En la Fig.4 se ilustran los principales componentes críticos que garantizan la operación continua y segura de un Data Center, organizados en cuatro categorías: infraestructura tecnológica, infraestructura física, sistemas de respaldo y recuperación, y monitoreo y gestión. Cada uno de estos elementos desempeña un papel fundamental para mantener la disponibilidad, integridad y eficiencia de los servicios tecnológicos que soportan las operaciones institucionales.

### 2.4.3 Conceptos clave

El concepto de Seguridad de la Información en un data center se basa en una secuencia de conceptos esenciales de protección, disponibilidad y confiabilidad de la infraestructura tecnológica y la información que almacena y procesa.

Estos argumentos no solo establecen los pilares o bases fundamentales de la seguridad, sino que también dirigen una serie de procesos y controles necesarios para su cumplimiento, es por ello que, el marco COBIT 2019 aborda estos principios a través de dominios específicos, enfocados en la gestión efectiva de la seguridad y la continuidad de los servicios.

La implementación de COBIT 2019 en el Data Center del GAD Municipal del Cantón Bolívar no solo refuerza la gobernanza de TI, sino que también mejora la gestión de los riesgos de seguridad, Esto asegura que las tecnologías de la información se conviertan en un facilitador estratégico para cumplir con los objetivos institucionales y proteger la información crítica, esta integración tanto técnica como organizacional es esencial para mantener la resiliencia y confiabilidad de los servicios tecnológicos municipales.

A continuación, se describen los conceptos clave que sustentan la seguridad en un Data Center y que son considerados por el marco COBIT 2019 en sus distintas prácticas de gestión:

- **Confidencialidad**

Se refiere a la protección de la información para que sólo las personas o sistemas autorizados tengan acceso a ella. Esto se logra mediante controles de acceso, cifrado, autenticación y políticas de manejo de la información, en COBIT 2019, la confidencialidad es gestionada principalmente dentro del dominio DSS05 - Gestión de la Seguridad de los Servicios, donde se establecen procesos para garantizar que los datos sensibles estén protegidos contra accesos indebidos [29].

En el marco de COBIT 2019, este principio se trata principalmente en el dominio DSS05 - Gestión de la Seguridad de los Servicios, este dominio establece prácticas y controles esenciales para prevenir accesos no autorizados, reducir al mínimo las fugas de información y garantizar la privacidad de los datos institucionales, por lo cual se considera que la correcta implementación de estas medidas es fundamental para proteger los activos de información y mantener la confianza en los servicios tecnológicos de la organización.

- **Integridad**

Garantiza que la información sea precisa, completa y que no sufra modificaciones no autorizadas durante su ciclo de vida. La integridad se mantiene a través de mecanismos como controles de acceso, registros de auditoría, y tecnologías para detección de alteraciones. COBIT 2019 integra la seguridad y la integridad en las políticas y controles dentro del dominio DSS05, asegurando que los datos estén protegidos contra corrupción y alteraciones [30].

Para asegurar la integridad se utiliza mecanismos como registros de auditoría, control de versiones, firmas digitales y políticas de verificación, paralelamente el marco COBIT 2019 también aborda este principio en el dominio DSS05, promoviendo prácticas que previenen la alteración de datos y aseguran la trazabilidad de cualquier modificación de la información.

- **Disponibilidad**

Implica que los sistemas, aplicaciones y datos estén accesibles cuando se necesiten por los usuarios autorizados, la disponibilidad es crítica para evitar interrupciones en servicios, especialmente en entornos como Data Centers. COBIT 2019 la aborda a través del dominio DSS04 - Gestión de la Continuidad, que define estrategias para prevenir interrupciones y garantizar la recuperación rápida en caso de fallos [31].

COBIT 2019 a través del dominio DSS04 permite la gestión de la continuidad , manteniendo la disponibilidad, este dominio sugiere implementar copias de seguridad, recuperación ante desastres y planes de operaciones preventivas que asegurarán una infraestructura resiliente contra fallos y perturbaciones.

- **Redundancia**

La redundancia consiste en la duplicación de elementos o sistemas para evitar fallos únicos que puedan afectar la operación incluyendo energía, conexiones de red, hardware y sistemas críticos, COBIT 2019 destaca la importancia de la redundancia para garantizar la disponibilidad y resiliencia, promoviendo su planificación dentro de DSS04 y APO12 (Gestión del Riesgo) [32].

Este concepto está relacionado con la planificación de la resiliencia y es abordado por COBIT 2019 en los dominios DSS04 y APO12 Gestión del Riesgo,una infraestructura redundante disminuye considerablemente la probabilidad de una caída total del sistema.

- **Resiliencia**

La resiliencia hace referencia a la capacidad del Data Center para soportar y recuperarse de fallos, ataques o desastres, garantizando la continuidad de los servicios y reduciendo al mínimo

los impactos negativos, en COBIT 2019, la resiliencia se integra en los procesos de gobernanza y gestión de riesgos (APO12) y continuidad (DSS04), promoviendo una infraestructura preparada para enfrentar incidentes y que pueda recuperarse rápidamente [33].

- **Alineación con COBIT 2019**

COBIT 2019 integra los conceptos antes mencionados a través de los siguientes dominios:

- **DSS04 - Gestión de la continuidad:** permite asegurar la disponibilidad y la recuperabilidad de los servicios.
- **DSS05 - Gestión de la seguridad del servicio:** permite garantizar la confidencialidad e integridad de la información.
- **APO12 - Gestión de riesgos:** facilita la identificación, evaluación y mitigación de riesgos relacionados con la seguridad y la continuidad.

Estos principios forman parte fundamental del marco COBIT 2019 y actúan de manera complementaria para asegurar que un Data Center opere bajo altos estándares de seguridad, confiabilidad y eficiencia. La Fig. 5 ilustra cómo se estructuran estos principios, divididos en dos grandes grupos:

- Principios del Sistema de Gobernanza, representados en color amarillo, que definen las características necesarias para construir un sistema eficaz de gobierno de TI.
- Principios del Marco de Gobernanza, representados en color verde, describen las características del propio COBIT 2019 como herramienta de gestión.

Esta clasificación ayuda a comprender cómo COBIT 2019 garantiza la gobernanza de la tecnología de la información y la gestión de riesgos, contribuyendo a una administración tecnológica sólida en organizaciones como el GAD Municipal del Cantón Bolívar

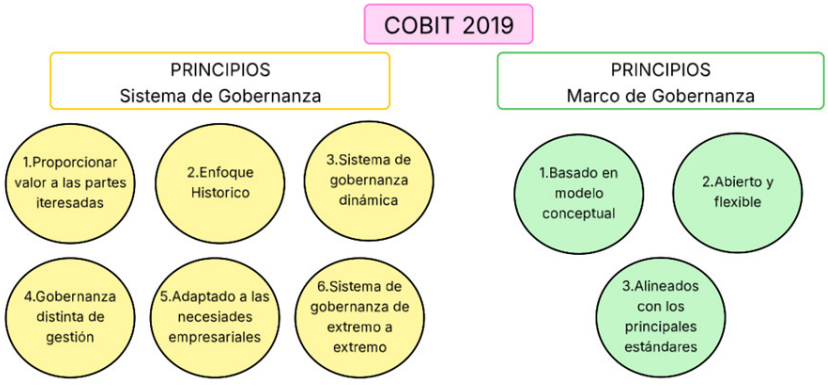


**Fig. 5**. Integración de principios COBIT 2019 adaptado de [12]

En el caso del GAD Municipal del Cantón Bolívar, aplicar estos conceptos dentro del marco COBIT 2019 permitirá estructurar una estrategia integral de seguridad informática, adaptada a sus necesidades y capacidades institucionales, al comprender y aplicar estos principios, se podrá fortalecer la infraestructura tecnológica existente, mejorar la confianza ciudadana en los servicios digitales municipales, y sentar las bases para una futura certificación bajo estándares internacionales de calidad y seguridad de la información.

### 2.4.4 Amenazas y riesgos en Centros de Datos

Los data centers enfrentan diversas amenazas que comprometen la seguridad, disponibilidad e integridad de los sistemas, lo que afecta la operación del GAD municipal del cantón Bolívar, identificar y gestionar estos riesgos es clave para garantizar la continuidad y la confianza en los servicios digitales, entre las principales tenemos:

- **Fallas eléctricas o de climatización.** Las interrupciones eléctricas o los problemas con la climatización pueden causar apagones, sobrecalentamiento y daños en el hardware, lo que lleva a la pérdida de datos y a costos elevados [34]. El dominio APO12 - Gestión del Riesgo de COBIT 2019 recomienda implementar controles preventivos, redundancia y un mantenimiento programado para mitigar estos riesgos.

- **Accesos no autorizados.** Pueden ocurrir de forma física o lógica, comprometiendo la confidencialidad y la integridad de la información [35]. El dominio DSS05 - Gestión de la Seguridad de los Servicios establece políticas de autenticación, autorización y monitoreo continuo.

- **Ataques cibernéticos.** Los ataques cibernéticos, como el ransomware, el malware y los ataques DDoS, pueden comprometer la disponibilidad y confidencialidad de los datos [36]. COBIT 2019 sugiere implementar mecanismos de detección temprana, una respuesta adecuada a incidentes y mantener los sistemas de seguridad actualizados de manera constante.

- **Desastres naturales.** Incendios, inundaciones o terremotos pueden causar daños significativos a la infraestructura, el dominio DSS04 - Gestión de la Continuidad enfatiza la planificación de la ubicación, el diseño físico y la implementación de planes de recuperación ante desastres [37].

- **Errores humanos.** Configuraciones incorrectas, negligencias o falta de capacitación generan vulnerabilidades y fallos operativos [38], siendo una de las causas más frecuentes de incidentes en Data Centers.

## 2.5 Estándares de seguridad para Data Center

Antes de presentar los principales estándares aplicables a la seguridad y operación de los Centros de Datos, es importante destacar que estos marcos normativos proporcionan lineamientos técnicos y de gestión que permiten garantizar la continuidad operativa, la protección física y lógica, y la calidad del servicio.

En la Tabla I se resumen los estándares más relevantes que orientan el diseño, mantenimiento y evaluación de los Data Centers, entre los que destacan la clasificación TIER del Uptime Institute, la norma TIA-942 y las recomendaciones de la International Data Center Authority (IDCA) [39]-[41].

Tabla I.
RESUMEN DE ESTÁNDARES DE SEGURIDAD PARA DATA CENTERS

| **Norma / Estándar** | **Descripción** | **Clasificación / Niveles** | **Principales Características** |
|---|---|---|---|
| **Clasificación TIER (Uptime Institute)** | Define niveles de disponibilidad y resiliencia en la infraestructura tecnológica de los Data Centers, determinando el grado de redundancia y tolerancia a fallos [40]. | ▪ TIER I: 99.67 %.<br>▪ TIER II: 99.74 %.<br>▪ TIER III: 99.98 %.<br>▪ TIER IV: 99.99 %. | ▪ Define las rutas de respaldo de energía eléctrica y las medidas de redundancia en el data center manteniendo el funcionamiento continuo.<br>▪ Mejoramiento de la continuidad operativa.<br>▪ Permite y garantiza la adaptación a los problemas y la continuidad ante fallos. |

*Continúa en la siguiente página*

**Continuación de la Tabla I: Estándares de seguridad para Data Centers**

| Norma / Estándar | Descripción | Clasificación / Niveles | Principales Características |
|---|---|---|---|
| hline **Norma TIA-942 (Telecommunications Infrastructure Standard for Data Centers)** | Regula el diseño, instalación y operación de infraestructura física, cableado estructurado, energía y seguridad física [41]. | ▪ Nivel 1: Básico.<br>▪ Nivel 2: Redundancia parcial.<br>▪ Nivel 3: Mantenimiento en paralelo.<br>▪ Nivel 4: Resistencia a fallos. | ▪ Existen áreas separadas que permiten el control de la temperatura.<br>▪ Organización del espacio mediante la optimización de los recursos eléctricos y de climatización sin comprometer la operación del data center.<br>▪ Mejora la protección de los equipos frente a riesgos y accesos no autorizados mejorando la seguridad y las condiciones ambientales. |

*Continúa en la siguiente página*

**Continuación de la Tabla I: Estándares de seguridad para Data Centers**

| Norma / Estándar | Descripción | Clasificación / Niveles | Principales Características |
|---|---|---|---|
| **Recomendaciones IDCA (International Data Center Authority)** | Promueve buenas prácticas internacionales en protección física y lógica, asegurando integridad, disponibilidad y confidencialidad [39]. | No se establecen niveles, se definen directrices generales. | ▪ Gestión de accesos.<br>▪ Sistema de respaldo doble.<br>▪ Planificación ante situaciones de desastre. |

Para el GAD municipal del cantón Bolívar, integrar los lineamientos de la norma TIA-942 en la evaluación ayudará a mejorar el diseño del cableado, la distribución eléctrica y la protección física, esto facilitara alinear el proyecto con los estándares internacionales de calidad para centros de datos públicos.

### 2.5.1 Normas técnicas relevantes

Las normas técnicas son esenciales para garantizar la seguridad y adecuada gestión de los Data Centers, protegiendo infraestructuras críticas. Entre las más importantes se encuentran las normas ISO/IEC 27001 y 27002, que establecen un marco integral para la gestión de la seguridad de la información en estos entornos [42].

La norma ISO/IEC 27001 establece los requisitos necesarios para implementar y optimizar un sistema de gestión de seguridad de la información (SGSI), su enfoque en la gestión de riesgos y en la aplicación de controles de seguridad resulta fundamental para proteger la información sensible en los data centers, garantizando así un proceso estructurado que refuerza la confianza de los usuarios [43].

Por su parte, la ISO/IEC 27002 complementa a la ISO/IEC 27001, proporcionando directrices para los controles específicos de seguridad, como acceso, seguridad física, gestión de incidentes y protección de la información. También aboga por la capacitación continua del personal, reduciendo riesgos derivados de errores humanos [44].

Cuando no se cuenta con sistemas de energía redundantes ni monitoreo térmico, pueden ocurrir tiempos de inactividad, altos costos y daños al hardware, en este contexto, COBIT 2019, a través del dominio APO12 - Gestión del riesgo, resalta la necesidad de tener respaldo eléctrico y monitoreo continuo para reducir estos riesgos.

## 2.6 Buenas prácticas de infraestructura tecnológica

Las buenas prácticas en la infraestructura tecnológica de un Data Center aseguran que los sistemas operen de manera eficiente, segura y confiable. Entre estas prácticas se incluyen la planificación de redundancia en sistemas de energía y refrigeración, el diseño adecuado del cableado estructurado y la implementación de controles estrictos de acceso. La adopción de normas como COBIT 2019 y las normativas ISO permite gestionar eficientemente los riesgos asociados con las infraestructuras tecnológicas.

Para el GAD Municipal del Cantón Bolívar, adoptar estas buenas prácticas es esencial para mejorar la infraestructura actual, reducir los riesgos tecnológicos y mejorar la calidad de los servicios digitales que brinda a la ciudadanía, a continuación, se presentan las prácticas más importantes.

### 2.6.1 Buenas prácticas internacionales

Las buenas prácticas internacionales se enfocan en la gestión del ciclo de vida del Data Center, desde su diseño hasta su operación continua. Estas prácticas aseguran que se implementen estrategias de seguridad eficaces, como la segmentación de redes, la autenticación multifactorial y el monitoreo constante de todos los sistemas críticos. Además, se promueve la optimización energética para minimizar el impacto ambiental y los costos operativos.

Por lo tanto, Alvarado y López [45] señalan que las principales prácticas incluyen:

- **Segmentación de red**: ayuda a segregar la red en diferentes zonas seguras y limita la propagación de amenazas en caso de ataques.
- **Verificación multifactor (MFA)**: haciendo referencia a los mecanismos de seguridad que permiten la verificación en múltiples capas, esto requiere la autenticación, reduciendo significativamente el riesgo de accesos no autorizados para acceder a los sistemas.

- **Monitoreo continuo y automático**: herramientas que permiten la supervisión constante de los sistemas tanto de anomalías o comportamientos inusuales en tiempo real, que permita la toma de decisiones de manera oportuna ante incidentes.

- **Optimización energética**: aplicación de medidas técnicas y operativas que ayudan a mantener sistemas de control climático eficientes, gestión inteligente de la energía, minimizando así el impacto ambiental así como la gestión de servidores virtuales.

El uso de estas practicas mejora el rendimiento técnico del data center,lo que asegura que el centro de datos apoyará con la transformación digital de los servicios públicos locales.

### 2.6.2 Diseño y organización del cableado

El diseño del cableado estructurado es un elemento esencial para la seguridad y el rendimiento de un Data Center, un diseño adecuado garantiza la facilidad de gestión y mantenimiento, minimiza los riesgos de interferencia electromagnética, y facilita la expansión de la infraestructura a medida que las necesidades cambian. La organización adecuada del cableado también incluye la segregación de cables de alimentación, datos y comunicaciones para mejorar la eficiencia y la seguridad.

Las mejores prácticas en este campo incluyen:

- **Planificación flexible y ampliable**: permite agregar nuevas capacidades sin tener que rehacer todo el sistema.

- **Separación física de cables**: esta práctica permite organizar los cables de energía, datos y voz, con la finalidad de reducir las interferencias entre sí.

- **Etiquetas y seguimiento**: esta práctica se utiliza con la finalidad de identificar de manera rápida y eficiente las conexiones que se encuentran en mal estado o, a su vez, en el caso de existir problemas en la red.

- **Uso de canaletas y bandejas**:esta práctica contribuye con varios beneficios dentro de ello, mantener un adecuado orden del cableado y asegurar una apropiada circulación de aire, previniendo así el sobrecalentamiento de los equipos tecnológicos.

Una infraestructura de cableado ordenada mejora no solo la seguridad, sino también la eficiencia en la gestión de incidentes y la capacidad de crecimiento tecnológico del GAD Municipal del Cantón Bolívar.

### 2.6.3 Control de acceso físico y redundancia

El control de acceso físico en un Data Center es una de las medidas más críticas para prevenir accesos no autorizados, este control se logra mediante sistemas de autenticación biométrica, tarjetas de acceso y cámaras de seguridad. Además, la redundancia es clave para asegurar la disponibilidad de los servicios; por lo tanto, se deben implementar sistemas de energía redundantes como UPS y generadores de respaldo, así como sistemas de refrigeración redundantes para evitar fallos [46].

## 2.7 Relación entre la infraestructura tecnológica, la gobernanza de TI y el cableado estructurado

La infraestructura tecnológica constituye la base operativa de los servicios de tecnología de la información en toda organización. De acuerdo con el marco COBIT 2019, su gestión se enmarca principalmente en el dominio APO03 - Gestión de la arquitectura empresarial, que establece la necesidad de alinear la infraestructura con los objetivos del negocio, garantizando seguridad, escalabilidad y eficiencia [12].

Dentro de esta infraestructura, el cableado estructurado desempeña un papel esencial al influir directamente en el rendimiento, la estabilidad y la disponibilidad de los sistemas. Un diseño adecuado permite reducir tiempos de respuesta ante fallos, minimizar interferencias electromagnéticas y facilitar el mantenimiento y la expansión de la red [40].

El marco COBIT 2019 también asocia el cableado con el dominio BAI09 - Gestión de los activos, que promueve la administración y documentación de los componentes físicos de TI, y con el dominio DSS04 - Gestión de la continuidad, el cual busca mantener la operación ante fallos en la infraestructura. Asimismo, el dominio APO12 - Gestión del riesgo enfatiza la identificación de vulnerabilidades asociadas al entorno tecnológico, incluyendo el cableado, con el fin de prevenir interrupciones del servicio [47].

Una infraestructura tecnológica bien gestionada fortalece la gobernanza de TI [48]. Al permitir decisiones basadas en información confiable, optimizando la eficiencia y seguridad organizacional, como se puede evidenciar en la Tabla II .

Tabla II.
RELACIÓN ENTRE LA INFRAESTRUCTURA TECNOLÓGICA Y LOS DOMINIOS DE COBIT 2019

| Dominio | Proceso | Descripción |
|---|---|---|
| **APO03** | Gestión de la arquitectura empresarial | Alinea la infraestructura tecnológica con los objetivos institucionales, asegurando una estructura segura, escalable y eficiente. |
| **APO12** | Gestión del riesgo | permite identificar y gestionar las vulnerabilidades en la infraestructura tecnológica, anticipándose a los incidentes que puedan interrumpir y afectar el correcto funcionamiento de las operaciones. |
| **BAI09** | Gestión de los activos | Promueve la gestión y facilita el registro de los componentes físicos, como el cableado estructurado, de acuerdo con las estrategias y estándares internacionales de TI. |
| **DSS04** | Gestión de la continuidad | Establece mecanismos para mantener la operación del sistema ante fallos o interrupciones relacionadas con la infraestructura tecnológica. |

## 2.8 Marco Referencial COBIT 2019

COBIT 2019, fue desarrollado por ISACA, este marco constituye la gobernanza y gestión de la tecnología, maximizando el valor de la información. medinate su estructura modular y adaptable que nos permite su aplicación en las diversas organizaciones públicas y privadas, generando el fortalecimiento de la seguridad, la eficiencia y el control de infraestructuras críticas como los data centers.

La versión 2019 actualiza el modelo previo incorporando principios de alineación estratégica, gestión de riesgos y optimización de recursos tecnológicos. COBIT se compone de 40 objetivos distribuidos en cinco dominios, que abarcan desde la planificación hasta la evaluación de las operaciones de TI [39].

En la Fig. 6 se representa gráficamente la relación entre los dominios y los procesos que conforman el marco COBIT 2019, mostrando su contribución al gobierno y gestión integral de TI en el GAD Municipal del Cantón Bolívar.

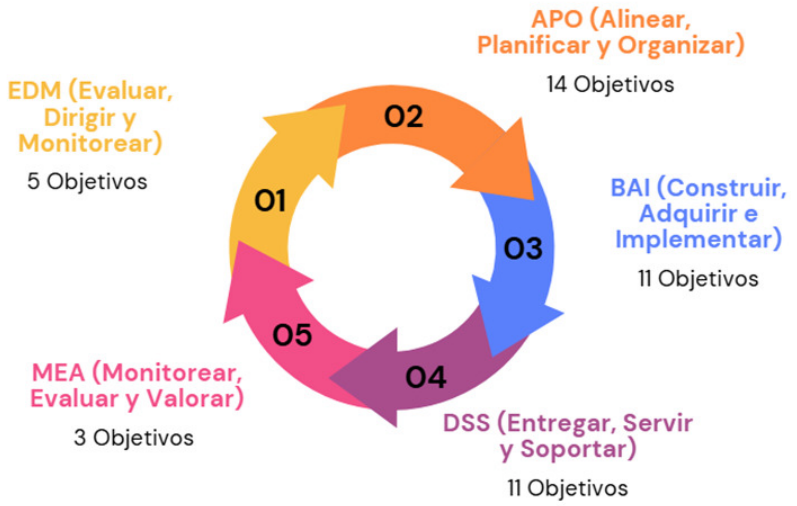


**Fig. 6**. Diagrama circular de los 5 dominios COBIT 2019 adaptado de [49]

### 2.8.1 Principios de gobernanza y gestión aplicables a la infraestructura física

En el ámbito de la infraestructura física de los Data Centers, Alvarado y López [45] señalan que los principios de COBIT 2019 que resultan relevantes incluyen:

- **Evaluación y gestión de riesgos (APO12):** permite identificar y mitigar amenazas a la infraestructura como fallas eléctricas, sobrecalentamiento o accesos no autorizados.
- **Gestión de la continuidad (DSS04):** Nos permite definir las medidas que ayudan el aseguramiento y la disponibilidad operativa ante las situaciones críticas y de vulnerabilidad.
- **Gestión de la seguridad (DSS05):** este dominio está centrado en la aplicación de controles físicos y lógicos dentro de la infraestructura, protegiendo los activos tecnológicos frente a los riesgos generados.

Estos principios permiten una gestión más sólida y proactiva, reduciendo los riesgos físicos y fortaleciendo la resiliencia del data center

### 2.8.2 Procesos COBIT 2019 relevantes para la infraestructura tecnológica

De acuerdo con el marco COBIT 2019, los procesos que se presentan a continuación resultan esenciales para la gestión eficaz de la infraestructura tecnológica [50].

Tabla III.
DOMINIOS Y PROCESOS RELEVANTES DEL MARCO COBIT 2019

| Dominio | Proceso | Descripción |
|---|---|---|
| APO03 | Gestión de la arquitectura empresarial | Alinea la infraestructura tecnológica con los objetivos organizacionales. |
| APO12 | Gestión del riesgo | Identifica, evalúa y gestiona los riesgos asociados o relacionados con la infraestructura. |
| BAI09 | Gestión de los activos | Monitorea, ayuda y mejora el uso de los recursos físicos y tecnológicos. |
| DSS01 | Gestión de operaciones | Administra las operaciones y servicios de TI para garantizar su eficiencia y continuidad. |
| DSS04 | Gestión de la continuidad | Garantiza la disponibilidad continua de los servicios críticos. |
| DSS05 | Gestión de la seguridad de los servicios | Implementa políticas de seguridad tanto físicas como lógicas. |
| EDM03 | Aseguramiento de la entrega de beneficios | Asegura que las inversiones en TI generen el valor y los beneficios esperados. |

La Tabla III detalla los procesos esenciales del marco COBIT 2019, los cuales son cruciales para la gestión eficiente de la infraestructura tecnológica en el data center del GAD municipal del cantón Bolívar, estos procesos están agrupados en distintos dominios que abordan desde la planificación y gestión del riesgo, hasta la operación, continuidad del servicio y seguridad.

Se identifican procesos destacados, por ejemplo, APO03 (gestión de la arquitectura empresarial), que busca alinear la infraestructura tecnológica con los objetivos institucionales; APO12 (gestión de riesgos), para permitir la identificación y mitigación de vulnerabilidades, y DSS04 y DSS05, para la continuidad operativa y la seguridad del servicio, respectivamente

También se incluyen el proceso DSS01, que gestiona las operaciones de TI para garantizar su eficiencia, y el proceso EDM03, que asegura que las inversiones en tecnología generen beneficios claros y estén alineadas con la estrategia institucional, esta selección de procesos proporciona un enfoque integral para mejorar la gobernanza y la seguridad del Data Center según los principios de COBIT 2019.

Implementar estos procesos relevantes en el GAD municipal del cantón Bolívar, asegurará la disponibilidad, confidencialidad e integridad de los servicios y datos municipales, lo que permitirá a la institución, tener un entorno tecnológico aceptable.

## 2.9 Trabajos relacionados

Esta sección analiza estudios recientes que están vinculados a la aplicación de marcos de gobernanza de TI en contextos institucionales públicos, particularmente COBIT 2019, donde se necesita reforzar la seguridad informática de su infraestructura tecnológica. Estos estudios apoyan la sugerencia de un plan de seguridad para el data center del GAD Municipal del cantón Bolívar, como también serán un referente tanto teórico como práctico para investigaciones posteriores.

En 2024, Oktaviana, Ferdiansyah y Pratama [51] realizaron un estudio titulado “Adopting COBIT 2019 for the Evaluation of Information Technology Risk Management in a Startup Company”, en el que aplicaron COBIT 2019 en una empresa emergente del sector turístico digital en Indonesia, su análisis se enfocó en el dominio APO12 (Gestión del Riesgo), y descubrió que el 72 % de los procesos evaluados presentaban deficiencias en los controles de riesgos tecnológicos, como resultado, se propuso una hoja de ruta que permitió mejorar el nivel de madurez de 1.3 a 2.7 en un período de seis meses, demostrando la flexibilidad del modelo COBIT 2019, incluso en organizaciones pequeñas.

De manera adicional, Sherly y Fianty [48] implementaron un proceso de evaluación de seguridad informática titulado “Information Security Evaluation of Data Centre Architecture Using COBIT 5”, que fue aplicado al centro de datos de la Universidad Islámica Estatal Syarif Hidayatullah de Yakarta, en donde pudieron identificar que el 65 % de los controles de seguridad no cumplían con los estándares mínimos, especialmente en las políticas de acceso y monitoreo. La aplicación de este marco permitió reducir en un 40 % las brechas de seguridad y mejorar en un

28 % la continuidad operativa, mediante las recomendaciones alineadas a los dominios DSS01 y DSS05.

En el caso latinoamericano, De Los Santos Guerrero (2025) desarrolló un trabajo titulado "Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana" [52], aplicando una metodología mixta que reveló un nivel de madurez promedio de 2.0 en los procesos de TI evaluados. Tras la implementación de recomendaciones basadas en COBIT 2019, se proyectó un incremento al nivel 3.5, además de una reducción estimada del 30 % en incidentes de seguridad durante auditorías internas.. La investigación concluyó que el marco permite alinear objetivos institucionales con las estrategias de TI y generar evidencia útil para auditorías futuras, lo cual es directamente comparable con el contexto del GAD Municipal del Cantón Bolívar.

Por otro lado, Alvarado [53] realizó un análisis titulado "Evaluation of IT Governance Maturity Using COBIT 2019: Case Study in IT Security Industry", en una organización especializada en ciberseguridad. El estudio mostró que el 60 % de los procesos se encontraban en nivel de madurez 1 (inicial) y un 30 % en nivel 2 (repetible). Se propuso una mejora escalonada que permitiría alcanzar nivel 4 en un horizonte de 18 meses, enfocándose en APO03 y DSS05 como pilares estratégicos.

En el contexto ecuatoriano, Ávila [54] publicó un estudio titulado "Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano". La revisión sistemática indicó que el 70 % de las instituciones públicas no contaban con planes de recuperación ante desastres, el 64 % carecían de métricas de seguridad y el 55 % no ofrecían capacitación continua al personal de TI. Estos datos reflejan un patrón estructural que también afecta al GAD del Cantón Bolívar, justificando la aplicación de un modelo como COBIT 2019 para subsanar estas brechas.

Finalmente, McIntosh y Susnjak [55] abordaron en su trabajo "From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for LLMs" la comparación entre COBIT 2019 y otros marcos frente a tecnologías emergentes como los modelos de lenguaje (LLMs). Aunque el estudio no se centró en Data Centers, se identificó que COBIT 2019 mantiene una cobertura del 80 % de los controles requeridos en entornos de alta complejidad, siendo superado sólo marginalmente por ISO 42001 en aspectos de inteligencia artificial, lo que demuestra su vigencia como marco robusto y adaptable.

En conjunto, estos trabajos evidencian que COBIT 2019 es un modelo flexible, aplicable tanto en instituciones públicas como privadas, y capaz de adaptarse a distintas realidades tecnológicas. Los hallazgos de estas investigaciones fundamentan metodológicamente la propuesta del presente estudio, orientado a mejorar la seguridad de la infraestructura del Data Center municipal mediante una estrategia alineada a estándares internacionales.

# CAPÍTULO III
# MATERIALES Y MÉTODOS

## 3.1 Metodología

La investigación se desarrolló bajo un enfoque mixto, integrando el método cuantitativo y cualitativo, el enfoque cuantitativo permitió medir, mediante listas de verificación y encuestas, el nivel de cumplimiento de los dominios definidos en COBIT 2019 en relación con la seguridad de la infraestructura del Data Center, por su parte, el enfoque cualitativo facilitó la interpretación de las condiciones observadas en el entorno físico y lógico, así como el análisis de las percepciones de los funcionarios responsables de las áreas involucradas.

## 3.2 Tipo de Investigación

El presente estudio se enmarca en la investigación científica aplicada al campo de la seguridad informática y la gestión tecnológica, su propósito es analizar la situación actual del Data Center del GAD Municipal del Cantón Bolívar y, con base en dicho diagnóstico, plantear un plan de seguridad alineado al marco referencial COBIT 2019, para lograrlo, se adoptan enfoques que permiten describir, analizar y proponer soluciones concretas, integrando tanto la observación directa de la infraestructura como la revisión de literatura especializada y estándares internacionales.

En cuanto al tipo de investigación, esta se clasifica en:

1. **Descriptiva**, al documentar y caracterizar el estado actual de la infraestructura tecnológica, física y lógica del Data Center.
2. **Aplicada**, ya que tiene como objetivo desarrollar un plan de seguridad informática que funcione como una propuesta práctica para mejorar la gestión tecnológica.
3. **Documental**: consiste en la revisión de literatura académica, normas y estándares, es decir, no se basa en experimentos ni encuestas, pero sí en la revisión y análisis de información existentes, con el objetivo de respaldar y justificar buenas prácticas de seguridad, como la implementación de COBIT 2019 en data centers.

### 3.3 Variables de investigación

Para el desarrollo de la presente investigación se establecieron las siguientes variables:

- **Variable dependiente:**
  Nivel de seguridad informática de la infraestructura tecnológica del Data Center del GAD Municipal del Cantón Bolívar.

- **Variables independientes:**
  En la Tabla IV se pueden evidenciar los dominios y procesos relevantes del marco COBIT 2019, que permiten evaluar la gestión y el control de la infraestructura tecnológica. Estos dominios son:

Tabla IV.
DOMINIOS Y PROCESOS BASADOS EN COBIT 2019

| **Dominio** | **Proceso** | **Descripción** |
|---|---|---|
| APO03 | Gestión de la arquitectura empresarial | Alinea la infraestructura tecnológica con los objetivos organizacionales. |
| DSS05 | Gestión de la seguridad de los servicios | Establece políticas de seguridad física y lógica. |

Estas variables independientes serán de ayuda para diseñar los instrumentos de recolección de información, como listas de verificación, encuestas y entrevistas, estas técnicas facilitarán una evaluación objetiva del nivel de madurez y cumplimiento de los controles de seguridad en el data center.

### 3.4 Población y muestra

La población objeto de estudio, estuvo conformada por los 200 funcionarios del GAD Municipal del Cantón Bolívar, quienes representan el universo total relacionado con la gestión y utilización de los recursos tecnológicos en la institución, para determinar el tamaño de la muestra, se utilizó la Ecuación 1 [56].

$$n = \frac{N\,Z^2\,p\,(1-p)}{e^2(N-1) + Z^2\,p\,(1-p)} \tag{1}$$

Para la presente investigación se consideraron los siguientes valores:

$$N = 200, \quad Z = 1{,}96, \quad p = 0{,}5, \quad q = 0{,}5, \quad e = 0{,}0906$$

Sustituyendo en la ecuación 1:

$$n = \frac{200 \times 1{,}96^2 \times 0{,}5 \times 0{,}5}{0{,}0906^2 \times (200 - 1) + 1{,}96^2 \times 0{,}5 \times 0{,}5}$$

$$n = \frac{200 \times 3{,}8416 \times 0{,}25}{0{,}00821 \times 199 + 0{,}9604}$$

$$n = \frac{192{,}08}{2{,}59419} = 74{,}05$$

Por tanto, el tamaño de muestra calculado es:

$$\boxed{n = 74}$$

Por lo cual, se estableció una muestra de 74 participantes, seleccionados de manera representativa desde todo el perfil administrativo de la entidad, esta cifra, atendiendo a su proporción, es suficiente para validar y fundamentar la confiabilidad del estudio.

### 3.5 Técnicas de recolección de información

Para el desarrollo de la presente investigación se aplicaron diversas técnicas de recolección de información con el fin de obtener una visión integral del estado de la gobernanza y seguridad de TI en el Data Center. Cada técnica permitió recopilar datos cualitativos y cuantitativos orientados al diagnóstico de madurez, la identificación de vulnerabilidades y la definición de las salvaguardas aplicables.

a) Entrevistas estructuradas

   Se realizaron entrevistas a responsables de las áreas técnicas y directivas del GAD municipal del cantón Bolívar, estas entrevistas facilitaron identificar el nivel de conocimiento y aplicación de las políticas de seguridad, así como las debilidades en los procesos asociados a los dominios de COBIT 2019, la información obtenida permitió analizar cómo la

institución participa en la toma de decisiones, en la distribución de recursos y en la gestión de incidentes relacionados con la seguridad.

b) Encuestas a usuarios y jefes departamentales

Se realizaron encuestas a usuarios finales y jefes departamentales, basadas en los dominios DSS04, DSS05, APO09, APO12, EDM02, MEA01 y BAI09. Las encuestas proporcionaron datos cuantitativos sobre la percepción del nivel de madurez, la continuidad de los servicios, la seguridad operativa y el nivel de capacitación del personal, los resultados fueron clave para estimar el nivel de madurez promedio (entre 1 y 2) y para identificar las brechas respecto al nivel objetivo (4).

c) Técnica del checklist

Se aplicó un checklist estructurado de control basado en los objetivos de COBIT 2019, con el fin de verificar el grado de cumplimiento de los procesos, controles y políticas establecidos en la institución, este instrumento permitió evaluar de manera práctica la existencia o ausencia de controles físicos, lógicos, administrativos y operativos en el Data Center, los ítems del checklist se agruparon de acuerdo con los dominios y procesos de COBIT 2019, y abarcaban aspectos como:

- Políticas establecidas de respaldo y continuidad (DSS04).
- Medidas que protegen físicamente el data center como controles de acceso físico, registro de visitas y sistemas de videovigilancia (DSS05).
- Monitoreo ambiental y segmentación de la red para evitar que un problema o ataque se propague (DSS01, DSS02).
- Evaluaciones regulares de riesgos y auditorías internas con la finalidad de revisar los riesgos y comprobar si la seguridad realmente funciona (APO12, MEA01).
- Registro del ciclo de vida de los activos tecnológicos, en donde se pueda saber qué equipos existen, fechas de adquisición, mantenimientos o retiros (APO09, BAI09).

El checklist se diseñó con criterios de evaluación binarios (cumple, cumple parcialmente o no cumple),lo que permitió medir el grado de implementación de cada control. Ayudó a obtener evidencia empírica y objetiva, reforzando el resultado de entrevistas y encuestas, así como proporcionando una base sólida para identificar brechas existentes.

d) Análisis técnico mediante Nmap

   Se ejecutó un escaneo de red utilizando la herramienta Nmap, con el propósito de identificar puertos abiertos, servicios expuestos y configuraciones inseguras en la infraestructura del Data Center, esta técnica permitió detectar vulnerabilidades reales en la seguridad lógica y contrastar los resultados con los obtenidos en el checklist y las entrevistas, entre los hallazgos más relevantes se encontraron servicios innecesarios activos, configuraciones por defecto y falta de segmentación de red, lo que incrementa la exposición a riesgos de intrusión.

La combinación de estas cuatro técnicas facilitaron el desarrollo de hallazgos y a la determinación del nivel de madurez de los dominios evaluados, proporcionando una visión integral para el diagnóstico, evaluación de brechas y desarrollo del plan de mejora institucional.

## 3.6 Procedimientos

Para la ejecución de la investigación se definió un conjunto de fases metodológicas que permiten llevar un control ordenado de las actividades y obtener resultados confiables.

La Fig. 7 muestra el diagrama de procediminetos planteado.

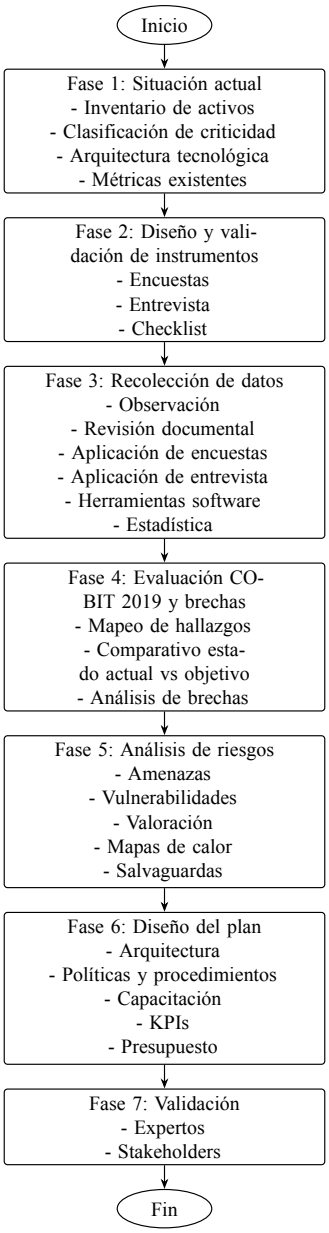


**Fig. 7**. Flujo del proceso para el desarrollo y validación del plan de seguridad

## 3.7 Fase 1: Situación Actual

### 3.7.1 Inventario de activos

Con el propósito de disponer de un control sistemático de los recursos tecnológicos, se elaboró un inventario de los equipos que conforman la infraestructura del Data Center, el inventario detalla los activos ubicados en los tres racks principales, considerando su estado actual y su importancia en la continuidad de los servicios institucionales, la Tabla V muestra el resumen de los equipos, software, bases de datos y personal técnico identificados.

Tabla V.
INVENTARIO DE ACTIVOS DEL DATA CENTER

| **Categoría / Rack** | **Activo** | **Estado** |
|---|---|---|
| **Equipos físicos** | | |
| Rack 1 | Firewall | Operativo |
| Rack 1 | Switch PoE | Operativo |
| Rack 1 | NVR (grabador de video en red) | Operativo |
| Rack 1 | CCR Internet | Operativo |
| Rack 1 | Servidor de Predios | Operativo |
| Rack 1 | CCR WiFi comunidades | Operativo |
| Rack 1 | UPS | Operativo |
| Rack 1 | UPS | Mal estado |
| Rack 1 | Servidor clon | Operativo |
| Rack 2 | Servidor clon | Operativo |
| Rack 2 | Servidor institucional | Operativo |
| Rack 3 | Switch (x2) | Operativos |
| **Software institucional** | | |
| Aplicaciones | Sistema de gestión de predios | Activo |
| Aplicaciones | Sistema contable (financiero) | Activo |
| Aplicaciones | Sistema de recursos humanos | Operativo |
| Aplicaciones | Sistema de atención ciudadana | En desarrollo |
| Aplicaciones | Herramientas ofimáticas (Microsoft 365 / LibreOffice) | Operativas |
| Aplicaciones | Antivirus institucional (ESET End-point) | Vigente |
| **Bases de datos (BDD)** | | |
| BDD 1 | Predios, Finanzas | Operativa |
| BDD 2 | Recursos Humanos | Operativa |
| BDD 3 | Atención Ciudadana | En pruebas |

*Continúa en la siguiente página*

| Categoría / Rack | Activo | Estado |
|---|---|---|
| BDD 4 | Drive institucional | Parcialmente implementado |
| **Personal técnico asignado** | | |
| Administrador de TI | Responsable de área de TI | Activo |

### 3.7.2 Clasificación de criticidad

De acuerdo con los lineamientos de COBIT 2019, los activos tecnológicos deben clasificarse en función de su impacto en la continuidad de los servicios y en la gestión de la información, la criticidad se definió como alta, media o baja, dependiendo de la función del activo en la operación institucional y su relación con los dominios evaluados (DSS, APO, BAI, EDM, MEA). La Tabla VI muestra la clasificación realizada.

Tabla VI.
INVENTARIO DE ACTIVOS CON RELACIÓN DE SERVICIO, CRITICIDAD E IMPACTO SEGÚN COBIT 2019

| Categoría | Activo | Servicio asociado | Estado | Criticidad | Impacto | Dominio COBIT 2019 |
|---|---|---|---|---|---|---|
| **Equipos físicos** | | | | | | |
| Rack 1 | Firewall principal | Protección perimetral e Internet | Operativo | Alta | Muy Alto | DSS05 |
| Rack 1 | Switch PoE | Red interna y telefonía IP | Operativo | Alta | Alto | DSS01 |
| Rack 1 | NVR (grabador de video en red) | Videovigilancia institucional | Operativo | Media | Medio | DSS05 |

*Continúa en la siguiente página*

| Categoría | Activo | Servicio asociado | Estado | Criticidad | Impacto | Dominio COBIT 2019 |
|---|---|---|---|---|---|---|
| Rack 1 | CCR Internet | Enrutamiento principal de red | Operativo | Alta | Muy Alto | DSS01 |
| Rack 1 | Servidor de Predios | Gestión catastral y de contribuyentes | Operativo | Alta | Muy Alto | BAI09 |
| Rack 1 | CCR WiFi comunidades | Conectividad comunitaria | Operativo | Alta | Alto | APO09 |
| Rack 1 | UPS 1 | Respaldo eléctrico principal | Operativo | Alta | Muy Alto | DSS01 |
| Rack 1 | UPS 2 | Respaldo eléctrico secundario | Mal estado | Alta | Muy Alto | DSS01 |
| Rack 1 | Servidor clon | Redundancia operativa (Predios) | Operativo | Media | Medio | BAI09 |
| Rack 2 | Servidor institucional | Aplicaciones internas y correo | Operativo | Alta | Muy Alto | DSS04 |
| Rack 2 | Servidor clon | Backup de aplicaciones y base de datos | Operativo | Media | Alto | DSS04 |
| Rack 2 | NAS / Almacenamiento | Copias de respaldo locales | Operativo | Alta | Muy Alto | DSS04 |
| Rack 3 | Switch (x2) | Conectividad entre racks | Operativos | Alta | Alto | DSS01 |

*Continúa en la siguiente página*

| Categoría | Activo | Servicio asociado | Estado | Criticidad | Impacto | Dominio COBIT 2019 |
|---|---|---|---|---|---|---|
| Rack 3 | Router WiFi administrativo | Acceso interno de red | Operativo | Media | Medio | DSS01 |
| Rack 3 | Aire acondicionado | Control ambiental del Data Center | Operativo | Alta | Alto | DSS01 |
| **Software institucional** | | | | | | |
| Aplicaciones | Sistema de gestión de predios | Servicio catastral | Operativo | Alta | Muy Alto | BAI09 |
| Aplicaciones | Sistema contable-financiero | Contabilidad y pagos | Operativo | Alta | Muy Alto | DSS04 |
| Aplicaciones | Sistema de RRHH | Nómina y talento humano | Operativo | Media | Alto | APO07 |
| Aplicaciones | Sistema de atención ciudadana | Trámites y solicitudes | En desarrollo | Media | Medio | DSS02 |
| Aplicaciones | Antivirus institucional | Seguridad de endpoints | Operativo | Alta | Alto | DSS05 |
| Aplicaciones | Herramientas ofimáticas | Productividad institucional | Operativo | Media | Medio | APO09 – Gestión de Activos |
| **Bases de datos (BDD)** | | | | | | |

*Continúa en la siguiente página*

| Categoría | Activo | Servicio asociado | Estado | Criticidad | Impacto | Dominio COBIT 2019 |
|---|---|---|---|---|---|---|
| BDD 1 | PostgreSQL (Predios, Finanzas) | Gestión tributaria y financiera | Operativa | Alta | Muy Alto | BAI09 |
| BDD 2 | MySQL (Recursos Humanos) | Gestión de personal | Operativa | Media | Alto | APO07 |
| BDD 3 | SQL Server Express (Atención Ciudadana) | Portal de trámites | En pruebas | Media | Medio | DSS02 |
| BDD 4 | Respaldos locales / Drive institucional | Recuperación de datos | Parcialmente operativo | Alta | Muy Alto | DSS04 |
| **Personal técnico y operativo** | | | | | | |
| Infraestructura | Administrador de sistemas | Gestión de servidores y red | Activo | Alta | Muy Alto | APO09 |
| Infraestructura | Soporte técnico | Equipos de usuario y cableado | Activo | Media | Alto | DSS01 |
| Infraestructura | Analista de sistemas | Desarrollo y mantenimiento de software | Activo | Alta | Alto | BAI09 |
| Infraestructura | Auxiliar TI | Monitoreo y documentación técnica | Activo | Media | Medio | DSS01 |

*Continúa en la siguiente página*

| Categoría | Activo | Servicio asociado | Estado | Criticidad | Impacto | Dominio COBIT 2019 |
|---|---|---|---|---|---|---|
| Infraestructura | Consultor externo | Mantenimiento de red e infraestructura | Contrato parcial | Alta | Alto | EDM02 |
| **Servicios complementarios** | | | | | | |
| Servicios externos | Conectividad ISP (Fibra Óptica) | Acceso a Internet institucional | Operativo | Alta | Muy Alto | DSS01 |
| Servicios externos | Plataforma de correo institucional | Comunicación interna y externa | Operativo | Alta | Muy Alto | DSS04 |
| Servicios externos | Servidor web institucional | Portal ciudadano | Operativo | Media | Alto | DSS02 |
| Servicios externos | Sistema de videovigilancia IP | Seguridad perimetral | Operativo | Alta | Alto | DSS05 |
| Servicios externos | Sistema de respaldo en la nube | Copias fuera del sitio | Parcial | Alta | Muy Alto | DSS04 |

### 3.7.3 Arquitectura tecnológica

La arquitectura tecnológica se estructuró de forma jerárquica, garantizando la seguridad, conectividad y disponibilidad de los servicios institucionales. En la primera capa se ubican los dispositivos de seguridad perimetral, conformados por el CCR que gestiona la conexión a Internet y el firewall, encargado de filtrar y proteger el tráfico entrante y saliente.

En la segunda capa se encuentran el router interno y el switch de distribución, responsables del enrutamiento y la conexión de los dispositivos de la red local. La tercera capa está compuesta por el servidor principal y la base de datos, respaldados por un sistema UPS que asegura continuidad eléctrica ante fallos.

Los equipos terminales PCs, cámaras IP, NVR, forman parte de la cuarta capa que ayuda a gestionar y almacenar sistemas de videovigilancia, y los usuarios acceden a los servicios de la red.

La Fig. 8 muestra la arquitectura tecnológica definida para el Data Center.

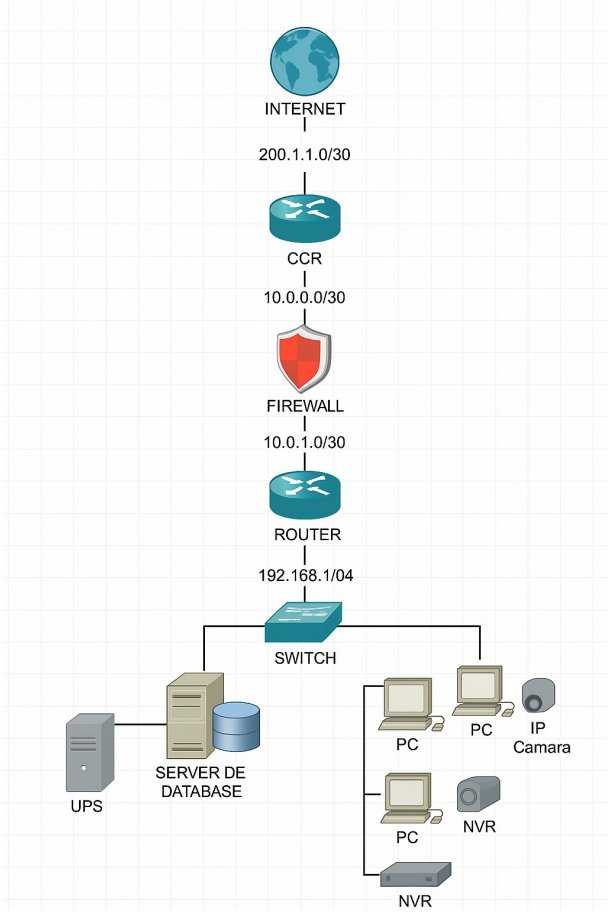


**Fig. 8**. Arquitectura tecnológica del Data Center

## Diagramas de red

El diseño de red del Data Center sigue una topología en estrella extendida, donde los switches PoE actúan como nodos de distribución hacia los servidores y dispositivos finales, el firewall se ubica como punto de control perimetral, gestionando el tráfico entrante y saliente, mientras que el CCR Internet establece la comunicación con el proveedor ISP mediante fibra óptica, el CCR

WiFi brinda conectividad inalámbrica a usuarios internos y puntos comunitarios, manteniendo segmentación lógica por VLAN para separar las redes administrativas, públicas y de servicios.

El diagrama de red incluye los siguientes elementos y se ilustran en la Fig.9:

- Cortafuegos perimetral con políticas de filtrado y traducción de direcciones de red (NAT).
- Enrutador CCR (equipo central de la red) para gestionar el control de tráfico y balanceo de carga de datos.
- Conmutadores PoE switches de acceso con enlaces troncales conectados a los racks, los mismos que proporcionan conectividad a los dispositivos finales.
- La infraestructura consta con servidores virtualizados distribuidos asignados en diferentes áreas como (Predios, Contabilidad, RRHH, Clones).
- Utiliza medios físicos de transmisión de datos como conexiones de fibra óptica y cables UTP categoría 5e.

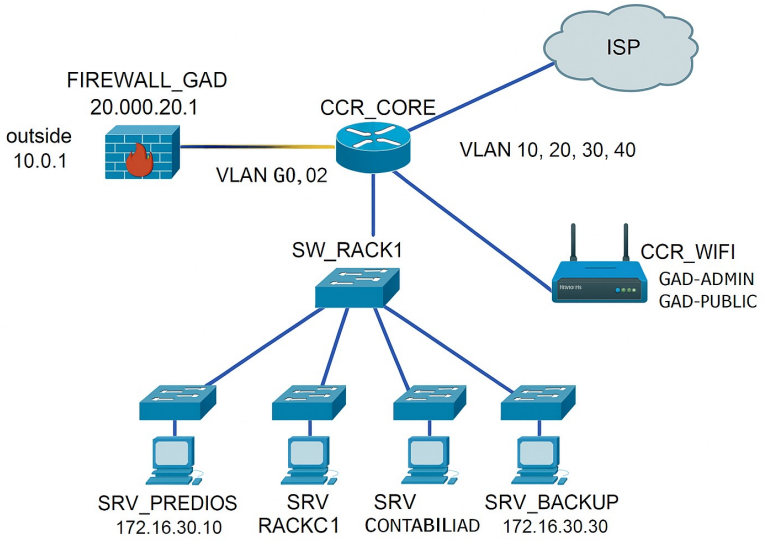


**Fig. 9**. Diagrama de red del Data Center con topología en estrella extendida y segmentación VLAN

### Planos de racks

El Data Center del GAD Municipal del Cantón Bolívar presenta actualmente una disposición física que no cumple con las condiciones óptimas de operación ni con las recomendaciones técnicas para entornos de misión crítica, la distribución del equipamiento en los racks carece de criterios de seguridad, ventilación y ordenamiento estructurado, lo que genera sobrecalentamiento, dificultad para el mantenimiento y vulnerabilidad ante fallas eléctricas o físicas.

Se identificaron varias deficiencias durante la inspección técnica de la infraestructura tecnológica, entre ellas tenemos, la falta de un sistema de climatización adecuado, los problemas en la gestión de cables, el uso ineficiente del espacio y la ausencia de controles de acceso físico, como consecuencia estas condiciones aumentan el riesgo de interrupciones en los servicios institucionales, la pérdida de información sensible y la disminución de la capacidad de rendimiento de los equipos tecnológicos.

En la Fig.10, se muestra y reporta la disposición actual de los racks de la siguiente manera:

- **Rack 1:** Incluye el firewall, el CCR principal, el NVR y un UPS. El equipo está diseñado sin un flujo de aire adecuado ni separación entre donde corre la energía y los datos, lo que crea una falta de circulación de aire y aumenta la temperatura interna.
- **Rack 2:** Contiene dos servidores 01 institucionales y 01 clon, conectados a un UPS secundario, sin mantenimiento de servicio, acumulación de polvo y el sistema de energía de respaldo deficiente que presenta un riesgo de interrupción para servicios cruciales.
- **Rack 3:** Aloja los switches de interconexión y el router WiFi, el cableado presnenta cruces entre líneas de datos y electricidad, no tiene bandejas para cables ni tampoco está etiquetado, lo que hace que el diagnóstico sea una pesadilla en caso de fallos o cortes.

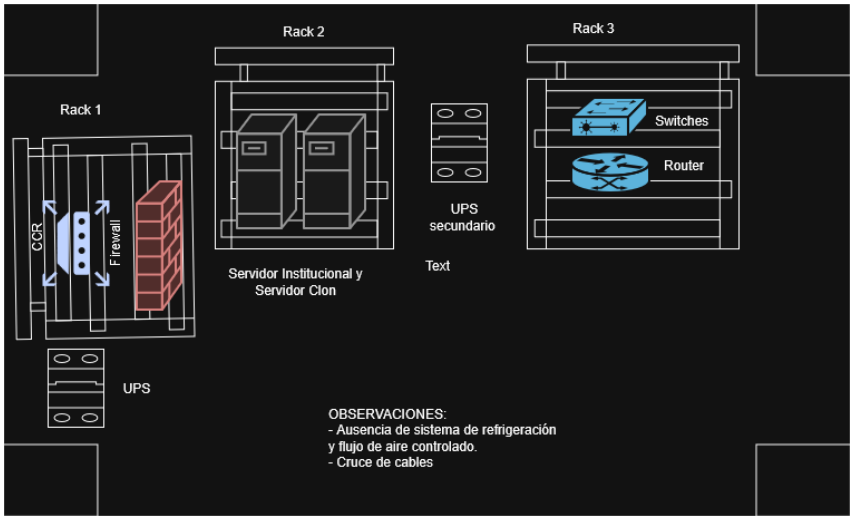


**Fig. 10**. Plano actual de racks del Data Center del GAD Municipal del Cantón Bolívar

En conjunto, la infraestructura refleja un estado de desorganización que afecta la estabilidad y confiabilidad del sistema de TI municipal, no se dispone de planos técnicos actualizados ni de un esquema documentado de interconexión entre racks, lo cual impide una gestión eficiente del mantenimiento y una adecuada respuesta ante incidentes.

**Rutas de cableado**

El Data Center del GAD carece de un sistema de cableado estructurado formalmente diseñado y administrado, en la actualidad, el tendido de cables se realiza de forma empírica, sin esquemas de distribución definidos ni documentación técnica que respalde la infraestructura existente, se evidencian conexiones improvisadas, cruces entre cableado eléctrico y de datos, ausencia de canaletas, desorganización en los racks y falta de rotulación que permita identificar los puntos de red o las rutas de conexión.

Esta situación refleja una gestión reactiva y no planificada de los recursos tecnológicos, generando vulnerabilidades operativas que impactan la disponibilidad y confiabilidad de los servicios de TI, bajo el enfoque de COBIT 2019, este escenario evidencia un nivel de madurez bajo en los procesos asociados a la gestión de activos de TI (BAI09) y la operación de servicios (DSS01), ya que no existe un control efectivo sobre la infraestructura física que soporte los servicios críticos.

**Zonas de acceso**

El Data Center del GAD cuenta con tres zonas definidas que estructuran el control físico y operativo de la infraestructura tecnológica, estas áreas se distribuyen de manera funcional para facilitar la gestión, seguridad y supervisión de los activos críticos, aunque aún requieren fortalecer sus mecanismos de control, monitoreo y trazabilidad conforme a los procesos del marco COBIT 2019, principalmente en los dominios DSS05 (Seguridad de los Servicios) y DSS01 (Operación de los Servicios

En la Fig.11 se ilustra la distribución actual por zonas que presenta el GAD.


**Fig. 11**. Zonas de acceso del Data Center del GAD Municipal del Cantón Bolívar

**Zona 1 – Seguridad Perimetral:** Corresponde al área de acceso controlado que delimita físicamente el entorno del Data Center, cuenta con cámaras de seguridad y cerraduras que restringen el ingreso únicamente a personal autorizado,no obstante, el sistema de videovigilancia necesita mejoras en su cobertura y almacenamiento de grabaciones, además de la implementación de registros automáticos de acceso para asegurar la trazabilidad y el respaldo ante incidentes.

**Zona 2 – Área Técnica:** En esta zona se concentran los racks, servidores principales, sistemas de comunicación y equipos de respaldo energético, el acceso se encuentra limitado al

personal del área de Tecnologías de la Información (TI), no obstante, se requiere una mejor organización interna del cableado estructurado, delimitación de rutas eléctricas y de datos, y un sistema de monitoreo ambiental (temperatura, humedad y energía) que asegure la continuidad operativa y reduzca el riesgo de fallos físicos.

**Zona 3 – Oficina Administrativa y de Monitoreo TI:**Está asignada a la gestión operativa y control administrativo del Data Center, desde este espacio se realizan las tareas de supervisión, soporte técnico y monitoreo general,en la actualidad no dispone de un sistema de control integral de cámaras, alarmas y registros de acceso físico, lo que limita la capacidad de respuesta ante eventos y la aplicación de procedimientos correctivos oportunos.

En conjunto, la definición de estas zonas constituye un avance significativo en la gestión física del Data Center, pero aún se requiere implementar controles automatizados, políticas documentadas y mecanismos de supervisión continua, para alcanzar un nivel de madurez óptimo en la seguridad de servicios (DSS05) y en la operación eficiente de la infraestructura tecnológica (DSS01) establecidos en COBIT 2019.

### 3.7.4 Métricas existentes

Se identificaron las métricas disponibles en la infraestructura tecnológica, considerando los registros de operación, continuidad y seguridad de los servicios, estas métricas se relacionaron con los dominios de COBIT 2019, permitiendo evidenciar cuáles se encuentran implementadas, cuáles son parciales y cuáles no se gestionan, la Tabla VII presenta el detalle de las métricas levantadas en el Data Center.

Tabla VII.
MÉTRICAS EXISTENTES EN LA INFRAESTRUCTURA DEL DATA CENTER

| **Dominio COBIT 2019** | **Métrica identificada** | **Fuente de información** | **Estado** |
|---|---|---|---|
| DSS01 – Operaciones | Tiempo promedio de resolución de incidentes | Reportes de soporte técnico | Medido parcialmente |
| DSS04 – Continuidad | Porcentaje de respaldos realizados | Logs de servidor de backup | Medido |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Métrica identificada | Fuente de información | Estado |
|---|---|---|---|
| DSS05 – Seguridad de Servicios | Registros de intentos de acceso | Logs de firewall y CCR Internet | Medido |
| APO12 – Gestión de Riesgos | Número de evaluaciones de riesgos anuales | Informes de auditoría interna | Limitado |
| MEA01 – Monitoreo y Evaluación | Auditorías de cumplimiento normativo | Documentos institucionales | No medido |

## 3.8 Fase 2: Diseño y validación de instrumentos

### 3.8.1 Encuesta

Con el objetivo de evaluar la madurez de los procesos de gobernanza y gestión de TI en el GAD Municipal del Cantón Bolívar, se aplicó una encuesta dirigida a los jefes departamentales y usuarios, el instrumento estuvo basado en el marco de referencia COBIT 2019, [12].

Se consideraron los dominios DSS05 (Seguridad de Servicios), DSS02 (Gestión de Incidentes), BAI09 (Gestión de Activos), APO09 (Gestión de Activos y Configuración), DSS01 (Gestión de Operaciones), DSS04 (Continuidad y Disponibilidad), APO12 (Gestión de Riesgos), EDM02 (Asegurar Beneficios), APO07 (Gestión de Recursos Humanos de TI) y MEA01 (Monitorear, Evaluar y Valorar Rendimiento y Conformidad), estos dominios permiten evaluar de manera integral la infraestructura, la gestión de incidentes, la continuidad operativa, la administración de riesgos, la gestión de activos, el aseguramiento de beneficios y la conformidad con estándares de seguridad.

Para cada cuestionario se utilizó una escala de tipo Likert de cinco niveles, que permite medir el grado de implementación de cada práctica como se puede ilustrar en la Tabla VIII, la escala de 0 a 5 se basa en el modelo de capacidad de COBIT 2019 [12], que permite medir el nivel de madurez de los procesos de TI, evaluando desde un proceso incompleto (0) hasta uno optimizado (5), esto facilita identificar el estado actual, las brechas existentes y las oportunidades de mejora en la gestión del data center.

Tabla VIII.
NIVELES DE MADUREZ SEGÚN COBIT 2019

| Nivel | Descripción |
|---|---|
| 0 – Incompleto o desconoce | El proceso no alcanza su propósito ni está implementado. |
| 1 – Realizado | El proceso se ejecuta, pero sin control formal ni consistencia. |
| 2 – Gestionado | El proceso está planificado, monitoreado y ajustado cuando es necesario. |
| 3 – Establecido | El proceso sigue procedimientos documentados y se implementa consistentemente. |
| 4 – Predecible | El proceso se mide y es capaz de alcanzar resultados esperados con estabilidad. |
| 5 – Optimizado | El proceso se mejora continuamente basado en datos y análisis de desempeño. |

La encuesta dirigida a los jefes departamentales tuvo como objetivo evaluar el nivel de cumplimiento de los procesos críticos de seguridad informática y gestión del Data Center en relación con los dominios de COBIT 2019, de forma complementaria, se aplicó una encuesta al área de Tecnologías de la Información (TI), con la finalidad de obtener la visión técnica respecto a la implementación de controles, el monitoreo de servicios y la gestión de riesgos.

En la Tabla IX, se detalla el cuestionario de la evaluación de madurez de los controles aplicado a los jefes departamentales del GAD Municipal del Cantón Bolívar basado en COBIT 2019
.

Tabla IX.
CUESTIONARIO DE EVALUACIÓN DE MADUREZ DE CONTROLES EN EL DATA CENTER BASADO EN COBIT 2019

| N° | Dominio COBIT 2019 | Pregunta | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|
| 1 | DSS05 (Seguridad de Servicios) | El Data Center cuenta con controles adecuados de acceso físico (biometría, tarjetas, cámaras) para restringir el ingreso de personal no autorizado. | | | | | | |
| 2 | DSS02 (Gestión de Incidentes) | Existe una política documentada de gestión de incidentes de seguridad informática en la infraestructura del Data Center. | | | | | | |
| 3 | BAI09 (Gestión de Activos) | La infraestructura eléctrica del Data Center dispone de redundancia (UPS, generadores) que aseguran continuidad del servicio. | | | | | | |
| 4 | APO09 (Gestión de Activos y Configuración) | El cableado estructurado se encuentra organizado, identificado y con mantenimiento preventivo documentado. | | | | | | |
| 5 | DSS01 (Gestión de Operaciones) | La organización realiza monitoreo ambiental (temperatura, humedad, humo, inundación) en tiempo real en el Data Center. | | | | | | |
| 6 | DSS04 (Continuidad y Disponibilidad) | Se cuentan con procedimientos de respaldo y recuperación de información críticos que se prueban de forma regular. | | | | | | |
| 7 | APO12 (Gestión de Riesgos) | Se realizan evaluaciones de riesgos periódicas sobre la seguridad de la infraestructura del Data Center. | | | | | | |
| 8 | EDM02 (Asegurar Beneficios) | La alta dirección aprueba y financia iniciativas de mejora en la seguridad del Data Center. | | | | | | |

Tabla IX.
CUESTIONARIO DE EVALUACIÓN DE MADUREZ DE CONTROLES EN EL DATA CENTER BASADO EN COBIT 2019 (CONTINUACIÓN)

| N° | Dominio COBIT 2019 | Pregunta | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|
| 9 | APO07 (Gestión de Recursos Humanos de TI) | Los usuarios y técnicos reciben capacitaciones regulares en seguridad informática. | | | | | | |
| 10 | MEA01 (Monitorear y Evaluar Rendimiento y Conformidad) | El Data Center cuenta con un plan documentado de mejora continua alineado a COBIT 2019. | | | | | | |

La encuesta aplicada a los usuarios permitió analizar la percepción general sobre la disponibilidad, continuidad y seguridad de los servicios, mientras que la encuesta aplicada al personal del departamento de TI proporcionó información detallada sobre la aplicación real de procedimientos, controles y políticas, esta doble perspectiva asegura una visión integral del estado de la gobernanza tecnológica, contrastando tanto la experiencia de uso como la gestión técnica.

En la Tabla X, se detalla el cuestionario de la evaluación de madurez de los controles aplicado a los usuarios de servicios que ofrece GAD Municipal del Cantón Bolívar basado en COBIT 2019 .

Tabla X.
CUESTIONARIO DE EVALUACIÓN DE MADUREZ DE CONTROLES EN EL DATA CENTER BASADO EN COBIT 2019 – DOMINIO DSS04

| N° | Dominio COBIT 2019 | Pregunta | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|
| 1 | DSS04 (Gestión de la continuidad) | ¿Los servicios que usted utiliza (ejemplo: sistema de recaudación, sitio web, trámites en línea) han estado disponibles de manera continua durante el último semestre? | | | | | | |

Tabla X.
CUESTIONARIO DE EVALUACIÓN DE MADUREZ DE CONTROLES EN EL DATA CENTER BASADO EN COBIT 2019 – DOMINIO DSS04 (CONTINUACIÓN)

| N° | Dominio COBIT 2019 | Pregunta | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|
| 2 | DSS04 (Gestión de la continuidad) | ¿Ha recibido notificaciones claras y oportunas cuando los sistemas no están funcionando o cuando se programan mantenimientos? | | | | | | |
| 3 | DSS04 (Gestión de la continuidad) | Cuando ocurre una caída de los servicios, ¿el tiempo de recuperación le parece adecuado para garantizar la continuidad de sus actividades? | | | | | | |
| 4 | DSS04 (Gestión de la continuidad) | ¿Cuenta con canales claros y accesibles para reportar incidentes de disponibilidad de los servicios? | | | | | | |
| 5 | DSS04 (Gestión de la continuidad) | ¿Cómo calificaría la calidad de la atención que recibe del área de informática (TI) cuando necesita apoyo? | | | | | | |

### 3.8.2 Entrevista

Con el propósito de complementar el análisis realizado a través de las encuestas aplicadas a la Gobernanza y a los usuarios del Data Center, se diseñó y aplicó una entrevista semiestructurada dirigida exclusivamente al Departamento de TI del GAD Municipal del Cantón Bolívar.

La entrevista se basa en el marco COBIT 2019 [12], que es una guía reconocida internacionalmente para la gobernanza y gestión de la tecnología de la información. La entrevista está particularmente dirigida a los dominios más relevantes para asegurar la seguridad y continuidad de la infraestructura tecnológica.

A continuación, se presentan los dominios COBIT 2019 considerados y las preguntas formuladas en la entrevista aplicada, las cuales se detallan en la Tabla XI.

Tabla XI.
DOMINIOS Y PREGUNTAS APLICADAS EN LA ENTREVISTA AL DEPARTAMENTO DE TI

| Dominio COBIT 2019 | Tema principal | Preguntas aplicadas |
|---|---|---|
| EDM02 – Asegurar beneficios | Gobernanza y soporte organizacional | ¿Cuál es el nivel de participación de la alta dirección en la definición de políticas de seguridad del Data Center?<br>¿Existen roles claramente definidos en cuanto a la gestión de la infraestructura? |
| DSS05 – Seguridad de servicios | Seguridad física y lógica | ¿Qué mecanismos de control de acceso físico existen actualmente?<br>¿Qué medidas de seguridad lógica, como firewalls, segmentación de red e IDS/IPS, protegen la infraestructura? |
| DSS04 – Continuidad y disponibilidad | Continuidad operativa | ¿Qué estrategias se implementan para asegurar la disponibilidad constante de los servicios del data center?<br>¿Se realizan simulacros o pruebas de contingencia documentadas? |
| APO12 – Gestión de riesgos | Riesgos y cumplimiento | ¿Con qué frecuencia realizan análisis de riesgos sobre la infraestructura?<br>¿Cómo aseguran el cumplimiento de normativas o buenas prácticas como ISO 27001 o COBIT? |
| MEA01 – Monitoreo y evaluación | Retos y mejoras | ¿Cuáles son los principales desafíos que enfrenta actualmente la seguridad del Data Center?<br>¿Qué proyectos de mejora priorizaría a corto plazo? |

Como se muestra en la Tabla XI, los dominios seleccionados del marco COBIT 2019 se utilizaron como base para formular las preguntas de la entrevista dirigida al Departamento de TI, esta relación permitió obtener información detallada sobre cómo se aplican los procesos de seguridad, continuidad, gobernanza y gestión de riesgos en el Data Center, lo que ayudó a identificar brechas y oportunidades de mejora, estos hallazgos fueron fundamentales para el diseño del plan de seguridad informática.

### 3.8.3 Checklist de COBIT 2019

Para la evaluación de los controles se elaboró un checklist de cumplimiento basado en el marco de referencia COBIT 2019, este instrumento permitió verificar, mediante evidencia directa, el grado de implementación de los controles asociados a los dominios evaluados, la información fue recopilada a partir de la entrevista técnica aplicada al jefe del Departamento de TI, la cual proporcionó los insumos necesarios para calificar cada control según su estado y evidencia.

El sistema de evaluación se apoyó en una escala de símbolos que facilita la interpretación de los resultados, representando tres niveles de cumplimiento: Cumple , Parcialmente cumple y No cumple. Cada símbolo está asociado a un estado operativo del control y a la evidencia encontrada, como se detalla en la Tabla XII.

Tabla XII.
INTERPRETACIÓN DE SÍMBOLOS DE CUMPLIMIENTO CON ESTADO Y EVIDENCIA

| Símbolo | Significado | Descripción | Estado del control | Evidencia |
|---|---|---|---|---|
| ✓ | Cumple | El control está implementado en su totalidad y cumple los criterios de COBIT 2019. | Implementado | Documentación técnica, políticas o reportes de verificación. |

Continúa en la siguiente página

Tabla XII (continuación)

| Símbolo | Significado | Descripción | Estado del control | Evidencia |
|---|---|---|---|---|
| ~ | Parcialmente cumple | El control existe, pero su aplicación es irregular o no cuenta con respaldo documental completo. | En implementación | Evidencia parcial: entrevistas o registros incompletos. |
| × | No cumple | El control no está implementado o no se hallaron evidencias que respalden su efectividad. | No implementado | No existe documentación ni práctica verificable. |

Posteriormente, se aplicó el checklist de evaluación, el cual permitió clasificar el cumplimiento de los controles definidos en cada dominio COBIT 2019, la Tabla XIII presenta los resultados del instrumento, indicando el control evaluado, el criterio de revisión y el nivel de cumplimiento observado.

Tabla XIII.
CHECKLIST DE EVALUACIÓN ADAPTADO A COBIT 2019

| Dominio COBIT 2019 | Control evaluado | Criterio de evaluación | Cumplimiento |
|---|---|---|---|
| DSS05 – Seguridad de Servicios | Control de acceso físico | Puertas de seguridad, tarjetas de proximidad, cámaras CCTV, registro de accesos. | ✓/ ~/ × |

Continúa en la siguiente página

Tabla XIII (continuación)

| Dominio COBIT 2019 | Control evaluado | Criterio de evaluación | Cumplimiento |
|---|---|---|---|
| DSS01 – Operaciones | Monitoreo ambiental | Sensores para temperatura, humedad y alarmas en caso de fallos eléctricos o térmicos. | ✓/ ~/ × |
| DSS04 – Continuidad y Disponibilidad | Plan de respaldo y recuperación | Respaldos automáticos y pruebas regulares de restauración. | ✓/ ~/ × |
| APO09 – Gestión de Activos | Inventario de equipos tecnológicos | Catálogo actualizado y organizado de todos los dispositivos. | ✓/ ~/ × |
| APO12 – Gestión de Riesgos | Evaluación periódica de riesgos | Planes de mitigación y seguimiento de vulnerabilidades. | ✓/ ~/ × |
| EDM02 – Asegurar Beneficios | Involucramiento de la alta dirección | Políticas aprobadas y presupuesto asignado. | ✓/ ~/ × |
| MEA01 – Monitoreo y Evaluación | Auditorías internas y revisiones | Informes con hallazgos y acciones correctivas registradas. | ✓/ ~/ × |

Como se observa en la Tabla XIII, los controles evaluados permitieron determinar el nivel de cumplimiento técnico de la infraestructura del Data Center, estos resultados servirán posteriormente como insumo para el análisis de brechas y la formulación de mejoras en las fases siguientes del proyecto.

# CAPÍTULO IV
# RESULTADOS Y ANÁLISIS

## 4.1 Recolección de datos

La recolección de información se realizó mediante la aplicación de las técnicas de observación directa, revisión documental, entrevista y encuestas dirigidas a los actores clave del área de Tecnologías de la Información (TI), como también herramientas de software NMAP, estas técnicas y herramientas permitieron obtener evidencia tanto cualitativa como cuantitativa sobre el estado actual de la seguridad informática, la gestión de riesgos, la disponibilidad de servicios y el cumplimiento de los dominios establecidos por COBIT 2019.

### 4.1.1 Observación directa

Durante la observación realizada en la infraestructura del Data Center del GAD Municipal del Cantón Bolívar, se identificó la ausencia de políticas formales de seguridad informática que regulen el uso, gestión y mantenimiento de los activos tecnológicos. Esta falta de normativas ha generado que las actividades relacionadas con el acceso, operación y protección de la infraestructura se lleven a cabo de manera empírica, dependiendo únicamente de la experiencia del personal y no de lineamientos estandarizados.

A continuación, se presentan los hallazgos principales registrados durante la observación:

- No se evidenció la existencia de un plan formal de respaldo y recuperación de la información (Dominio DSS04).
- El 80 % de los equipos tecnológicos no tienen etiquetas de identificación y no se encuentran actualizados en el inventario de activos (Dominio APO09).
- No existen controles documentados sobre el acceso físico al Data Center; el ingreso depende exclusivamente del personal presente (Dominio DSS05).
- Se detectó la ausencia de un monitoreo ambiental automatizado; las verificaciones se realizan de forma manual (Dominio DSS01).

- No se encontró evidencia de evaluaciones de riesgos periódicas ni matrices actualizadas (Dominio APO12).

A continuación en la Fig.12, se presenta un gráfico que ilustra los porcentajes de cumplimiento correspondientes a cada uno de los hallazgos:

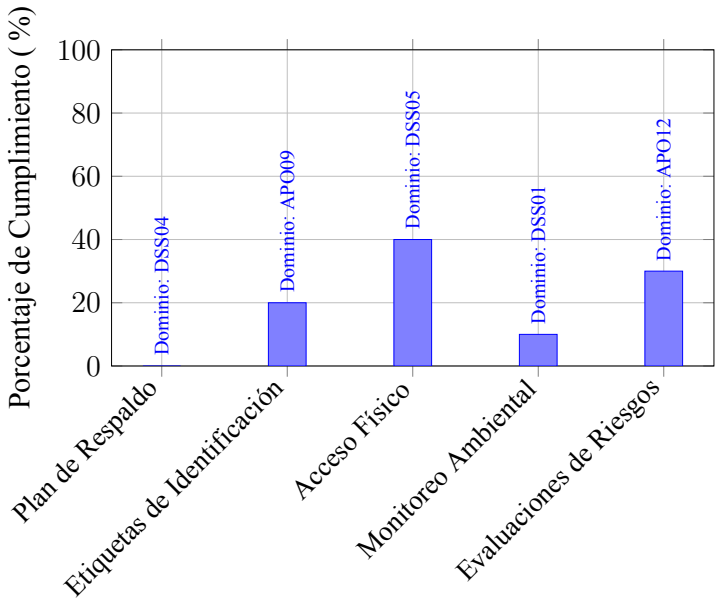


**Fig. 12**. Gráfico de barras de los hallazgos principales encontrados durante la observación en la infraestructura del Data Center

Los resultados observacionales se correlacionan con los valores obtenidos del checklist de COBIT 2019, como se puede evidenciar en la Tabla XIII. En dicha tabla, la mayoría de los controles se calificaron como parcialmente cumplidos (~) o no cumplidos (×), lo cual refuerza la conclusión de que el Data Center carece de políticas formales y de mecanismos sistemáticos de seguimiento.

La falta de políticas formales implica diversos riesgos, tales como: la falta de control sobre los accesos físicos y lógicos, una mayor exposición a incidentes de seguridad derivados de errores humanos, una organización deficiente del cableado y los equipos, y dificultades para realizar un seguimiento adecuado de las acciones realizadas sobre los sistemas críticos.

### 4.1.2 Revisión documental

En la revisión documental se constató que la institución carece de normativas, manuales o procedimientos escritos que sustenten la seguridad y el manejo adecuado del Data Center, no se

hallaron registros de auditorías internas ni informes de monitoreo ambiental, lo que refleja una madurez organizacional baja en relación con los criterios del marco COBIT 2019.

Los principales resultados obtenidos mediante esta técnica fueron los siguientes:

- Se verificó la inexistencia de políticas de respaldo y continuidad de servicios formalmente aprobadas (DSS04).
- No se encontró un inventario digital completo de los activos tecnológicos ni documentación actualizada sobre las mejoras realizadas (APO09).
- No se han registrado actas ni informes de evaluación de riesgos (APO12).
- No se encontraron auditorías internas o externas ni documentos relacionados con los dominios MEA01 o DSS05 en los últimos 24 meses.
- Se comprobó y evidenció la ausencia de reuniones o informes ejecutivos relacionados con el aseguramiento de beneficios (EDM02).

A continuación en la Fig.13, se presenta el gráfico combinado que ilustra los resultados observacionales de los hallazgos por dominio de COBIT 2019:

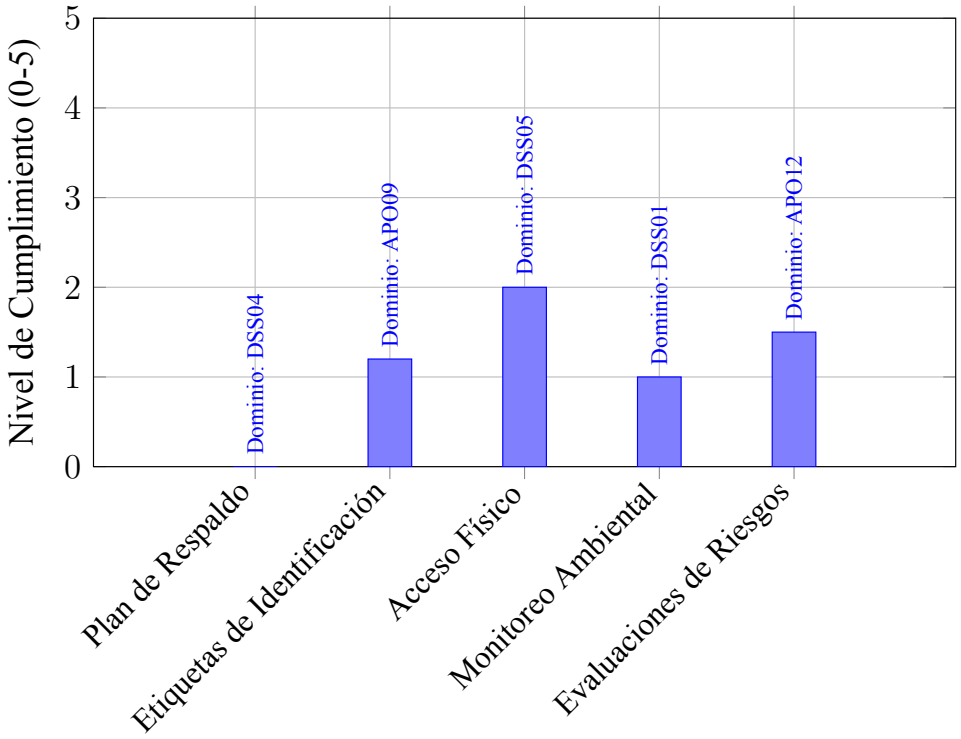


**Fig. 13**. Gráfico combinado de los hallazgos principales por dominio de COBIT 2019, evidenciando un nivel de madurez promedio estimado de 1.2 sobre 5 (nivel Realizado")

Esta situación refleja debilidades en la gestión institucional, ya que sin políticas claras no se establecen responsabilidades, ni se definen planes de contingencia o estrategias de continuidad de servicios. en consecuencia, la capacidad del GAD Municipal del Cantón Bolívar para cumplir con los estándares internacionales definidos por COBIT 2019 es limitada, evidenciando un nivel de madurez promedio estimado de 1.2 sobre 5 (nivel "Realizado").

### 4.1.3 Aplicación de Encuestas

**Resultados de la aplicación de encuesta dirigida a los jefes departamentales del GAD Municipal del Cantón Bolívar**

Los resultados se agruparon por dominio COBIT 2019, como se puede evidenciar en la Tabla IX, calculando el promedio de las respuestas obtenidas en cada uno de ellos, la media refleja el nivel de madurez percibido por los encuestados, permitiendo identificar las áreas críticas que requieren mayor atención y aquellas en las que se presentan avances más significativos.

En la Tabla XIV se muestran los promedios alcanzados en cada dominio evaluado, lo que constituye una visión general del estado de madurez institucional desde la perspectiva de los responsables departamentales.

Tabla XIV.
PROMEDIO DE MADUREZ POR DOMINIO COBIT 2019 EN ENCUESTA A JEFES DEPARTAMENTALES, BASADO EN COBIT 2019

| **Dominio COBIT 2019** | **Promedio (0–5)** |
|---|---|
| DSS05 – Seguridad de Servicios | 1.40 |
| DSS02 – Gestión de Incidentes | 0.92 |
| APO12 – Gestión de Riesgos | 0.92 |
| DSS04 – Continuidad y Disponibilidad | 1.21 |
| APO09 – Gestión de Activos | 1.69 |
| DSS01 – Operaciones | 0.46 |
| EDM02 – Asegurar Beneficios | 1.23 |

Tabla XIV.
PROMEDIO DE MADUREZ POR DOMINIO COBIT 2019 EN ENCUESTA A JEFES DEPARTAMENTALES (CONTINUACIÓN)

| **Dominio COBIT 2019** | **Promedio (0–5)** |
|---|---|
| APO07 – Gestión del Personal | 0.93 |
| BAI09 – Gestión de Activos | 0.85 |
| MEA01 – Monitoreo y Evaluación | 1.50 |

Los resultados de la encuesta aplicada a los jefes departamentales, como se puede observar en la Tabla XIV, muestran diferentes niveles de madurez en los dominios de COBIT 2019. A continuación, se detallan los hallazgos más relevantes:

1. DSS05 – Seguridad de Servicios (1.40): bajo nivel de implementación de controles, con mecanismos básicos pero sin un monitoreo constante de la infraestructura crítica.
2. DSS02 – Gestión de Incidentes (0.92): Se encontró que ocurrieron deficiencias significativas debido a que no se establecieron procedimientos definidos para identificar, analizar y responder a los incidentes.
3. APO12 – Gestión de Riesgos (0.92): El GAD no realiza evaluaciones de riesgo de forma periódica, ni mucho menos cuenta con regulaciones formales, lo que condiciona y limita la capacidad de anticiparse y responder ante futuras amenazas y vulnerabilidades.
4. DSS04 – Continuidad y Disponibilidad (1.21): Existen planes de respaldo y recuperación parciales, es decir, no se prueban regularmente, además, no se realizan simulacros de manera periódica para evaluar la efectividad ante fallos reales.
5. APO09 – Gestión de Activos (1.69): uno de los dominios con mejor valoración, destacándose por un mayor orden en la administración de activos, aunque persisten dificultades en la documentación y control del ciclo de vida.
6. DSS01 – Operaciones (0.46): El dominio más débil con el peor resultado en la evaluación, por la escasez de controles ambientales (temperatura, humedad, energía) acompañado de la falta de procedimientos claros en la supervisión diaria de las operaciones.

7. EDM02 – Asegurar Beneficios (1.23): Se evidencia la falta de compromiso y participación por parte de los directivos o directores con la gobernanza de TI, lo que afecta negativamente entre la alineación estratégica de TI con los los objetivos estratégicos de la institución.

8. APO07 – Gestión del Personal (0.93): baja capacitación y concienciación en seguridad informática, lo que representa un riesgo humano importante para la continuidad de los servicios.

9. BAI09 – Gestión de Activos (0.85): Los procesos de adquisición y mantenimientos presentan fallos, como consecuencia de la falta de control sobre el ciclo de vida de los activos tecnológicos.

10. MEA01 – Monitoreo y Evaluación (1.50): Es uno de los dominios mejor calificados, sin embargo, aún asi resulta necesario contar con un sistema sólido de mejora continua.

**Resultados de la aplicación de encuesta dirigida a los usuarios de servicios del GAD Municipal del Cantón Bolívar**

Como se observa en la Tabla XV, los datos obtenidos reflejan que, si bien los usuarios perciben una disponibilidad aceptable en algunos aspectos, como la atención proporcionada por el área de TI, aún existen limitaciones en elementos críticos. Entre estos se incluyen la comunicación oportuna de incidentes y el tiempo de recuperación ante caídas. Los resultados presentados en esta tabla constituyen la base para su análisis.

Tabla XV.
PROMEDIO DE RESPUESTAS POR PREGUNTA – DOMINIO DSS04

| **Pregunta** | **Promedio** |
|---|---|
| 1. ¿Los servicios que usted utiliza (ejemplo: sistema de recaudación, sitio web, trámites en línea) han estado disponibles de manera continua durante el último semestre? | 2.25 |
| 2. ¿Ha recibido notificaciones claras y oportunas sobre fallos en los sistemas o programaciones de mantenimiento? | 2.01 |

| Pregunta | Promedio |
|---|---|
| 3. Cuando ocurre una caída de los servicios, ¿el tiempo de recuperación le parece adecuado para garantizar la continuidad de sus actividades? | 2.29 |
| 4. ¿Cuenta con canales claros y accesibles para reportar incidentes de disponibilidad de los servicios? | 2.22 |
| 5. ¿Cómo calificaría la calidad de la atención que recibe del área de informática (TI) cuando necesita apoyo? | 2.91 |

Por otra parte es importante analizar los resultados de manera desagregada por cada ítem evaluado en el dominio DSS04, se observa que las percepciones de los usuarios presentan variaciones significativas:

- La pregunta 1, sobre la disponibilidad continua de los servicios, obtuvo un promedio de 2.25, lo que sugiere que los usuarios perciben una estabilidad moderada en los sistemas, aunque hay áreas que pueden mejorar.
- La pregunta 2, relacionada con la notificación de caídas o mantenimientos, fue calificada con la puntuación más baja de 2.01. Esta calificación reflejó una debilidad en los mecanismos de comunicación en forma de aviso oportuno, lo cual es necesario para la continuidad de las operaciones.
- La pregunta 3, se refiere al tiempo de recuperación de incidentes en promedio, se estableció en 2.29, lo cual no está tan lejos de la disponibilidad general, lo que indica que la probabilidad de recuperación rápida del servicio no está asegurada
- La pregunta 4, relacionada a los canales de reporte de incidentes, recibió un promedio de 2.22, en el cual los métodos de comunicación que se desarrollaron fueron percibidos por los usuarios como insuficientes o poco claros.
- Por último, la pregunta 5, relacionada a la calidad del cuidado proporcionado a los usuarios por el área de TI obtuvo la calificación más alta con un puntaje de 2.91, este valor indica una actitud positiva en proporcionar asistencia directa al usuario, en el dominio.

En conjunto, los resultados muestran que que las principales fortalezas que se han reconocido se correlacionan con el apoyo brindado por el área de TI, así como las debilidades más significativas que podrían centrarse en la comunicación de incidentes y los mecanismos de reporte. A su vez, estos hallazgos nos permiten determinar las direcciones que podemos tomar para cerrar la brecha que existe hacia el nivel de madurez objetivo.

**Validación cuantitativa mediante el instrumento (Alfa de Cronbach)**

Con el propósito de garantizar la fiabilidad estadística de las encuestas aplicadas, se procedió a realizar una validación cuantitativa mediante el coeficiente Alfa de Cronbach ($\alpha$). Este indicador permite evalúar y determinar si las preguntas miden de manera coherente la dimensión de análisis.

El procedimiento de cálculo se desarrolló de la siguiente forma:

**a) Preparación de los datos**

En primer lugar, se recopilaron todas las respuestas obtenidas de las encuestas aplicadas a los dos grupos de estudio:

- **Jefes departamentales:** quienes evaluaron los procesos asociados a los dominios DSS05, DSS02, APO12, DSS04, APO09, DSS01, EDM02, APO07, BAI09 y MEA01.
- **Usuarios de servicio:** Personal que solo usa el sistema, los mismos que solo respondieron las preguntas relacionadas con el dominio DSS04 de COBIT 2019, que evalúa la continuidad y disponibilidad de los servicios de TI.

Cada respuesta fue registrada a través de una escala tipo Likert de cinco niveles, con valores comprendidos entre 0 y 5, de acuerdo con los niveles de madurez definidos por COBIT 2019, conforme se muestra en la Tabla XVI. Para el análisis estadístico, todos los valores fueron transformados a formato numérico, extrayendo únicamente el valor de madurez seleccionado por cada participante.

Tabla XVI.
ESCALA DE VALORES DE MADUREZ COBIT 2019

| **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|
| Incompleto | Realizado | Gestionado | Establecido | Predecible | Optimizado |

**b) Cálculo del coeficiente Alfa de Cronbach**

Según Cronbach (1951), la consistencia interna del instrumento se calcula mediante la siguiente ecuación 2 [57] :

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum S_i^2}{S_T^2}\right) \tag{2}$$

donde:

- $k$: número total de ítems del instrumento,
- $S_i^2$: varianza de cada ítem,
- $S_T^2$: varianza total de la suma de los ítems por participante.

Para el grupo de jefes departamentales, se procesaron 10 ítems correspondientes a los 10 dominios evaluados. En el caso de los usuarios finales, se analizaron 5 ítems del dominio DSS04. En ambos casos, los datos brutos se obtuvieron directamente de las matrices de respuestas proporcionadas por los participantes.

A continuación, se muestra la Tabla XVII y Tabla XVIII con los datos que se utilizarán en la fórmula del coeficiente Alfa de Cronbach:

Tabla XVII.
CÁLCULO DEL COEFICIENTE ALFA DE CRONBACH JEFE DEPARTAMETALES

| **Ítem** | **Varianza del ítem ($S_i^2$)** | **Varianza total ($S_T^2$)** |
|---|---|---|
| 1 | 0.1908 | 1.1190 |
| 2 | 0.2708 | 0.8487 |
| 3 | 0.2405 | 1.2419 |
| 4 | 0.2220 | 0.8926 |
| 5 | 0.1605 | 1.1710 |
| 6 | 0.1605 | 1.0278 |
| 7 | 0.1469 | 0.9941 |
| 8 | 0.2591 | 0.9224 |
| 9 | 0.2223 | 0.9599 |
| 10 | 0.2372 | 0.8224 |
| **Total** | **2.1106** | **10.0** |

Tabla XVIII.
CÁLCULO DEL COEFICIENTE ALFA DE CRONBACH USUARIOS FINALES

| **Ítem** | **Varianza del ítem ($S_i^2$)** | **Varianza total ajustada ($S_T^2$)** |
|---|---|---|
| 1 | 0.2613 | 0.8810 |
| 2 | 0.6223 | 1.0367 |
| 3 | 0.5700 | 1.3210 |
| 4 | 0.3342 | 1.2014 |
| 5 | 0.3226 | 1.0200 |
| **Total** | **2.1106** | **5.46** |

En la tabla anterior, se deben ingresar las varianzas correspondientes para cada ítem ($S_i^2$) y la varianza total ($S_T^2$), que se calcularán a partir de los datos obtenidos de las matrices de respuestas. Estos valores se utilizarán para sustituir en la fórmula del coeficiente Alfa de Cronbach.

**c) Resultados de fiabilidad**

Los resultados obtenidos indican lo siguiente:

- **Encuesta a jefes departamentales:** $\alpha = 0{,}8766$ significa que la consistencia interna es alta, lo que indica que los elementos utilizados para evaluar los dominios de COBIT 2019 están correlacionados con precisión y rastrean consistentemente la madurez de los procesos medidos.
- **Encuesta a usuarios finales:** $\alpha = 0{,}7668$ muestra una fiabilidad aceptable, lo que por lo tanto es un método adecuado para monitorear la percepción de la disponibilidad y continuidad de los servicios de TI del centro de datos.

**d) Interpretación de los valores**

Los valores del coeficiente Alfa de Cronbach calculados para ambos grupos de estudio son los siguientes:

- **Jefes departamentales:** $\alpha = 0{,}8766$
- **Usuarios finales:** $\alpha = 0{,}7668$

A continuación, se presenta la interpretación de estos valores utilizando la escala de fiabilidad mostrada en la Tabla XIX.

Tabla XIX.
ESCALA DE INTERPRETACIÓN DEL COEFICIENTE ALFA DE CRONBACH

| **Rango de $\alpha$** | **Nivel de fiabilidad** | **Interpretación** |
|---|---|---|
| $\alpha \geq 0{,}90$ | Excelente | Muy alta consistencia interna |
| $0{,}80 \leq \alpha < 0{,}90$ | Buena | Alta consistencia interna |
| $0{,}70 \leq \alpha < 0{,}80$ | Aceptable | Fiabilidad adecuada |
| $0{,}60 \leq \alpha < 0{,}70$ | Cuestionable | Requiere revisión |
| $\alpha < 0{,}60$ | Deficiente | No confiable |

En base a estos valores:

- Para los jefes departamentales, el valor obtenido de $\alpha = 0{,}8766$ se encuentra en el rango de Buena fiabilidad ($0{,}80 \leq \alpha < 0{,}90$), lo que indica una alta consistencia interna, esto significa que los ítems empleados para medir los diferentes dominios de COBIT 2019 están fuertemente correlacionados y miden de manera coherente la madurez de los procesos evaluados.

- Para los usuarios finales, el valor obtenido de $\alpha = 0{,}7668$ se encuentra dentro del rango de Aceptable ($0{,}70 \leq \alpha < 0{,}80$), lo que refleja una fiabilidad adecuada, este valor es suficiente para evaluar la percepción de disponibilidad y continuidad de los servicios TI del Data Center, aunque se recomienda revisar la consistencia interna en futuras investigaciones.

De este modo,se determina que la fiabilidad de ambos instrumentos es adecuada y aceptable alcanzando un nivel satisfactorio, confirmando que las encuestas poseen una estructura consistente y fiable, apropiada para evaluar la madurez y el grado de cumplimiento de los procesos del data center según los principios y dominios del marco COBIT 2019.

### 4.1.4 Aplicación de Entrevista

**Resultados obtenidos en la aplicación de Entrevista**

La información obtenida de la entrevista fue sintetizada en la Tabla XX, donde se presentan los controles evaluados, los criterios de verificación aplicados y el grado de cumplimiento observado, esta sistematización facilitó el contraste entre las evidencias documentales y las percepciones del personal técnico, fortaleciendo el diagnóstico general sobre el estado actual de la seguridad informática institucional.

Tabla XX.
CHECKLIST DE SEGURIDAD DEL DATA CENTER BASADO EN COBIT 2019 CON RESPUESTAS DE LA ENTREVISTA Y EL CHECKLIST APLICADO

| Dominio COBIT 2019 | Control Evaluado | Criterio de Evaluación | Cumplimiento |
|---|---|---|---|
| DSS05 (Seguridad de Servicios) | Control de acceso físico | Puertas de seguridad, tarjetas de proximidad, cámaras CCTV, registro de accesos | × |
| DSS01 (Operaciones) | Monitoreo ambiental | Sensores de temperatura, humedad, humo, inundación con alertas en tiempo real | × |
| DSS04 (Continuidad y Disponibilidad) | Plan de respaldo y recuperación | Copias de seguridad automáticas, pruebas de restauración documentadas | × |
| APO09 (Gestión de Activos) | Gestión de cableado estructurado | Cableado ordenado, etiquetado, con rutas de respaldo | ∼ |
| APO12 (Gestión de Riesgos) | Evaluación de riesgos periódica | Matriz de riesgos, informes de mitigación y seguimiento | ∼ |
| EDM02 (Asegurar Beneficios) | Involucramiento de la alta dirección | Actas de reuniones, presupuesto asignado a seguridad | × |
| MEA01 (Monitoreo y Evaluación) | Auditorías internas de seguridad | Evidencia de auditorías, informes de hallazgos y acciones correctivas | × |

Continúa en la siguiente página

| Dominio COBIT 2019 | Control Evaluado | Criterio de Evaluación | Cumplimiento |
|---|---|---|---|
| APO12 / EDM02 (Recursos y Riesgos) | Identificación de principales desafíos: limitaciones económicas | Falta de financiamiento para proyectos de seguridad | $\times$ |
| EDM02 / APO09 (Planificación) | Proyectos de mejora priorizados con presupuesto asignado | Registro de iniciativas y proyectos de corto plazo documentados | $\sim$ |

### 4.1.5 Estadística

**Estadísticas de las encuestas dirigidas a los jefes departamentales**

Para el tratamiento de los datos obtenidos en la encuesta aplicada a los jefes departamentales, se emplearon medidas estadísticas descriptivas con el fin de resumir y analizar los resultados en la escala de madurez COBIT 2019,lo que implica que estas medidas permitan identificar tanto el nivel promedio alcanzado en cada dominio, como el grado de dispersión en las respuestas de los participantes.

En primer lugar, se calculó la media aritmética ($\bar{x}$), la cual refleja el valor promedio de las respuestas registradas en la escala de 0 a 5, La media se determina mediante la siguiente Ecuación 3 [58]:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n} \tag{3}$$

donde $x_i$ corresponde al valor obtenido en cada respuesta y $n$ representa el número total de observaciones.

Posteriormente, se calculó la desviación estándar (s), que mide el grado de dispersión de los datos respecto al valor medio, y se expresa en la Ecuación 4 :

$$s = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}} \tag{4}$$

Finalmente, se obtuvo la varianza ($s^2$) [58], definida como el cuadrado de la desviación estándar y utilizada como medida del grado de variabilidad de los datos en la Ecuación 5:

$$s^2 = \frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1} \tag{5}$$

La aplicación de estas ecuaciones permitió obtener los valores de media, desviación estándar y varianza por cada dominio COBIT 2019 considerado en la investigación, generando una visión cuantitativa del estado de madurez y de la homogeneidad de las percepciones entre los encuestados, estos cálculos se constituyen en la base para el análisis comparativo con el nivel objetivo de madurez previamente definido, y para la determinación de las brechas existentes.

Con el fin de complementar el análisis, en la Tabla XXI se presentan además los estadísticos descriptivos de cada dominio, incluyendo la media, desviación estándar y la varianza, lo cual permite observar la dispersión de las respuestas y el nivel de homogeneidad entre los jefes departamentales encuestados.

Tabla XXI.
ESTADÍSTICOS DESCRIPTIVOS DE LA ENCUESTA A JEFES DEPARTAMENTALES POR DOMINIO COBIT 2019, BASADO EN COBIT 2019

| **Dominio COBIT 2019** | **Media** | **Desviación estándar** | **Varianza** |
|---|---|---|---|
| DSS05 – Seguridad de Servicios | 1.40 | 1.30 | 1.69 |
| DSS02 – Gestión de Incidentes | 0.92 | 1.19 | 1.41 |
| APO12 – Gestión de Riesgos | 0.92 | 1.13 | 1.27 |
| DSS04 – Continuidad y Disponibilidad | 1.21 | 1.03 | 1.06 |
| APO09 – Gestión de Activos | 1.69 | 1.32 | 1.73 |
| DSS01 – Operaciones | 0.46 | 0.78 | 0.60 |
| EDM02 – Asegurar Beneficios | 1.23 | 1.01 | 1.03 |
| APO07 – Gestión del Personal | 0.93 | 1.10 | 1.21 |
| BAI09 – Gestión de Activos | 0.85 | 1.07 | 1.14 |
| MEA01 – Monitoreo y Evaluación | 1.50 | 0.71 | 0.50 |

**Estadísticas de las encuestas dirigidas a los usuarios de servicio del GAD**

Para profundizar en el análisis de la encuesta aplicada a los usuarios respecto al dominio DSS04 (Continuidad y Disponibilidad), se realizó un tratamiento estadístico de los datos obtenidos, este procedimiento permite describir con mayor claridad la tendencia de las respuestas y la homogeneidad en las percepciones de los participantes.

como se puede evidenciar en la Tabla XXII,se utilizaron tres medidas principales: la media, que indica el valor central de las respuestas; la desviación estándar, que muestra cuánto se alejan los datos de ese valor promedio; y la varianza, que cuantifica la dispersión total de las observaciones, con estas métricas es posible valorar no solo el nivel alcanzado por cada ítem evaluado, sino también la consistencia de las opiniones de los usuarios, lo que aporta una visión más precisa del estado actual del dominio DSS04.

Tabla XXII.
RESULTADOS ESTADÍSTICOS DE LA ENCUESTA DE USUARIOS – DOMINIO DSS04

| **Pregunta** | **Media** | **Desviación Estándar** | **Varianza** |
|---|---|---|---|
| 1. Disponibilidad de los servicios utilizados | 2.25 | 1.22 | 1.48 |
| 2. Avisos claros y a tiempo sobre caídas o mantenimientos | 2.01 | 1.38 | 1.91 |
| 3. Tiempo de recuperación tras caídas | 2.29 | 1.26 | 1.58 |
| 4. Canales claros para reportar incidentes | 2.22 | 1.24 | 1.54 |
| 5. Calidad de la atención recibida del área de TI | 2.91 | 1.04 | 1.08 |

**Estadísticas de la entrevista mediante check list**

El análisis del checklist aplicado al Data Center permitió identificar el nivel de cumplimiento de los controles de seguridad en relación con los dominios de COBIT 2019, como se observa en la Tabla XXIII, ninguno de los controles evaluados alcanzó un cumplimiento total, mientras que un 33.3 % se encuentra parcialmente implementado y un 66.7 % no cumple con los criterios establecidos, estos resultados evidencian una debilidad significativa en la gestión de seguridad,

lo que refuerza la necesidad de priorizar acciones correctivas y de mejora alineadas con las mejores prácticas de gobernanza de TI.

Tabla XXIII.
RESUMEN PORCENTUAL DEL CUMPLIMIENTO DE CONTROLES DE SEGURIDAD

| Símbolo | Cantidad de Controles | Porcentaje |
|---|---|---|
| ✓ | 0 | 0 % |
| ∼ | 3 | 33.3 % |
| × | 6 | 66.7 % |
| **Total** | **9** | **100 %** |

### 4.1.6 Herraminetas software

**Escaneo herramienta NMAP**

Nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada en el campo de la ciberseguridad para el análisis de redes, la detección de hosts activos y la identificación de puertos y servicios disponibles, su principal utilidad radica en permitir a los administradores y auditores de seguridad conocer con precisión qué servicios se encuentran expuestos en una infraestructura tecnológica, así como descubrir configuraciones inseguras o vulnerabilidades que puedan ser explotadas por atacantes.

En el marco de esta investigación, se empleó Nmap como herramienta de diagnóstico para evaluar la seguridad de la infraestructura del data center del GAD municipal del cantón Bolívar, se revisó la existencia de servicios innecesarios, puertos abiertos y posibles puntos de acceso no gestionados.

El análisis efectuado mediante la herramienta Nmap permitió identificar vulnerabilidades críticas en la seguridad lógica y perimetral del Data Center, los hallazgos principales se relacionan con la exposición de puertos abiertos, la existencia de servicios sin mecanismos robustos de autenticación, el uso de configuraciones por defecto y la ausencia de segmentación de tráfico.

Como se muestra en la Tabla XXIV, hay brechas sustanciales con respecto al nivel de madurez objetivo (4) que comprometen la disponibilidad, confidencialidad e integridad de los servicios institucionales.

Tabla XXIV.
HALLAZGOS IDENTIFICADOS CON LA HERRAMIENTA NMAP Y SU BRECHA FRENTE AL NIVEL OBJETIVO

| **Dominio COBIT 2019** | **Hallazgo identificado** | **Brecha (Objetivo 4)** |
|---|---|---|
| DSS05 – Seguridad de Servicios | Puertos abiertos sin control documentado (HTTP 80, HTTPS 443, SSH 22 y secundarios). | 2.60 |
| DSS05 – Seguridad de Servicios | Servicios expuestos sin autenticación robusta ni cifrado avanzado. | 2.60 |
| APO12 – Gestión de Riesgos | Los dispositivos de red mantienen configuraciones predeterminadas, lo que incrementa la vulnerabilidad. | 3.08 |
| MEA01 – Monitoreo y Evaluación | Ausencia de segmentación y filtrado de tráfico que incrementa la probabilidad de movimientos laterales. | 2.50 |

## 4.2 Evaluación COBIT 2019 y brechas

### 4.2.1 Mapeo de hallazgos encontrados

**Encuesta jefes departamentales**

El análisis consolidado de los dominios COBIT 2019 aplicados al Data Center permitió determinar los hallazgos encontrados frente al nivel objetivo establecido en (4), tal como se observa en la Tabla XXV, los resultados evidencian que los dominios presentan valores por debajo del umbral esperado, con brechas que oscilan entre 2.31 y 3.54 puntos, este escenario refleja deficiencias en aspectos críticos como la gestión de operaciones (DSS01), riesgos (APO12), incidentes (DSS02) y activos (BAI09, APO09), lo que compromete la continuidad, seguridad y gobernanza de la infraestructura tecnológica, dichos hallazgos justifican la necesidad de diseñar e implementar un plan de seguridad alineado con COBIT 2019 que reduzca la brecha identificada y garantice la mejora continua de los procesos de TI.

Tabla XXV.
MAPEO DE HALLAZGOS POR DOMINIO COBIT 2019

| **Dominio COBIT 2019** | **Hallazgo principal** | **Brecha frente al nivel objetivo (4)** |
|---|---|---|
| DSS01 – Operaciones | Ausencia de controles ambientales y gestión limitada de operaciones críticas | 3.54 |
| DSS02 – Gestión de Incidentes | No existen procedimientos formales ni métricas de respuesta a incidentes | 3.08 |
| DSS04 – Continuidad y Disponibilidad | Carencia de planes de respaldo documentados y simulacros de contingencia | 2.79 |
| DSS05 – Seguridad de Servicios | Falta de controles de acceso físico y segmentación de red | 2.60 |
| APO09 – Gestión de Activos | Cableado estructurado desorganizado y débil gestión de inventarios | 2.31 |
| APO12 – Gestión de Riesgos | Evaluaciones de riesgos no estandarizadas ni frecuentes | 3.08 |
| APO07 – Gestión del Personal | Limitada capacitación del personal en seguridad informática | 3.07 |
| BAI09 – Gestión de Activos | Falta de procesos de actualización y mantenimiento del ciclo de vida de activos | 3.15 |
| EDM02 – Asegurar Beneficios | Escasa participación de la alta dirección en la definición de políticas de seguridad | 2.77 |

| Dominio COBIT 2019 | Hallazgo principal | Brecha frente al nivel objetivo (4) |
|---|---|---|
| MEA01 – Monitoreo y Evaluación | Débil aplicación de estándares y falta de auditorías internas regulares | 2.50 |

**Encuesta usuarios de servicios**

El mapeo de hallazgos realizado a partir de la encuesta aplicada a los usuarios, enfocada en el dominio DSS04 (Continuidad y Disponibilidad), permitió identificar debilidades específicas en los procesos de continuidad operativa del Data Center, los resultados muestran que los usuarios desconocen procedimientos claros ante interrupciones, no se cuenta con pruebas documentadas de recuperación de respaldos y persisten interrupciones no planificadas en servicios críticos. Asimismo, se evidenció la ausencia de redundancia total en la infraestructura y la dependencia de acciones manuales no formalizadas para asegurar la continuidad, estos hallazgos reflejan brechas significativas respecto al nivel objetivo de madurez (4), lo que compromete la resiliencia y confiabilidad de los servicios tecnológicos ofrecidos, tal como se presenta la Tabla XXVI.

Tabla XXVI.
MAPEO DE HALLAZGOS EN ENCUESTA DE USUARIOS – DOMINIO DSS04

| Pregunta | Hallazgo principal | Brecha (Objetivo 4) |
|---|---|---|
| 1 | Los usuarios desconocen procedimientos claros para actuar en caso de interrupciones. | 3.0 |
| 2 | No existen pruebas documentadas de recuperación de respaldos. | 2.8 |
| 3 | El acceso a servicios críticos presenta interrupciones no planificadas. | 2.5 |
| 4 | No se evidencia redundancia total en la infraestructura de TI. | 3.2 |

| Pregunta | Hallazgo principal | Brecha (Objetivo 4) |
|---|---|---|
| 5 | La continuidad del servicio depende de acciones manuales no formalizadas. | 3.1 |

**Entrevista**

El levantamiento de información mediante la entrevista aplicada a al jefe del departamento de TI, complementada con el checklist de verificación, permitió identificar una serie de hallazgos críticos que afectan la seguridad y gobernanza del Data Center, como se observa en la Tabla XXVII, las principales debilidades se concentran en la falta de controles físicos y lógicos, ausencia de planes de continuidad documentados, evaluaciones de riesgos poco frecuentes y escasa participación de la alta dirección en la definición de políticas de seguridad.

Estos hallazgos respaldan los bajos niveles de cumplimiento reflejados en los resultados porcentuales y sirven como base para desarrollar un plan de seguridad alineado con COBIT 2019

Tabla XXVII.
HALLAZGOS IDENTIFICADOS POR DOMINIO COBIT 2019 Y SU BRECHA FRENTE AL NIVEL OBJETIVO

| Dominio COBIT 2019 | Hallazgo identificado | Brecha (Objetivo 4) |
|---|---|---|
| DSS05 – Seguridad de Servicios | No existen controles de acceso físico (biometría, tarjetas, cámaras) ni segmentación de red adecuada; seguridad lógica limitada al firewall básico | 2.60 |
| DSS01 – Operaciones | No se dispone de monitoreo ambiental integral (sensores de temperatura, humedad, humo, inundación) | 3.54 |
| DSS04 – Continuidad y Disponibilidad | Ausencia de planes de respaldo documentados y falta de pruebas periódicas de recuperación | 2.79 |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Hallazgo identificado | Brecha (Objetivo 4) |
|---|---|---|
| DSS02 – Gestión de Incidentes | No se cuenta con procedimientos formales ni métricas de atención a incidentes | 3.08 |
| APO09 – Gestión de Activos | Cableado estructurado desorganizado y sin documentación técnica formal | 2.31 |
| APO12 – Gestión de Riesgos | Evaluaciones de riesgos poco frecuentes (1–2 veces/año) y sin normativa formal | 3.08 |
| APO07 – Gestión del Personal | Personal sin programas continuos de capacitación en seguridad informática | 3.07 |
| BAI09 – Gestión de Activos | Ausencia de procesos de actualización y mantenimiento del ciclo de vida de activos | 3.15 |
| EDM02 – Asegurar Beneficios | Escasa participación de la alta dirección en la definición de políticas de seguridad y en la asignación de recursos | 2.77 |
| MEA01 – Monitoreo y Evaluación | Falta de auditorías internas y no aplicación de estándares internacionales (ej. ISO 27001, COBIT) | 2.50 |

### 4.2.2 Comparativo estado actual vs objetivo

**Encuestas jefe departamentales del GAD**

El análisis de los resultados obtenidos a partir de las encuestas aplicadas a los jefes departamentales permitió identificar el nivel de madurez actual de los dominios COBIT 2019 y compararlo con el nivel objetivo establecido en el modelo. Como se muestra en la Tabla XXVIII, ninguno de los dominios alcanzó el nivel de madurez esperado (nivel 4), estipulado en los parámetros de COBIT 2019, según lo señalado por [12]. Este resultado pone de manifiesto brechas significativas, que evidencian deficiencias en la gestión y gobernanza del Data Center.

En particular, los dominios DSS01 Operaciones (brecha de 3.54), BAI09 Gestión de Activos (3.15), así como APO12 Gestión de Riesgos y DSS02 Gestión de Incidentes (ambos con 3.08), destacan como los más críticos al presentar mayores carencias en continuidad operativa, administración de activos y respuesta a incidentes, estas áreas requieren atención prioritaria debido a su impacto directo en la disponibilidad y seguridad de los servicios institucionales.

A diferencia de ello, los dominios que muestran avances significativos en sus prácticas son Gestión de Activos APO09 (brecha de 2.31), MEA01 Monitoreo y Evaluación (2.50), y DSS05 Seguridad del Servicio (2.60), pero aún necesitan fortalecerse para asegurar una alineación completa con las mejores prácticas internacionales.

Tabla XXVIII.
COMPARACIÓN ENTRE NIVEL ACTUAL, NIVEL OBJETIVO Y BRECHA POR DOMINIO COBIT 2019

| Dominio COBIT 2019 | Nivel Actual (Media) | Nivel Objetivo | Brecha |
|---|---|---|---|
| DSS05 – Seguridad de Servicios | 1.40 | 4 | 2.60 |
| DSS02 – Gestión de Incidentes | 0.92 | 4 | 3.08 |
| APO12 – Gestión de Riesgos | 0.92 | 4 | 3.08 |
| DSS04 – Continuidad y Disponibilidad | 1.21 | 4 | 2.79 |
| APO09 – Gestión de Activos | 1.69 | 4 | 2.31 |
| DSS01 – Operaciones | 0.46 | 4 | 3.54 |
| EDM02 – Asegurar Beneficios | 1.23 | 4 | 2.77 |
| APO07 – Gestión del Personal | 0.93 | 4 | 3.07 |
| BAI09 – Gestión de Activos | 0.85 | 4 | 3.15 |
| MEA01 – Monitoreo y Evaluación | 1.50 | 4 | 2.50 |

La Fig. 14 complementa este análisis al representar gráficamente la comparación entre los niveles actuales y el objetivo de cada dominio, destacando visualmente las brechas existentes, estos resultados confirman la necesidad de implementar un plan de mejora progresivo y estructurado que permita reducir las brechas, mejorar los controles de seguridad y asegurar una gobernanza de TI más robusta y alineada con el marco de referencia COBIT 2019.

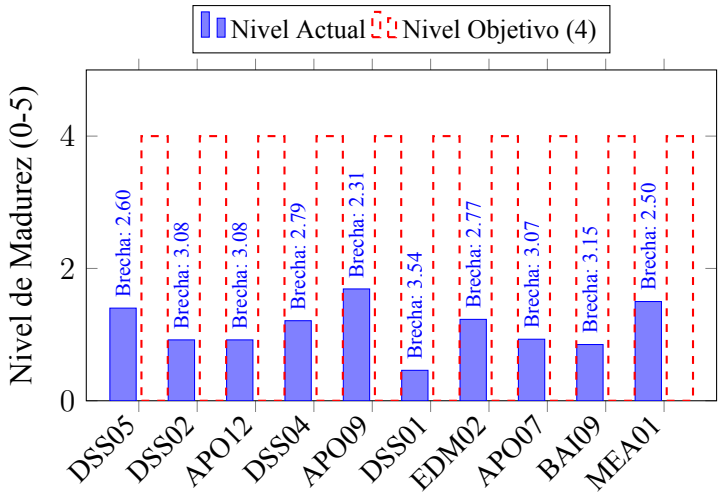


**Fig. 14**. Comparación entre nivel actual y nivel objetivo con la brecha identificada por dominio COBIT 2019

### Encuestas usuarios de servicios

Con base en los resultados estadísticos de las encuestas aplicadas a los usuarios, se elaboró un mapa de madurez del dominio DSS04 (Continuidad y Disponibilidad), es asi que ne la figura 15 permite observar de manera comparativa el nivel alcanzado en cada ítem frente al nivel objetivo definido en 4, facilitando la identificación de brechas y áreas críticas de mejora.

Los promedios obtenidos por pregunta se distribuyen entre 2.01 y 2.91, evidenciando un nivel de madurez intermedio con un promedio global de 2.34, la desviación estándar calculada refleja que existe una variabilidad moderada en las respuestas de los usuarios, lo que indica que la percepción de la continuidad de los servicios no es homogénea, la varianza, por su parte, confirma estas diferencias en la valoración de los distintos aspectos evaluados.

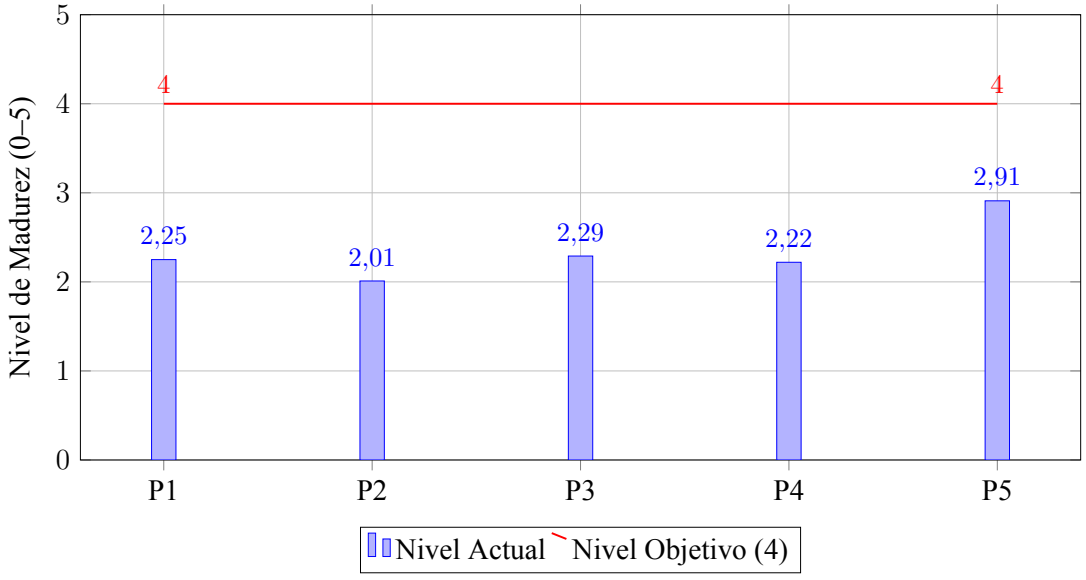


**Fig. 15**. Mapa de madurez del dominio DSS04 con resultados de encuestas de usuarios

**Entrevista**

La Fig. 16, representa el mapa de madurez de los dominios evaluados bajo el marco COBIT 2019 en el Data Center, el gráfico de barras permite visualizar el nivel alcanzado en cada dominio en una escala de 0 a 5, donde 0 representa la ausencia total de cumplimiento y 5 corresponde a un estado de madurez óptimo.

Los resultados evidencian que la mayoría de los dominios evaluados se ubican en el nivel (0), lo que refleja la ausencia de controles adecuados y de mecanismos formales de gestión. De manera, los dominios DSS01 (Operaciones), DSS04 (Continuidad y Disponibilidad), APO09 (Gestión de Activos), EDM02 (Asegurar Beneficios) y MEA01 (Monitoreo y Evaluación) no alcanzan ningún nivel de madurez, lo que demuestra una aplicación limitada de prácticas y políticas fundamentales, siendo prioritaria su mejora en estas áreas consideradas críticas.

Por su parte, el dominio DSS05 (Seguridad de Servicios) presenta un nivel de madurez de 1, debido a la existencia de un firewall como único mecanismo de protección lógica, sin que existan controles físicos ni medidas adicionales, Asimismo, el dominio APO12 (Gestión de Riesgos) se sitúa en nivel 2, ya que si bien se realizan análisis de riesgos una o dos veces al año, estos no siguen un estándar formal ni están alineados a buenas prácticas internacionales.

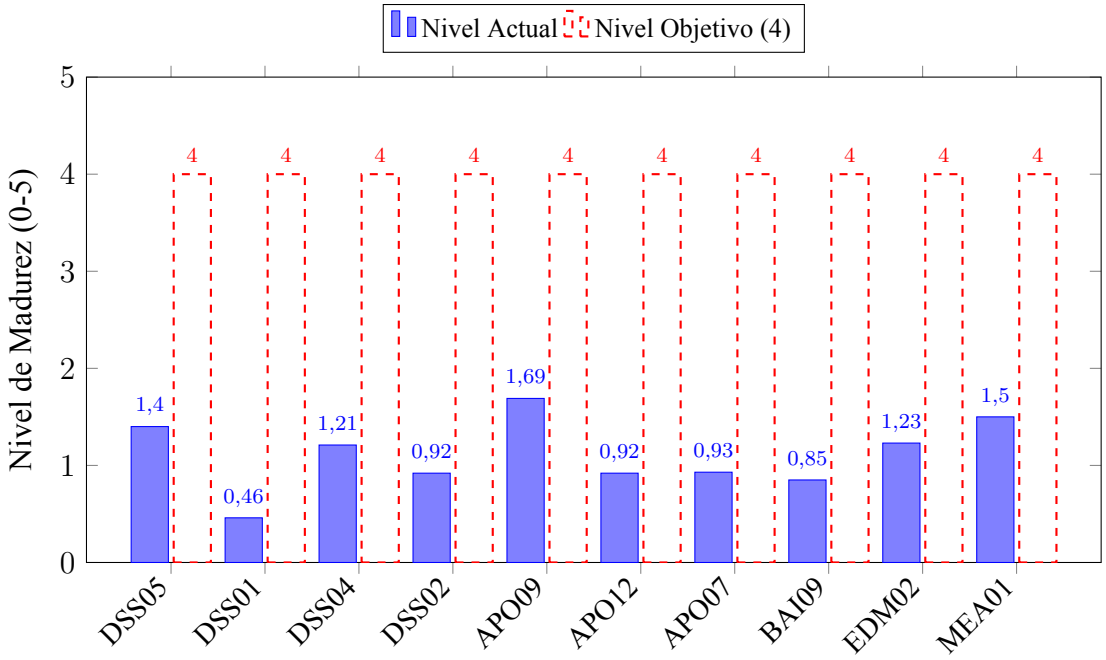


**Fig. 16**. Comparación entre nivel actual y nivel objetivo de madurez por dominio COBIT 2019 en gráfico de barras

### 4.2.3 Análisis de brechas

El análisis de brechas se desarrolló con el propósito de determinar el grado de madurez alcanzado por los dominios de COBIT 2019 y establecer las diferencias existentes respecto al nivel objetivo definido, para ello, se integraron los resultados obtenidos mediante entrevistas, encuestas, checklist y análisis técnico (Nmap), lo que permitió identificar las principales deficiencias en los procesos de TI y priorizar las áreas de mejora.

La entrevista realizada al encargado de TI y encuestas a los jefes departamentales proporcionaron información útil sobre los procesos de gestión, continuidad y seguridad, además las encuestas a los usuarios finales, centradas principalmente en el dominio de DSS04 (Continuidad y Disponibilidad), resultaron en un nivel promedio de 2.34, por el contrario, los resultados de las encuestas a los jefes de departamento mostraron niveles de madurez que varían entre 0.9 y 1.6, principalmente en los dominios de APO09 (Gestión de Activos), APO12 (Gestión de Riesgos) y MEA01 (Monitoreo y Evaluación).

El análisis técnico con Nmap evidenció vulnerabilidades relacionadas con puertos abiertos, configuraciones por defecto y falta de políticas de filtrado y autenticación robusta, afectando la confidencialidad, integridad y disponibilidad de la información, los resultados globales presentados en la Tabla XXIX muestran que la institución alcanza un nivel de madurez promedio entre 1 y 2, lo que evidencia la ausencia de procesos formalizados y la existencia de brechas significativas frente al nivel objetivo (4).

Tabla XXIX.
RESUMEN DE NIVELES DE MADUREZ POR DOMINIO COBIT 2019

| Dominio COBIT 2019 | Nivel Actual | Nivel Objetivo | Brecha |
|---|---|---|---|
| DSS04 – Continuidad y Disponibilidad | 2.34 | 4 | 1.66 |
| APO09 – Gestión de Activos | 1.69 | 4 | 2.31 |
| MEA01 – Monitoreo y Evaluación | 1.50 | 4 | 2.50 |
| DSS05 – Seguridad de Servicios | 1.40 | 4 | 2.60 |
| DSS01 – Operaciones | 0.46 | 4 | 3.54 |

| Dominio COBIT 2019 | Nivel Actual | Nivel Objetivo | Brecha |
|---|---|---|---|
| BAI09 – Gestión de Activos (Procesos específicos) | 0.85 | 4 | 3.15 |
| APO12 – Gestión de Riesgos | 0.92 | 4 | 3.08 |
| DSS02 – Gestión de Incidentes | 0.92 | 4 | 3.08 |
| EDM02 – Asegurar Beneficios | 1.23 | 4 | 2.77 |
| APO07 – Gestión del Personal | 0.93 | 4 | 3.07 |

Como se observa en la Fig. 17, todos los dominios se encuentran por debajo del nivel objetivo, destacando las mayores brechas en DSS01 (Operaciones), APO12 (Gestión de Riesgos) y BAI09 (Gestión de Activos), con valores superiores a 3 puntos, los dominios con mejor desempeño son DSS04 (Continuidad y Disponibilidad) y APO09 (Gestión de Activos), aunque aún presentan desviaciones considerables que requieren acciones correctivas.

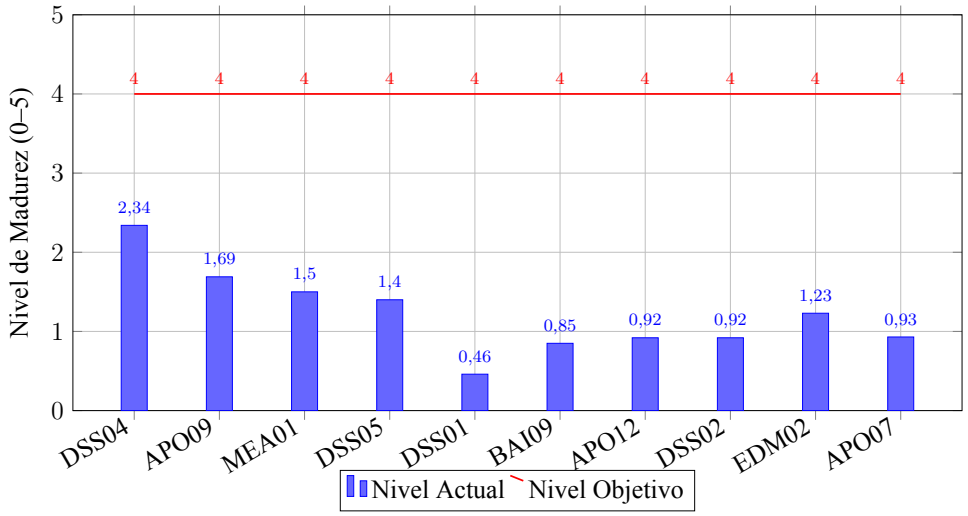


**Fig. 17**. Comparación de niveles de madurez actuales vs. objetivo en los dominios COBIT 2019

En síntesis, el análisis de brechas demuestra que la institución mantiene un nivel de madurez limitado, con prácticas no estandarizadas y una débil gestión de riesgos, estos resultados constituyen la base técnica para el plan de mejora, orientado a fortalecer los procesos de gobernanza de TI y alcanzar la alineación con las mejores prácticas del marco COBIT 2019.

## 4.3 Análisis de Riesgos

### 4.3.1 Amenazas

Con base en los resultados del diagnóstico y el análisis de brechas, se identificaron las principales amenazas que afectan la infraestructura tecnológica y la gestión de la información en el Data Center, estas amenazas se asocian directamente con los dominios de COBIT 2019 evaluados, permitiendo establecer una trazabilidad entre los hallazgos técnicos, los riesgos y los procesos de gobernanza de TI.

La Tabla XXX presenta la relación entre cada dominio COBIT 2019 y las amenazas detectadas, destacando los aspectos más críticos que impactan la confidencialidad, integridad y disponibilidad de la información.

Tabla XXX.
IDENTIFICACIÓN DE AMENAZAS POR DOMINIO COBIT 2019

| **Dominio COBIT 2019** | **Amenazas identificadas** |
|---|---|
| DSS01 – Operaciones | Interrupción de servicios críticos debido a fallas eléctricas o sobrecalentamiento; falta de monitoreo ambiental integral; pérdida de datos por la ausencia de respaldo automático. |
| DSS02 – Gestión de Incidentes | Los problemas no se detectan ni se atienden de manera oportuna, existen retrasos en la identificación y respuesta de los incidentes ;los protocolos de notificación no están establecidos;la falta de indicadores o métricas para medir el impacto y gravedad de los incidentes. |
| DSS04 – Continuidad y Disponibilidad | Hay interrupciones de servicios por eventos externos como desastres naturales o problemas técnicos (hardware, software, red); no hay pruebas documentadas de recuperación; la infraestructura tecnológica existente tiene equipos que no son adecuados para garantizar la continuidad y disponibilidad de los servicios. |

| Dominio COBIT 2019 | Amenazas identificadas |
|---|---|
| DSS05 – Seguridad de Servicios | Se identificó accesos no autorizados al data center, como también cuentas de usuarios vulnerables debido a contraseñas débiles y poco seguras, por otra parte, en la red los puertos abiertos sin protección y limitación al mitigar ataques de denegación de servicio (DDoS). |
| APO07 – Gestión del Personal | Falta de capacitación en temas de seguridad y ciberseguridad; fallos humanos al gestionar la información; violación de políticas vinculada a la falta de conocimiento. |
| APO09 – Gestión de Activos | Falta de controles físicos y administrativos que dan paso al robo o pérdida de equipos; no existe un registro actualizado de inventarios; activos sin registro ni control del ciclo de vida; desorganización en el cableado y las conexiones, lo que genera riesgos de fallos, dificultades de mantenimiento y posibles interrupciones del servicio. |
| APO12 – Gestión de Riesgos | Existe un déficit en la identificación temprana de vulnerabilidades, también se carece de una matriz de riesgos actualizada y no existen planes de mitigación de respuestas ante la gestión de incidentes. |
| BAI09 – Gestión de Activos | No existe una gestión adecuada de los equipos tecnológicos, como servidores, computadoras y aplicaciones, que se encuentran obsoletos tanto en hardware como en software; fallas debido a la falta de mantenimiento y a limitaciones técnicas de compatibilidad entre componentes críticos. |
| EDM02 – Asegurar Beneficios | Las decisiones de TI no están completamente alineadas con los objetivos estratégicos, existiendo una baja supervisión y control en el cumplimiento tanto de políticas como de buenas prácticas institucionales. |

| Dominio COBIT 2019 | Amenazas identificadas |
|---|---|
| MEA01 – Monitoreo y Evaluación | No cuenta con mecanismos adecuados para supervisar, evaluar y mejorar la seguridad, tanto en auditorías internas como en externas; falta de indicadores de rendimiento y acciones correctivas lo que conlleva que las acciones de mejora no se implementen ni se verifiquen adecuadamente. |

La identificación de amenazas evidencia que los dominios más comprometidos son DSS05 (Seguridad de Servicios), DSS04 (Continuidad y Disponibilidad) y APO12 (Gestión de Riesgos), al concentrar los riesgos con mayor probabilidad e impacto, estos resultados servirán como base para la elaboración de la matriz de riesgos y la propuesta del plan de seguridad, orientado a mitigar las amenazas detectadas y fortalecer la resiliencia tecnológica del GAD.

### 4.3.2 Vulnerabilidades

El análisis de vulnerabilidades permitió detectar las debilidades que incrementan la probabilidad de materialización de las amenazas descritas en la sección anterior, estas vulnerabilidades se relacionan directamente con los dominios de COBIT 2019 aplicados, abarcando aspectos físicos, lógicos, de gestión y de gobernanza de TI.

La Tabla XXXII muestra las principales vulnerabilidades detectadas por dominio, destacando los puntos críticos que necesitan atención urgente para reducir los riesgos operativos e institucionales.

Tabla XXXI.
IDENTIFICACIÓN DE VULNERABILIDADES DEL DATA CENTER SEGÚN DOMINIOS COBIT 2019

| **Categoría** | **Vulnerabilidad Identificada** | **Fuente de hallazgo** | **Dominio COBIT 2019** |
|---|---|---|---|
| Seguridad física | Ausencia de controles de acceso físico (biometría, tarjetas, cámaras) | Entrevista / Checklist | DSS05, DSS01 |
| Seguridad lógica | Falta de segmentación de red, IDS/IPS, monitoreo en tiempo real (solo firewall básico) | Nmap / Checklist | DSS05 |
| Continuidad | Inexistencia de estrategias documentadas de respaldo y recuperación | Entrevista / Checklist | DSS04 |
| Continuidad | No se realizan pruebas ni simulacros de contingencia | Entrevista | DSS04 |
| Gestión de activos | Desorganización y falta de documentación en el cableado estructurado | Checklist | APO09 |
| Gestión de activos | Ausencia de procesos documentados para el ciclo de vida de los activos tecnológicos; falta de políticas de mantenimiento y actualización; riesgo de obsolescencia tecnológica | Entrevista / Checklist | BAI09 |

*Continúa en la siguiente página*

| Categoría | Vulnerabilidad Identificada | Fuente de hallazgo | Dominio COBIT 2019 |
|---|---|---|---|
| Gobernanza | Escasa participación de la alta dirección en la definición de políticas de seguridad | Entrevista | EDM02 |
| Gobernanza | Ausencia de roles definidos en la gestión de infraestructura | Entrevista | EDM02 |
| Gestión de riesgos | Evaluaciones de riesgos limitadas (1–2 veces/año, sin normativa formal) | Entrevista | APO12 |
| Cumplimiento | No se aplican estándares ni regulaciones internacionales (ISO 27001, COBIT) | Checklist / Entrevista | MEA01 |
| Usuarios | Falta de capacitación y concienciación en seguridad informática | Encuestas a usuarios y departamentos | APO07, MEA01 |
| Exposición externa | Servicios abiertos detectados en el escaneo Nmap (riesgo de ataques externos) | Nmap | DSS05, APO12, MEA01 |

### 4.3.3 Valoración de vulnerabilidades

En esta fase se realizó la valoración de las vulnerabilidades identificadas, considerando su probabilidad de ocurrencia y el impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información, la valoración permite determinar la criticidad de cada vulnerabilidad y establecer prioridades para la gestión de riesgos, alineando los resultados con los dominios de COBIT 2019.

La Tabla XXXII presenta las principales vulnerabilidades del Data Center, vinculadas con las fuentes de hallazgo y su respectivo nivel de impacto estimado, el impacto fue clasificado en tres

niveles —Alto, Medio y Bajo— según la magnitud del daño esperado en caso de materialización de la amenaza.

Tabla XXXII.
VALORACIÓN DE VULNERABILIDADES DEL DATA CENTER SEGÚN DOMINIOS COBIT 2019 E IMPACTO SOBRE LA SEGURIDAD CIA

| Categoría | Vulnerabilidad Identificada | Fuente de hallazgo | Dominio COBIT 2019 | C | I | A | Amenaza Relacionada |
|---|---|---|---|---|---|---|---|
| Seguridad física | Ausencia de controles de acceso físico (biometría, tarjetas, cámaras) | Entrevista / Checklist | DSS05, DSS01 | Alto | Medio | Bajo | Accesos no autorizados al Data Center |
| Seguridad lógica | Falta de segmentación de red, IDS/IPS y monitoreo en tiempo real (solo firewall básico) | Nmap / Checklist | DSS05 | Medio | Alto | Alto | Exposición de puertos sin protección |
| Continuidad | Inexistencia de estrategias documentadas de respaldo y recuperación | Entrevista / Checklist | DSS04 | Bajo | Medio | Alto | Caída de servicios ante desastres o fallas técnicas |

Continúa en la siguiente página

| Categoría | Vulnerabilidad Identificada | Fuente de hallazgo | Dominio COBIT 2019 | C | I | A | Amenaza Relacionada |
|---|---|---|---|---|---|---|---|
| Continuidad | No se realizan pruebas ni simulacros de contingencia | Entrevista | DSS04 | Bajo | Bajo | Medio | Falta de pruebas documentadas de recuperación |
| Gestión de activos | Desorganización y falta de documentación en el cableado estructurado | Checklist | APO09 | Bajo | Medio | Medio | Robo o pérdida de equipos |
| Gestión de activos | Ausencia de procesos documentados para el ciclo de vida de los activos tecnológicos; falta de mantenimiento y actualización | Entrevista / Checklist | BAI09 | Bajo | Medio | Alto | Obsolescencia de hardware y software |

Continúa en la siguiente página

| Categoría | Vulnerabilidad Identificada | Fuente de hallazgo | Dominio COBIT 2019 | C | I | A | Amenaza Relacionada |
|---|---|---|---|---|---|---|---|
| Gobernanza | Escasa participación de la alta dirección en la definición de políticas de seguridad | Entrevista | EDM02 | Alto | Medio | Bajo | Desalineación con los objetivos estratégicos |
| Gobernanza | Ausencia de roles definidos en la gestión de infraestructura | Entrevista | EDM02 | Bajo | Alto | Medio | Ausencia de un control adecuado sobre la infraestructura |
| Gestión de riesgos | Evaluaciones de riesgos limitadas (1–2 veces/año, sin normativa formal) | Entrevista | APO12 | Medio | Medio | Medio | Falta de identificación temprana de vulnerabilidades |

Continúa en la siguiente página

| Categoría | Vulnerabilidad Identificada | Fuente de hallazgo | Dominio COBIT 2019 | C | I | A | Amenaza Relacionada |
|---|---|---|---|---|---|---|---|
| Cumplimiento | No se aplican estándares ni regulaciones internacionales (COBIT 2019) | Checklist / Entrevista | MEA01 | Alto | Alto | Medio | No cumplimiento de normativas internacionales |
| Usuarios | Falta de capacitación y concienciación en seguridad informática | Encuestas a usuarios y departamentos | APO07, MEA01 | Alto | Medio | Bajo | Error humano en la manipulación de información |
| Exposición externa | Servicios abiertos detectados en el escaneo Nmap (riesgo de ataques externos) | Nmap | DSS05, APO12, MEA01 | Alto | Alto | Medio | Ataques de denegación de servicio (DDoS) |

Del análisis de la Tabla XXXII, se evidencia que las vulnerabilidades encontradas en ella impactan de manera transversal las tres partes críticas de la seguridad de la información: confidencialidad, integridad y disponibilidad (CIA). Sin embargo, las mayores implicaciones se concentran en la disponibilidad e integridad de los servicios del Centro de Datos, debido a la ausencia de estrategias formales para la copia de seguridad, recuperación y mantenimiento preventivo.

Asimismo, la falta de controles de acceso físico y lógico genera riesgos elevados sobre la confidencialidad de la información institucional, exponiendo los sistemas a accesos no autorizados o a manipulación indebida de datos, estas deficiencias reflejan un nivel de madurez bajo en

la gestión de la seguridad de la información, especialmente en los dominios DSS05 (Seguridad de Servicios), DSS04 (Continuidad y Disponibilidad) y APO12 (Gestión de Riesgos) del marco COBIT 2019.

En términos generales, el 70 % de las vulnerabilidades presenta un impacto alto, evidenciando una falta de alineación entre los controles operativos y los principios de seguridad definidos por el marco de referencia, este resultado sugiere la necesidad de fortalecer la gobernanza tecnológica mediante políticas de seguridad documentadas, mecanismos de control automatizados y procesos de auditoría continua orientados a preservar la disponibilidad, integridad y confidencialidad de los activos críticos del Data Center.

### 4.3.4 Mapa de Calor

Con base en la valoración de las vulnerabilidades identificadas y su estimación de impacto, se construyó el mapa de calor de riesgos mostrado en la Fig. 21, este mapa permite visualizar la concentración de los riesgos según su probabilidad de ocurrencia y el impacto potencial sobre la infraestructura tecnológica del Data Center, los datos utilizados para crear este mapa se derivan de la clasificación de las vulnerabilidades según su probabilidad de ocurrencia y el nivel de impacto en los principios de seguridad de la información: confidencialidad, integridad y disponibilidad (CIA), como se evidencia en la Tabla XXXII.

**Justificación de los Datos Utilizados en el Mapa de Calor**

La probabilidad de ocurrencia de cada vulnerabilidad se determinó a partir de los resultados obtenidos en las entrevistas, el análisis de documentación y los escaneos realizados en el Data Center, cada vulnerabilidad fue clasificada en tres niveles de probabilidad:

- Alta: Vulnerabilidades con alta probabilidad de ocurrir debido a la falta de controles, protocolos establecidos o vulnerabilidades conocidas en la infraestructura.
- Media: Vulnerabilidades con probabilidad moderada de ocurrir, es decir no es seguro que ocurra, pero ya ha pasado antes, así que existe riesgo real, basados en incidentes previos.
- Baja: Vulnerabilidades detectadas que pueden ser poco probables, originarias por la falta de medidas preventivas.

El impacto potencial de cada vulnerabilidad se evaluó en función del daño que podría causar a cada principio de seguridad (CIA) si la vulnerabilidad se materializa, el impacto fue clasificado de la siguiente manera:

- Alto: Un impacto significativo en la confidencialidad, integridad o disponibilidad de los datos o servicios del Data Center, que podría paralizar operaciones críticas o comprometer gravemente la seguridad.
- Medio: Un impacto que perjudicaría operaciones fundamentales, pero no interrumpiría la operación completa del sistema y tampoco pondría en serio peligro los datos.
- Bajo: Un impacto menor, que solo puede afectar a las áreas o departamentos no críticos, existiendo un daño mínimo en los datos y en la prestación de servicios.

**Distribución de los Riesgos en el Mapa de Calor**

En el mapa de calor, los riesgos se ubicaron en las áreas correspondientes a su probabilidad y nivel de impacto, la mayoría de los riesgos se encuentran en la zona de alta criticidad, lo que indica que las vulnerabilidades más graves están relacionadas con la seguridad de servicios (DSS05), continuidad operativa (DSS04) y gestión de riesgos (APO12), esto subraya la necesidad urgente de implementar acciones preventivas inmediatas para mitigar estos riesgos.

La Fig. 21 ilustra cómo las principales vulnerabilidades, como la falta de segmentación de red y la ausencia de estrategias de respaldo, se encuentran en áreas de alto impacto y alta probabilidad, lo que resalta la situación crítica de seguridad en el data center, por lo tanto, las acciones de mitigación deben centrarse principalmente en los dominios DSS05, DSS04 y APO12.

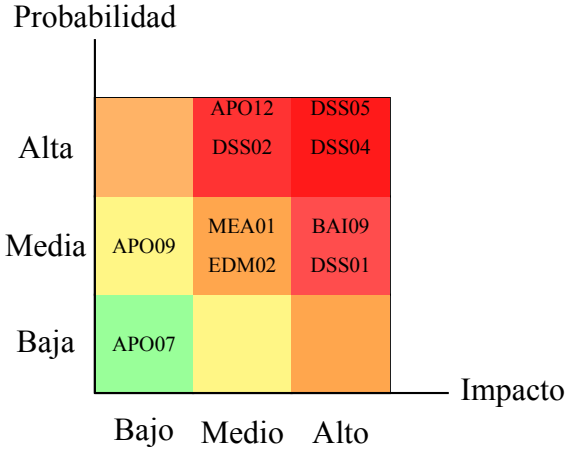


**Fig. 18**. Mapa de calor de riesgos del Data Center según probabilidad e impacto

### 4.3.5 Salvaguardas

Para la evaluación de salvaguardas se utilizo la metodología PILAR, por su enfoque integral en la gestión de riesgos y por su compatibilidad con los marcos normativos internacionales de seguridad de la información, esta herramienta trabaja bajo los lineamientos de la norma ISO/IEC 27002, la cual establece buenas prácticas para la implementación de controles de seguridad orientados a la protección de los activos de información, dicha norma resulta totalmente compatible con los principios de gobernanza y gestión definidos por el marco COBIT 2019, lo que permite mantener una coherencia metodológica en el proceso de evaluación.

**Evaluación de salvaguardas**

La evaluación de salvaguardas se realizó, considerando los riesgos, vulnerabilidades y brechas identificadas en los dominios COBIT 2019 aplicados al Data Center del GAD Municipal del Cantón Bolívar, este proceso permitió definir las medidas de protección necesarias para reducir la probabilidad de ocurrencia de los incidentes y mitigar su impacto sobre la confidencialidad, integridad y disponibilidad de la información institucional.

La herramienta PILAR facilita la definición de niveles de implementación (L1–L5) para cada salvaguarda, donde L1 representa la inexistencia de controles y L5 el estado óptimo de madurez, caracterizado por procesos automatizados, auditados y en mejora [18], en este contexto, las salvaguardas fueron asignadas en función del grado de formalización y aplicación dentro del GAD Municipal del Cantón Bolívar, considerando tanto controles técnicos como administrativos.

Significado de los niveles L0 a L5 de la aplicación PILAR, donde se realizó la evaluación de los activos críticos, tabla XXXIII.

Tabla XXXIII.
NIVELES DE MADUREZ E INTERPRETACIÓN PRÁCTICA, ADAPTADO DE [18].

| **Nivel** | **Descripción** | **Interpretación práctica** |
|---|---|---|
| L0 | Inexistente | No existe ningún tipo de control implementado. |
| L1 | Implementación mínima | El control existe de manera informal o parcial. |
| L2 | Implementación básica | El control está documentado y parcialmente aplicado. |

Cuadro XXXIII– *continuación*

| Nivel | Descripción | Interpretación práctica |
|---|---|---|
| L3 | Implementación completa | El control está completamente implementado y operando. |
| L4 | Gestión activa | El control es monitoreado y revisado regularmente. |
| L5 | Optimización y mejora continua | El control se mejora continuamente con métricas y análisis. |

La Tabla XXXIV presenta la evaluación de las salvaguardas, agrupadas según su naturaleza (gobernanza, técnica o física) y clasificadas por tipo de defensa o protección (TDP), para cada salvaguarda se indica el nivel actual (CURRENT), determinado a partir del diagnóstico de brechas, y el nivel objetivo (TARGET) establecido en función del marco COBIT 2019 y las mejores prácticas internacionales.

Del análisis se evidencia que la mayoría de las salvaguardas críticas se encuentran entre los niveles L1 y L2, lo que indica un grado inicial de implementación, las áreas con mayor necesidad de fortalecimiento corresponden a la seguridad lógica (DSS05), la continuidad operativa (DSS04) y la gestión de riesgos (APO12), donde las brechas alcanzan valores significativos, en estos casos, se recomienda alcanzar niveles de madurez entre L4 y L5, que representan la consolidación de políticas documentadas, procedimientos estandarizados y controles automatizados.

La falta de salvaguardas pone en riesgo directamente la seguridad de los servicios y la continuidad operativa, las salvaguardas de alta prioridad son la identificación y autenticación (IA), el control de acceso lógico (AC), la gestión de incidentes (IM) y la protección física de equipos e instalaciones, paralelamente se identificó la necesidad de fortalecer las estrategias y planificación en el ámbito de capacitación al personal (APO07) y el monitoreo continuo (MEA01), ya que se consideran esenciales para mantener la efectividad del sistema de seguridad.

Tabla XXXIV.
EVALUACIÓN DE SALVAGUARDAS: SITUACIÓN ACTUAL Y NIVELES OBJETIVO SEGÚN METODOLOGÍA PILAR

| Aspecto | TDP | Recomendado | Salvaguarda | Nivel Actual | Nivel Objetivo |
|---|---|---|---|---|---|
| G | EL | 8 | Identificación y autenticación de usuarios (IA) — Implementar sistemas biométricos y contraseñas robustas. | L2 | L4–L5 |
| G | EL | 7 | Control de acceso lógico (AC) - Implementar políticas de acceso basadas en roles y segmentación de la red. | L2 | L4–L5 |
| G | PR | 4 | Protección de la información (INF) - Aplicar medidas de cifrado de datos para proteger los datos en tránsito y en reposo, realizar respaldos seguros, confiables y verificar la integridad de los datos. | L2 | L4 |

| Aspecto | TDP | Recomendado | Salvaguarda | Nivel Actual | Nivel Objetivo |
|---|---|---|---|---|---|
| T | PR | 6 | Protección de claves criptográficas (SC-12) — Establecer una política de gestión y rotación periódica de claves. | L1 | L3–L4 |
| G | PR | 5 | Protección de los servicios (SRV) - Implementar IDS/IPS, firewall avanzado y monitoreo continuo. | L2 | L4–L5 |
| G | PR | 5 | Protección de las aplicaciones informáticas (SW) - Realizar actualizaciones y parcheos periódicos de sistemas y software. | L2 | L4 |
| G | PR | 4 | Protección de los equipos informáticos (HW) - Establecer mantenimientos preventivos y correctivos e implementar un sistema de control ambiental inteligente en el Data Center. | L3 | L4–L5 |

| Aspecto | TDP | Recomendado | Salvaguarda | Nivel Actual | Nivel Objetivo |
|---|---|---|---|---|---|
| G | PR | 4 | Protección de las comunicaciones (COM) - Implementar mecanismos de cifrado VPN y segmentación segura de la infraestructura de las redes. | L2 | L4 |
| G | PR | 4 | Proteger los medios donde se almacena la información (MEDIA) — Emplear almacenamiento mediante cifrado y eliminar los datos de manera controlada y segura. | L2 | L4 |
| A | AUX | 3 | Elementos auxiliares (E-AUX) - Instalar sensores de temperatura,inundación y humo para la mitigación temprana. | L2 | L4 |

| Aspecto | TDP | Recomendado | Salvaguarda | Nivel Actual | Nivel Objetivo |
|---|---|---|---|---|---|
| G | PR | 5 | Protección física de los equipos (PF) - Instalar sistemas de control biométrico, cerraduras electrónicas y cámaras CCTV. | L2 | L4–L5 |
| G | PR | 5 | Protección de las instalaciones (INST) - Implementar sistemas de climatización redundantes y controles de acceso físico. | L3 | L5 |
| G | PR | 5 | Gestión del personal (HR) - Establecer programas de capacitación para definir roles y funciones en materia de seguridad. | L2 | L4 |

| Aspecto | TDP | Recomendado | Salvaguarda | Nivel Actual | Nivel Objetivo |
|---|---|---|---|---|---|
| G | CR | 5 | Gestión de incidentes (IM) - Establecer un protocolo para administrar incidentes, que posibilite la documentación y el registro de cada acción y respuesta ejecutada. | L1 | L4 |
| G | CR | 5 | Gestión de riesgos (RM) — Formalizar metodología periódica de evaluación y tratamiento de riesgos. | L2 | L4–L5 |
| G | PR | 4 | Monitoreo y auditoría (MEA01) - Realizar auditorías periódicas de registros de logs y métricas de rendimiento para garantizar la seguridad del data center. | L2 | L4 |

La Tabla XXXV, se puede observar que existe una relación entre las vulnerabilidades identificadas, los riesgos asociados y los dominios de COBIT 2019, que fueron afectados mediante las salvaguardas propuestas en la metodología PILAR. Indicando el nivel de madurez actual (L1–L2) y el nivel objetivo (L4–L5), siguiendo el modelo de COBIT 2019 que establece la mejora continua.

Tabla XXXV.
RELACIÓN ENTRE VULNERABILIDADES, RIESGOS, DOMINIOS COBIT 2019 Y SALVAGUARDAS PROPUESTAS

| Vulnerabilidad Identificada | Riesgo Asociado | Dominio COBIT 2019 | Salvaguarda Propuesta | Descripción Técnica | Nivel Actual | Nivel Objetivo |
|---|---|---|---|---|---|---|
| Ausencia de controles de acceso físico (biometría, tarjetas, cámaras) | Acceso no autorizado a instalaciones y exposición de información sensible | DSS05, DSS01 | Identificación y autenticación de usuarios (IA) | Implementar sistemas biométricos y contraseñas robustas | L2 | L4–L5 |
| Falta de segmentación de red y monitoreo IDS/IPS | Intrusión no detectada y pérdida de integridad de datos | DSS05 | Control de acceso lógico (AC) | Implementar políticas de acceso basadas en roles y segmentación de red | L2 | L4–L5 |
| Inexistencia de estrategias documentadas de respaldo y recuperación | Pérdida de información crítica y tiempo de inactividad prolongado | DSS04 | Gestión de copias de seguridad (CP) | Definir e implementar procedimientos automáticos de respaldo y restauración | L2 | L4–L5 |

Continúa en la siguiente página

| Vulnerabilidad Identificada | Riesgo Asociado | Dominio COBIT 2019 | Salvaguarda Propuesta | Descripción Técnica | Nivel Actual | Nivel Objetivo |
|---|---|---|---|---|---|---|
| Falta de pruebas de contingencia | Interrupción prolongada de operaciones | DSS04 | Pruebas de continuidad operativa (CO) | Realizar simulacros periódicos de contingencia y recuperación | L2 | L4 |
| Ausencia de mantenimiento y documentación de activos tecnológicos | Fallas recurrentes por obsolescencia o incompatibilidad de sistemas | APO09, BAI09 | Inventario y ciclo de vida de activos (AS) | Actualizar inventario tecnológico e implementar cronogramas de mantenimiento | L2 | L4 |
| Escasa participación de la alta dirección en la definición de políticas | Falta de liderazgo y gobernanza tecnológica | EDM02 | Política de seguridad institucional (PS) | Establecer políticas aprobadas y respaldadas por la alta dirección | L1 | L4 |

Continúa en la siguiente página

| Vulnerabilidad Identificada | Riesgo Asociado | Dominio COBIT 2019 | Salvaguarda Propuesta | Descripción Técnica | Nivel Actual | Nivel Objetivo |
|---|---|---|---|---|---|---|
| Evaluaciones de riesgo limitadas | Subestimación de amenazas y decisiones reactivas | APO12 | Evaluación de riesgos periódica (RA) | Aplicar metodología formal de gestión de riesgos (COBIT 2019, ISO 27005) | L2 | L5 |
| Falta de capacitación del personal en seguridad informática | Errores humanos y brechas operativas | APO07, MEA01 | Programa de concienciación en seguridad (SE) | Desarrollar capacitaciones y auditorías internas anuales | L2 | L4 |
| Servicios abiertos expuestos en internet (Nmap) | Ataques externos y denegación de servicio | DSS05, APO12 | Protección de la información (INF) | Aplicar cifrado de datos en tránsito, firewalls y revisión de puertos | L2 | L5 |

**Determinación de salvaguardas**

La determinación de salvaguardas se realizó con base en los resultados obtenidos del análisis de riesgos y vulnerabilidades del Data Center, aplicando la metodología PILAR (Protección de

Infraestructuras Críticas), este proceso permitió identificar y asociar medidas de control técnico, organizativo y estratégico orientadas a reducir la probabilidad y el impacto de los riesgos identificados en los dominios de COBIT 2019 evaluados.

En la Tabla XXXVI, se puede observar las salvaguardas propuestas y los temas asociados para su determinación entre ellos tenemos:

- Fortalecer la seguridad física y lógica, mediante la implementación de controles inteligentes de acceso biométricos, sistemas integrados de videovigilancia , segmentación de redes y sistemas que ayuden a la detección y prevención de amenazas externas (IDS/IPS).
- Ejecución de políticas de apoyo a la seguridad correctamente documentadas, así como planes de contingencia y pruebas ininterrumpidas de recuperación que garanticen la permanencia de las operaciones y los servicios al interior de la institución.
- Para que exista una mejor gobernanza de TI, se recomienda establecer roles, responsabilidades y funciones bien definidos, mediante la formación de un comité de seguridad que ayude a supervisar los riesgos y controlar los activos tecnológicos.
- Para promover y fortalecer una cultura de seguridad organizacional, se realizará capacitación continua mediante campañas de concienciación dirigidas a todos los empleados con la finalidad de que cada persona sepa cómo proteger la información y cómo actuar ante incidentes.
- Acoplarse a las normas internacionales como la ISO/IEC 27001 y aplicar las mejores prácticas de el marco referencial COBIT 2019.

Tabla XXXVI.
DETERMINACIÓN DE SALVAGUARDAS DEL DATA CENTER SEGÚN METODOLOGÍA PILAR Y COBIT 2019

| **Activo / Proceso** | **Riesgo o Vulnerabilidad Detectada** | **Salvaguarda Propuesta** | **Tipo de Control** | **Dominio COBIT 2019** | **Nivel-(L1–L5)** |
|---|---|---|---|---|---|
| Infraestructura física | Accesos no autorizados al Data Center | Implementación de control de acceso biométrico, CCTV y registro de ingreso | Preventivo | DSS05 – Seguridad de Servicios | L2 |
| Sistemas eléctricos y climatización | Riesgo de sobrecalentamiento por falta de redundancia | Instalación de climatización redundante y sensores de temperatura/humedad | Correctivo | DSS01 – Operaciones | L2 |
| Red de datos | Falta de segmentación de red y políticas de IDS/IPS | Implementación de VLAN, firewall de nueva generación e IDS/IPS centralizado | Preventivo | DSS05 – Seguridad de Servicios | L3 |

*Continúa en la siguiente página*

| Activo / Proceso | Riesgo o Vulnerabilidad Detectada | Salvaguarda Propuesta | Tipo de Control | Dominio COBIT 2019 | Nivel (L1–L5) |
|---|---|---|---|---|---|
| Gestión de respaldos | No existen planes documentados de respaldo o recuperación | Creación de plan de contingencia, política de respaldo y simulacros trimestrales | Correctivo | DSS04 – Continuidad y Disponibilidad | L2 |
| Gestión de riesgos TI | Evaluaciones de riesgo informales y no periódicas | Implantar procedimiento de gestión de riesgos anual con matriz CIA y revisión por dirección | Estratégico | APO12 – Gestión de Riesgos | L2 |
| Activos tecnológicos | Falta de inventario actualizado y control del ciclo de vida | Implementar software CMDB para control de activos y mantenimiento programado | Preventivo | APO09 – Gestión de Activos | L3 |

*Continúa en la siguiente página*

| Activo / Proceso | Riesgo o Vulnerabilidad Detectada | Salvaguarda Propuesta | Tipo de Control | Dominio COBIT 2019 | Nivel (L1–L5) |
|---|---|---|---|---|---|
| Gobernanza de TI | Falta de roles definidos y escasa participación de directivos | Establecer comité de seguridad de TI y roles formales con responsabilidades claras | Organizativo | EDM02 – Asegurar Beneficios | L2 |
| Usuarios internos | Escasa capacitación en seguridad informática | Programa de formación anual en seguridad y manejo de información sensible | Preventivo | APO07 – Gestión del Personal | L3 |
| Monitoreo y auditoría | No existen auditorías internas ni control de cumplimiento normativo | Implementar auditorías semestrales basadas en ISO 27001 y COBIT 2019 | Detectivo | MEA01 – Monitoreo y Evaluación | L2 |
| Servicios expuestos | Puertos abiertos y configuraciones inseguras detectadas con Nmap | Cierre de servicios innecesarios, endurecimiento del sistema y revisión mensual | Correctivo | DSS05 – Seguridad de Servicios | L3 |

*Continúa en la siguiente página*

| Activo / Proceso | Riesgo o Vulnerabilidad Detectada | Salvaguarda Propuesta | Tipo de Control | Dominio COBIT 2019 | Nivel (L1–L5) |
|---|---|---|---|---|---|
| Plataformas críticas | Ausencia de pruebas de continuidad operativa | Simulacros de caída de servicios y validación de tiempos RTO/RPO | Preventivo | DSS04 – Continuidad y Disponibilidad | L2 |
| Mantenimiento de hardware | Riesgo de obsolescencia tecnológica | Plan de renovación de equipos críticos cada 3 años y control de garantías | Correctivo | BAI09 – Gestión de Activos | L3 |
| Cumplimiento normativo | No aplicación de estándares internacionales | Adopción progresiva de ISO/IEC 27001 y políticas basadas en COBIT 2019 | Estratégico | MEA01 – Monitoreo y Evaluación | L2 |

El análisis de madurez evidenció que la mayoría de las salvaguardas se encuentran en un nivel de implementación entre L2 y L3, lo que representa una gestión parcial con controles definidos pero no completamente integrados ni monitoreados, los dominios más críticos corresponden a DSS05 (Seguridad de Servicios), DSS04 (Continuidad y Disponibilidad) y APO12 (Gestión de Riesgos), que requieren priorización inmediata para reducir la exposición ante incidentes de seguridad.

**Matriz de priorización de salvaguardas**

La Tabla XXXVII muestra la priorización de las salvaguardas identificadas, clasificadas por su nivel de impacto en la reducción del riesgo y el costo estimado de aplicación, esta priorización facilita la planificación de la implementación de las medidas de seguridad de forma ordenada, maximizando los recursos institucionales y asegurando la mejora continua del sistema de gestión de seguridad de la información.

Esto se realiza en tres fases para la ejecución:

- **Corto plazo (0–6 meses):** Integración de controles críticos que tengan una alta efectividad y viabilidad inmediata al momento de la ejecución.
- **Mediano plazo (6–12 meses):**Acciones de mejora y fortalecimiento interno para los controles direccionados en la mejora de la organización.
- **Largo plazo (más de 12 meses):**Implementar controles y decisiones estratégicas para mejorar las inversiones tecnológicas de mayor impacto.

La clasificación considera tanto la prioridad de implementación como la relación costo-beneficio, con el fin de asegurar una reducción efectiva del riesgo en los dominios evaluados de COBIT 2019.

Tabla XXXVII.
MATRIZ DE PRIORIZACIÓN DE IMPLEMENTACIÓN DE SALVAGUARDAS SEGÚN PILAR Y COBIT 2019

| **Dominio COBIT 2019** | **Salvaguarda propuesta** | **Impacto** | **Costo estimado** | **Plazo de ejecución** |
|---|---|---|---|---|
| DSS05 – Seguridad de Servicios | Implementar control de acceso físico (biometría, CCTV) y firewall de nueva generación con IDS/IPS integrado. | Alto | Alto | Corto plazo |

| Dominio COBIT 2019 | Salvaguarda propuesta | Impacto | Costo estimado | Plazo de ejecución |
|---|---|---|---|---|
| DSS04 – Continuidad y Disponibilidad | Desarrollar y ejecutar un plan de continuidad del negocio (BCP) y un plan de recuperación ante desastres (DRP) | Alto | Medio | Corto plazo |
| APO12 – Gestión de Riesgos | Definir y formalizar una política de gestión de riesgos de TI en la institución, con evaluaciones periódicas de manera anual. | Alto | Bajo | Corto plazo |
| DSS01 – Operaciones | Instalar sensores ambientales conectados al sistema de monitoreo con alertas automáticas. | Alto | Medio | Mediano plazo |
| DSS02 – Gestión de Incidentes | Definir y ejecutar un procedimiento para la atención y respuesta a la gestión de incidentes, con indicadores de desempeño de manera formal. | Medio | Bajo | Mediano plazo |
| BAI09 – Gestión del Ciclo de Vida de Activos | Establecer políticas de actualización tecnológica y mantenimiento preventivo de infraestructura crítica. | Alto | Alto | Largo plazo |

| Dominio COBIT 2019 | Salvaguarda propuesta | Impacto | Costo estimado | Plazo de ejecución |
|---|---|---|---|---|
| APO09 – Gestión de Activos | Crear un inventario de activos de TI que incluya una codificación única y un control de versiones para el software institucional. | Medio | Bajo | Mediano plazo |
| EDM02 – Asegurar Beneficios | Formar un Comité de Seguridad de la Información liderado por la alta dirección. | Alto | Bajo | Corto plazo |
| APO07 – Gestión del Personal | Ejecutar un programa anual de capacitación en ciberseguridad y buenas prácticas digitales. | Medio | Bajo | Mediano plazo |
| MEA01 – Monitoreo y Evaluación | Implementar auditorías internas y tableros de control (dashboards) para el seguimiento de KPIs de seguridad. | Alto | Medio | Largo plazo |

La Fig. 19 muestra la priorización de las salvaguardas identificadas de acuerdo con su impacto en la mitigación del riesgo y el costo estimado de implementación, siguiendo la metodología PILAR y los lineamientos de COBIT 2019.

Las salvaguardas a corto plazo, que aparecen en color verde, tienen un alto impacto y un coste bajo; por lo tanto, es necesario ponerlas en marcha de inmediato (DSS05, DSS04, APO12, EDM02). Las de mediano plazo se indican con color amarillo y requieren una inversión moderada; pueden llevarse a cabo entre los seis meses y el año siguiente (DSS01, DSS02, APO09, APO07). En cambio, las salvaguardas a largo plazo se identifican con color rojo; tienen costes altos y son complejas. Por eso es recomendable planificarlas para más de un año (BAI09, MEA01).

Esta priorización permite sentar las bases para mejorar gradualmente la seguridad del Data Center, mediante una hoja de ruta que maximice progresivamente los recursos, logrando así un equilibrio entre el costo y la efectividad de las medidas.

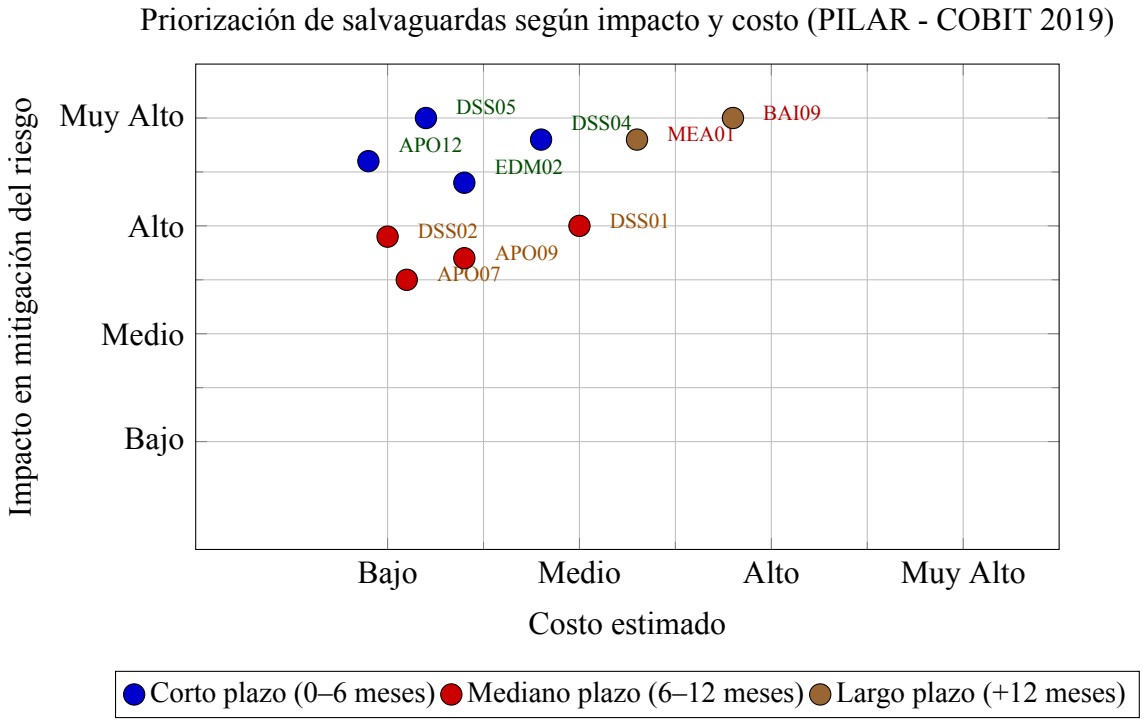


**Fig. 19**. Gráfica de priorización de salvaguardas según impacto, costo y plazo de ejecución

### 4.3.6 Evaluación de los Riesgos

La Fig. 20 se muestra la comparación entre los riesgos antes y después de aplicar las salvaguardas identificadas, la gráfica refleja el cambio en los valores de probabilidad e impacto de los riesgos, utilizando una escala de 0 a 1, donde 1.0 indica un riesgo máximo y 0.0 un riesgo mínimo.

Se puede observar cómo, después de implementar las medidas de mitigación, los riesgos más críticos inicialmente ubicados en las zonas de alta criticidad se han desplazado a zonas de menor impacto y menor probabilidad, esto demuestra que las salvaguardas aplicadas han tenido un impacto positivo, reduciendo significativamente los riesgos en los dominios clave del Data Center.

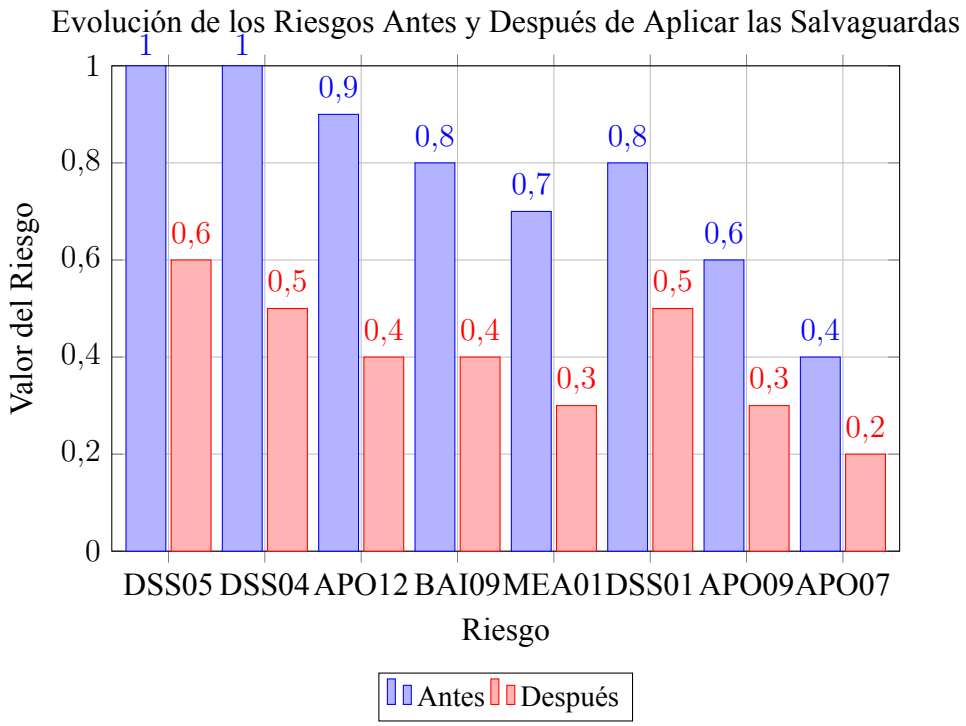


**Fig. 20**. Evalución de los riesgos antes y después de aplicar las salvaguardas en el Data Center

A continuación se muestran los mapas de calor que reflejan la evolución de los riesgos en el data center del GAD municipal de Bolívar, en la Fig.21, se muestra el primer mapa de calor en donde se puede evidenciar la evaluación inicial de los riesgos, clasificados según su impacto y probabilidad, lo que permite identificar las áreas más vulnerables de la infraestructura.

Por otra parte, en la Fig. 22 se muestra el segundo mapa de calor, en el cual se presentan los resultados obtenidos después de implementar las salvaguardas propuestas, así como las mejoras en seguridad, infraestructura y gestión de riesgos, las cuales disminuyeron considerablemente los riesgos en las áreas más críticas, demostrando el éxito de las medidas de seguridad adoptadas.

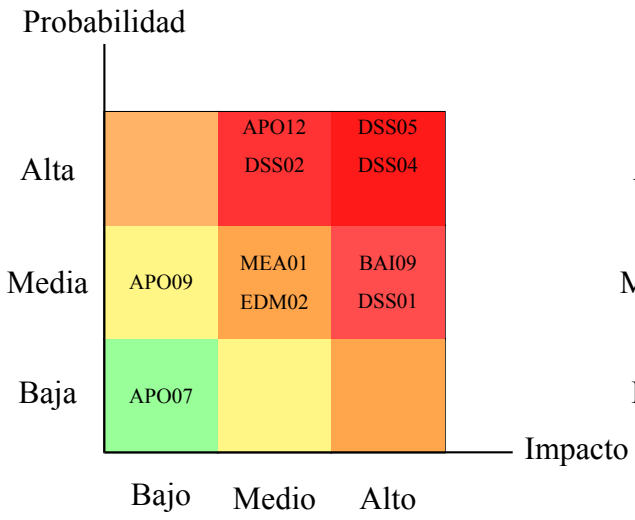


**Fig. 21**. Mapa de calor de riesgos del Data Center según probabilidad e impacto

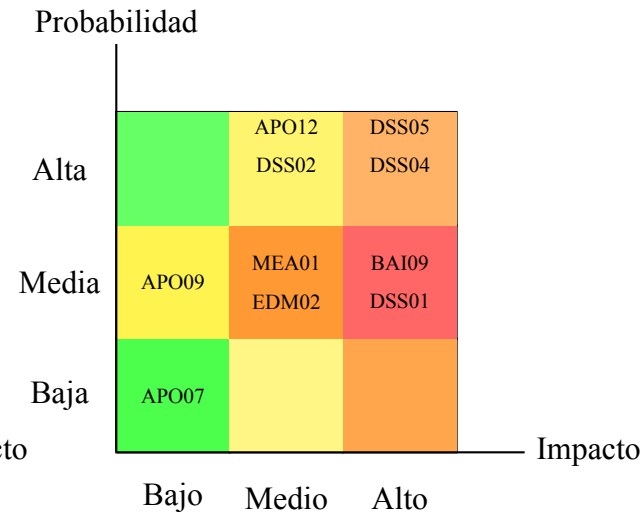


**Fig. 22**. Mapa de calor de riesgos del Data Center luego de aplicar salvaguardas

Se ha demostrado que, después de adoptar las salvaguardas para la infraestructura del centro de datos del GAD municipal, varios aspectos han mejorado significativamente. El primer mapa de calor (Fig. 21) muestra el estado inicial, destacando riesgos de alto impacto y alta probabilidad como los dominios DSS05 y DSS04 que necesitaban una respuesta inmediata.

El segundo mapa de calor (Fig. 22) refleja una reducción en los riesgos tras la implementación de las medidas de seguridad, especialmente en el dominio DSS05, que pasó de alto impacto a bajo impacto con probabilidad media, esto demuestra la efectividad de las salvaguardas.

Después de que se adoptaron las salvaguardias, continúan existiendo riesgos en varios dominios, como por ejemplo el DSS01 y BAI09. Sin embargo, resulta fundamental destacar que este proceso ha ayudado a entender la evaluación y el fortalecimiento de la administración de riesgos, así como la mejora de la madurez de la infraestructura tecnológica, esto hace posible que el GAD Municipal funcione y trabaje con más seguridad y confianza.

### 4.4 Diseño del Plan

El plan de seguridad detallado presentado en la Tabla XLII, integra las debilidades identificadas durante el diagnóstico COBIT 2019 con los hallazgos y salvaguardas priorizadas mediante la herramienta PILAR, cada acción de mejora responde a vulnerabilidades de alto impacto que

afectan la confidencialidad, integridad y disponibilidad de la información institucional, la combinación de ambos marcos permite establecer un enfoque híbrido de gobernanza y seguridad, que garantiza la trazabilidad de riesgos desde su detección hasta su mitigación efectiva.

Las medidas propuestas abarcan desde la implementación de controles técnicos (como firewalls, IDS/IPS, SIEM, segmentación de red) hasta acciones de gestión (comités, capacitación y documentación de procesos), priorizando las de alto impacto y bajo costo según la matriz de priorización, este plan constituye la base operativa para la ejecución del plan de mejora de seguridad del data center del GAD Municipal del cantón Bolívar, orientado a alcanzar un nivel de madurez de 3 a 4 en los dominios evaluados de COBIT 2019.

Tabla XXXVIII.
PLAN DE SEGURIDAD DETALLADO POR DOMINIO COBIT 2019 Y SALVAGUARDAS PRIORIZADAS SEGÚN PILAR

| Dominio COBIT 2019 | Debilidad identificada / Hallazgo PILAR | Impacto | Acción de mejora y salvaguarda propuesta |
|---|---|---|---|
| DSS05 – Seguridad de Servicios | Ausencia de controles de acceso físico (biometría, tarjetas, cámaras) y deficiencias en la seguridad perimetral física. | Alto | Establecer un sistema integral de control de acceso que incluya autenticación biométrica, cámaras IP, registro digital de entradas y salidas, y vigilancia remota, junto con sensores de intrusión y alarmas conectadas a un centro de monitoreo disponible las 24 horas, los 7 días de la semana. |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Debilidad identificada / Hallazgo PILAR | Impacto | Acción de mejora y salvaguarda propuesta |
|---|---|---|---|
| DSS05 – Seguridad de Servicios | Falta de segmentación de red, IDS/IPS y monitoreo en tiempo real. Vulnerabilidades detectadas por servicios expuestos según PILAR. | Alto | Implementar un firewall de nueva generación (NGFW), segmentación de red mediante VLAN, sistemas IDS/IPS y una plataforma SIEM para detección temprana y análisis de eventos, aplicar políticas de bloqueo dinámico ante intentos de intrusión. |
| DSS01 – Operaciones | Deficiencias en los controles ambientales (temperatura, humedad, humo), lo que genera el riesgo de fallas no detectadas en el entorno físico del Data Center. | Alto | Instalar sensores ambientales conectados al sistema de operaciones, con alertas automáticas y monitoreo remoto, y documentar los protocolos de respuesta ante variaciones críticas en el ambiente. |
| DSS04 – Continuidad y Disponibilidad | Inexistencia de estrategias de respaldo y recuperación. Falta de políticas de continuidad detectada en PILAR. | Alto | Crear y poner en marcha un Plan de Continuidad Operativa (PCO) y uno de recuperación ante desastres (DRP) que estén documentados, establecer respaldos automáticos con almacenamiento redundante y llevar a cabo una validación mensual de la restauración. |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Debilidad identificada / Hallazgo PILAR | Impacto | Acción de mejora y salvaguarda propuesta |
|---|---|---|---|
| DSS04 – Continuidad y Disponibilidad | No se llevan a cabo simulacros de contingencia ni se registran las pruebas de recuperación. | Medio | Realizar simulacros semestrales de fallos de sistema y restauración de servicios. Documentar los resultados y acciones correctivas derivadas de cada ejercicio. |
| APO09 – Gestión de Activos | Cableado estructurado que no está organizado, carece de documentación y mantenimiento, lo cual incrementa la posibilidad de que ocurran desconexiones accidentales. | Medio | Establecer un estándar para el cableado estructurado mediante etiquetado físico y digital, integrar los registros en el sistema de gestión de activos (CMDB) y realizar auditorías visuales cada seis meses. |
| BAI09 – Gestión de Activos (procesos específicos) | Existencia de fallas tecnológicas recurrentes ya que no existen políticas establecidas. | Alto | Establecer un sistema automatizado de gestión de activos tecnológicos, que incluya control de inventario, calendario de mantenimiento, actualización de firmware y reemplazo programado de hardware crítico. |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Debilidad identificada / Hallazgo PILAR | Impacto | Acción de mejora y salvaguarda propuesta |
|---|---|---|---|
| EDM02 – Asegurar Beneficios | Limitada participación de la alta dirección y ausencia de políticas de seguridad formalmente establecidas. | Alto | Establecer el comité institucional de seguridad de la información (CSI), con la participación de directivos y responsables de TI, y garantizar la aprobación de políticas y presupuestos de seguridad a nivel estratégico. |
| EDM02 – Asegurar Beneficios | Ausencia de roles definidos en la gestión de infraestructura. Descoordinación y duplicidad de funciones. | Alto | Existe la necesidad de estructurar formalmente el área de Tecnologías de la Información para definir roles y organigramas mediante un manual de funciones de TI, como también de elaborar matrices RACI mediante la asignación de responsabilidades en seguridad, soporte y operaciones. |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Debilidad identificada / Hallazgo PILAR | Impacto | Acción de mejora y salvaguarda propuesta |
|---|---|---|---|
| APO12 – Gestión de Riesgos | Evaluaciones de riesgo no sistemáticas, que se realizan una o dos veces al año, sin ninguna matriz que mida el impacto y la probabilidad. | Medio | Adoptar un proceso de evaluación continua de riesgos siguiendo COBIT 2019 y la metodología PILAR, utilizar matrices de calor para priorizar riesgos y mantener un registro histórico de amenazas, vulnerabilidades y acciones de mitigación. |
| APO12 – Gestión de Riesgos | Exposición de puertos y servicios detectados por escaneo Nmap. Riesgo de explotación remota. | Alto | Desactivar servicios no esenciales, actualizar el firmware y aplicar parches de seguridad críticos, y configurar un monitoreo automatizado para detectar cambios |
| MEA01 – Monitoreo y Evaluación | Falta de auditorías internas y de cumplimiento de estándares. | Alto | Realizar auditorías internas periódicas estimadas cada seis meses, alineadas al marco referencial COBIT 2019 y los estándares ISO/IEC 27001, establecer un cuadro de mando con indicadores clave (KPI) para medir el nivel de madurez de cada proceso. |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Debilidad identificada / Hallazgo PILAR | Impacto | Acción de mejora y salvaguarda propuesta |
|---|---|---|---|
| APO07 – Recursos Humanos | Falta de capacitación y concienciación por parte del personal que labora en el GAD en seguridad de la información, lo que aumenta el riesgo de que ocurran incidentes debido a errores humanos. | Medio | Crear un programa de formación en ciberseguridad, phishing, contraseñas seguras y uso ético de los recursos tecnológicos de manera anual, realizar simulacros de respuesta ante incidentes cada trimestre |
| MEA01 – Monitoreo y Evaluación | Falta de monitoreo completo de logs y correlación de eventos. | Alto | Implementar una plataforma centralizada para el registro y análisis de eventos (SIEM). Establecer procedimientos para la revisión diaria de logs críticos y el escalamiento automático de alertas. |

### 4.4.1 Estructura

La estructura del plan de seguridad se diseñó considerando los resultados del diagnóstico de madurez de COBIT 2019, los hallazgos obtenidos con la herramienta PILAR y las acciones de mejora establecidas en la tabla XLII, esta estructura busca asegurar una implementación ordenada, medible y sostenible del sistema de seguridad de la información del Data Center del GAD Municipal del Cantón Bolívar.

El plan está estructurado en cuatro elementos clave, cada uno con un propósito específico: políticas y procedimientos, capacitación, indicadores de rendimiento (KPIs) y presupuesto, elementos que lo hacen viable y medible.

### 4.4.2 Políticas y procedimientos

Las siguientes políticas se establecen como parte del plan de mejora de la seguridad de la información del Data Center, con el objetivo de mitigar los riesgos detectados en los dominios evaluados de COBIT 2019, cada política responde a las debilidades identificadas durante el diagnóstico y a las salvaguardas priorizadas mediante la herramienta PILAR.

**DSS05 – Seguridad de Servicios (Física y Lógica)**

**Debilidad:** Falta de controles de acceso físico (biometría, cámaras, tarjetas) y deficiencias en la seguridad perimetral.

**Política:** Implementar controles de acceso físico y lógico al data center utilizando tecnologías inteligentes de autenticación biométrica, como cámaras IP y vigilancia perimetral, garantizando así la trazabilidad del ingreso y salidas de personas.

**Procedimiento:**

- Implementar dispositivos biométricos y cámaras con grabación continua en un lapzo de 90 días.
- Elaborar un registro digital de accesos, que será administrado únicamente por el responsable de TI.
- Limitar el acceso a personas desconocidas, será exclusivamente al personal autorizado mediante credenciales individuales.
- Conectar alarmas y sensores de movimiento con notificaciones automáticas.
- Realizar y documentar las revisiones mensuales de los registros de acceso físico y lógico.

**DSS05 – Seguridad de Red**

**Debilidad:** Ausencia de segmentación de la red, IDS/IPS y monitoreo en tiempo real; se detectaron servicios expuestos.

**Política:** Implementar una arquitectura de red segmentada y protegida por un firewall de nueva generación, con monitoreo activo y detección temprana de intrusiones.

**Procedimiento:**

- Configurar VLANs que permitan aislar los entornos críticos y administrativos.
- Implementación de sistemas IDS/IPS junto con una plataforma SIEM para la correlación de eventos de seguridad.
- Realizar escaneos mensuales utilizando herramientas como Nmap para identificar puertos expuestos.
- Desactivar o eliminar servicios no esenciales y registrar los cambios realizados.
- Elaborar reportes semanales de incidentes y análisis de tráfico.

**DSS01 – Operaciones**

**Debilidad:** Ausencia de sensores ambientales y monitoreo del entorno físico del data center.
**Política:** Implementar un control ambiental automatizado que garantice condiciones de operación preventivas y óptimas para evitar fallos por temperatura, humedad o humo.
**Procedimiento:**

- Adquirir e instalar sensores de temperatura, humedad y detección de humo, conectados al sistema de monitoreo.
- Configurar alarmas automáticas en caso de que los parámetros mencionados no se encuentren en el rango de operación normal.
- Obtener mensualmente registros de las condiciones ambientales mencionadas.
- Realizar cada tres meses mantenimientos preventivos en el sistema eléctrico y de climatización de las áreas de operación.

**DSS04 – Continuidad y Disponibilidad**

**Debilidad:** No hay estrategias documentadas de recuperación y respaldo .
**Política:** Asegurar que los servicios tecnológicos sigan funcionando de manera continua, incluso en situaciones imprevistas, mediante la implementación de un Plan de Continuidad Operativa (PCO) y un Plan de Recuperación ante Desastres (DRP) bien definidos y documentados.

**Procedimiento:**

- Configurar los respaldos que se tengan de manera automática diariamente en especial en entornos redundantes, asegurando que los datos estén protegidos en todo momento, incluso en situaciones imprevistas.
- Se realizará las pruebas mensuales pertinentes de restauración para confirmar que las copias de seguridad sean fiables y puedan ser recuperadas rápidamente cuando sea necesario.
- Redactar y mantener una documentación clara y actualizada sobre las políticas de recuperación de datos y las actualizaciones de software, de modo que todo el equipo esté al tanto de los procedimientos a seguir.
- Organizar simulacros de contingencia dos veces al año, con el objetivo de garantizar que el personal esté bien preparado y sepa cómo reaccionar ante situaciones de emergencia.
- Asegurar que las copias de seguridad estén también almacenadas en lugares remotos, fuera de las instalaciones principales, para proteger la información en caso de desastres o situaciones críticas.

**APO09 – Gestión de Activos**

**Debilidad:** Actualmente, se evidencia una desorganización en el cableado estructurado, así como la falta de documentación adecuada, lo que dificulta el control, mantenimiento y la identificación oportuna de incidencias.

**Política:** Establecer un proceso estándar y ordenado para la gestión tanto física como documental del cableado estructurado y de los demás activos tecnológicos, alineado con las mejores prácticas y normas internacionales vigentes.

**Procedimiento:**

- Para comenzar, etiquetar de manera única cada cable, utilizando códigos claros y fácilmente identificables, con el fin de facilitar su localización y mantenimiento.
- Asimismo, registrar en el sistema de gestión de configuración (CMDB) la ubicación exacta y el estado de cada conexión, garantizando un control completo y actualizado de la infraestructura.

- De manera complementaria, actualizar los diagramas de red y la topología de la infraestructura cada seis meses, de modo que reflejen de forma precisa cualquier cambio, ajuste o mejora realizada.

- Por último, realizar inspecciones visuales de los racks y patch-panels al menos dos veces al año, asegurando que el cableado se mantenga organizado y en condiciones óptimas de funcionamiento.

**BAI09 – Ciclo de Vida de Activos**

**Debilidad:** Actualmente, se observa la ausencia de políticas claras y debidamente formalizadas para el mantenimiento y la renovación tecnológica, situación que, con el tiempo, ha provocado la obsolescencia de algunos activos y, en consecuencia, ha incrementado el riesgo de fallos operativos.

**Política:** Establecer un sistema integral que permita gestionar de manera eficiente, ordenada y sostenible todo el ciclo de vida de los activos tecnológicos, comprendiendo desde su adquisición y puesta en operación hasta su desactivación o retiro definitivo.

**Procedimiento:**

- Para comenzar, registrar cada activo tecnológico en el sistema de gestión de configuración (CMDB) desde el momento de su adquisición, garantizando su seguimiento continuo hasta el retiro final y asegurando, en todo momento, la trazabilidad y el control de la información.

- De forma complementaria, planificar y ejecutar mantenimientos preventivos, junto con actualizaciones periódicas de firmware y software, con el objetivo de mantener un rendimiento óptimo y prolongar la vida útil de los activos.

- Adicionalmente, programar la sustitución de equipos críticos considerando criterios como su antigüedad, nivel de desgaste o desempeño, de manera que se prevengan fallos inesperados que puedan afectar la continuidad de los servicios.

- Por último, realizar una revisión anual tanto del inventario de activos como de las políticas de mantenimiento y renovación, asegurando que la infraestructura tecnológica se mantenga actualizada y alineada con las necesidades institucionales.

**EDM02 – Gobernanza y Roles**

**Debilidad:** Se identifica una escasa participación de la alta dirección en los procesos de seguridad de la información, así como la ausencia de roles y responsabilidades claramente definidos, lo que debilita la gobernanza y la toma de decisiones estratégicas en materia de seguridad.
**Política:** Reforzar la gobernanza de la seguridad de la información mediante la creación del Comité Institucional de Seguridad de la Información (CSI), así como a través de la definición clara y formal de roles y responsabilidades, asegurando la participación activa de la alta dirección.
**Procedimiento:**

- En primer lugar, conformar el Comité Institucional de Seguridad de la Información (CSI), integrado por miembros de la alta dirección y responsables del área de TI, con el fin de garantizar una supervisión adecuada y un liderazgo efectivo en materia de seguridad.
- Posteriormente, aprobar de manera anual las políticas de seguridad de la información, el presupuesto asignado y el plan de acción correspondiente, asegurando su alineación con los objetivos institucionales.
- Asimismo, implementar matrices RACI que permitan clarificar de forma precisa las responsabilidades operativas y estratégicas de todos los actores involucrados en la gestión de la seguridad.
- Finalmente, mantener actualizado el manual de funciones del personal de TI, con el propósito de asegurar que todos los roles estén claramente definidos, documentados y comprendidos por los colaboradores.

**APO12 – Gestión del Riesgo**

**Debilidad:** Las evaluaciones de riesgo actuales carecen de una estructura formal y sistemática; además, mediante el uso de la herramienta PILAR, se ha identificado la exposición de varios servicios críticos, lo que incrementa el nivel de vulnerabilidad institucional.
**Política:** Implementar un enfoque continuo, estructurado y ordenado para la gestión del riesgo, integrando la metodología PILAR y alineándose con los principios y buenas prácticas establecidas en COBIT 2019.
**Procedimiento:**

- En primer lugar, construir una matriz de análisis de riesgos que relacione de manera clara el impacto y la probabilidad de ocurrencia de los riesgos identificados.
- Posteriormente, establecer una clasificación por niveles de riesgo (bajo, medio, alto y crítico), basada en su gravedad potencial y en el impacto que podrían generar sobre los procesos institucionales.
- A continuación, definir y aplicar controles preventivos y correctivos que permitan reducir o mitigar los riesgos, priorizando aquellos que representen una mayor amenaza para la organización.
- Asimismo, documentar los riesgos residuales y actualizar, de forma semestral, el mapa de calor que permita visualizar de manera integral la situación general del riesgo.
- Finalmente, compartir los hallazgos y resultados con el Comité Institucional de Seguridad de la Información (CSI), con el fin de que sean revisados, validados y considerados en la toma de decisiones estratégicas.

**APO07 – Recursos Humanos**

**Debilidad:** Se evidencia una falta de capacitación estructurada en ciberseguridad, así como una conciencia limitada del personal respecto a los riesgos asociados al uso de los sistemas de información, lo que incrementa la probabilidad de incidentes de seguridad.

**Política:** Implementar un programa continuo y sistemático de formación en seguridad de la información dirigido a todo el personal, con el propósito de fortalecer las competencias, promover una cultura organizacional de prevención y fomentar prácticas responsables orientadas a la protección de los activos de información.

**Procedimiento:**

- En primer lugar, se debe crear un calendario anual de capacitaciones, con el objetivo de garantizar que todos los empleados reciban formación continua y actualizada en temas de ciberseguridad.
- Asimismo, se debe incluir contenidos esenciales como el uso de contraseñas seguras, la identificación de ataques de phishing y el manejo responsable y seguro del correo electrónico, los cuales constituyen principios fundamentales de la ética digital.

- De manera complementaria, es necesario organizar simulacros de ciberataques, preferentemente cada tres meses, con el fin de poner a prueba la preparación, reacción y nivel de conciencia del personal frente a posibles incidentes de seguridad.

- Finalmente, se debe realizar una evaluación detallada de los resultados obtenidos en los simulacros, reforzando de forma oportuna aquellos temas en los que se evidencie un menor nivel de desempeño o comprensión.

**MEA01 – Monitoreo y Evaluación**

**Debilidad:** Se evidencia la falta de auditorías internas realizadas de manera regular, así como la ausencia de un monitoreo efectivo y continuo de logs y eventos críticos, lo que limita la detección oportuna de incidentes de seguridad.

**Política:** Garantizar una supervisión continua, sistemática y efectiva de los sistemas y procesos tecnológicos, mediante la ejecución de auditorías internas periódicas y la implementación de un monitoreo centralizado de eventos de seguridad.

**Procedimiento:**

- En primer lugar, implementar una plataforma SIEM que permita realizar análisis avanzados y la correlación de eventos en tiempo real, facilitando la detección temprana de amenazas.

- De manera continua, monitorear diariamente los logs críticos de servidores y firewalls, con el propósito de identificar comportamientos anómalos o posibles incidentes de seguridad.

- Asimismo, realizar auditorías internas de forma semestral, alineadas con los lineamientos de COBIT 2019 e ISO 27001, a fin de evaluar el nivel de cumplimiento normativo y el desempeño de los controles implementados.

- Adicionalmente, definir e implementar indicadores clave de rendimiento (KPI) que permitan medir de manera objetiva el cumplimiento de las políticas y el grado de madurez de los controles de seguridad.

- Finalmente, documentar de forma detallada todos los hallazgos derivados de las auditorías y desarrollar planes de acción correctivos, orientados a mitigar y corregir las vulnerabilidades identificadas.

### 4.4.3 Capacitación

La fase de capacitación tiene como objetivo fortalecer las competencias del personal técnico y administrativo en materia de seguridad de la información, asegurando la correcta aplicación de las políticas establecidas en el plan de mejora, se busca crear una cultura institucional orientada a la prevención, la respuesta ante incidentes y la gobernanza efectiva de TI, alineada con COBIT 2019.

A continuación, en la Tabla XXXIX se ilustra la estructura el plan de capacitación en seguridad de la información.

Tabla XXXIX.
ESTRUCTURACIÓN DEL PLAN DE CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

| **Módulo** | **Tema** | **Duración** | **Modalidad** | **Objetivo principal** |
|---|---|---|---|---|
| 1 | Introducción a la seguridad de la información | 20 min | Exposición | Sensibilizar al personal sobre la importancia de la protección de la información institucional y los riesgos asociados al manejo inadecuado de datos. |

*Continúa en la siguiente página*

| Módulo | Tema | Duración | Modalidad | Objetivo principal |
|---|---|---|---|---|
| 2 | Identificación de amenazas y vulnerabilidades comunes | 25 min | Estudio de casos prácticos | Hacer que le personal que labora en el GAD, aprenda a identificar las amenazas más frecuentes, como el phishing, el malware y los accesos no autorizados, como también desarrollar habilidades para detectarlas en el entorno laboral. |
| 3 | Gestión de contraseñas y autenticación segura | 20 min | Demostración práctica | Instruir sobre las mejores prácticas para crear, almacenar y actualizar contraseñas seguras, así como integrar el uso de autenticación multifactor para mejorar la seguridad. |

*Continúa en la siguiente página*

| Módulo | Tema | Duración | Modalidad | Objetivo principal |
|---|---|---|---|---|
| 4 | Continuidad operativa y copias de seguridad | 25 min | Taller guiado | Capacitar al personal en la realización de respaldos automáticos y en los pasos del procedimiento de restauración ante incidentes. |
| 5 | Manejo seguro de equipos y cableado estructurado | 20 min | Práctica supervisada | Concienciar al personal de las buenas practicas sobre los bienes, para que hagan un uso correcto y adecuado de los equipos y estén en la capacidad de realizar un mantenimiento preventivo y ayuden a asegurar el etiquetado correcto de los activos tecnológicos. |

*Continúa en la siguiente página*

| Módulo | Tema | Duración | Modalidad | Objetivo principal |
|---|---|---|---|---|
| 6 | Clasificación y manejo de la información sensible | 20 min | Actividad grupal | Esta medida busca definir los diferentes niveles de confidencialidad de la información así como reforzar el cumplimiento de políticas de acceso basadas en roles, con el fin de prevenir accesos no autorizados y garantizar la protección de la información institucional. |
| 7 | Evaluación y reporte de incidentes de seguridad | 25 min | Simulación | Simular escenarios reales de incidentes de seguridad, capacitando en el uso del formato de reporte y escalamiento de incidentes al comité de seguridad. |

*Continúa en la siguiente página*

| Módulo | Tema | Duración | Modalidad | Objetivo principal |
|---|---|---|---|---|
| 8 | Cultura de seguridad y gobernanza institucional | 20 min | Panel participativo | Impulsar la comunicación efectiva mediante el refuerzo de responsabilidades al personal encargado de la gobernanza de TI, creando un comité de seguridad que promueva la mejora continua. |

**Materiales de apoyo:**

- Manual del usuario con políticas y procedimientos de seguridad
- Guía de configuración de equipos
- Plantilla para el informe de reporte de incidentes de seguridad
- Folletos para clasificar la información
- Guía para la copia de seguridad y recuperación de datos

**Evaluación:** Al terminar cada sesión de capacitación, se llevará a cabo una evaluación corta en un lapso de tiempo de 5 a 10 minutos mediante cuestionarios digitales para que puedan ser realizados desde sus dispositivos móviles, y cuando sea el caso se realizara ejercicios prácticos con el fin de valorar la comprensión del contenido y detectar áreas que necesitan ser mejoradas.

### 4.4.4 KPIs - Key Performance Indicators

Con el propósito de evaluar la efectividad de las acciones implementadas en el plan de seguridad, se definieron indicadores clave de desempeño (KPIs) alineados a los dominios COBIT 2019 y las salvaguardas priorizadas mediante PILAR, estos indicadores permitirán medir el avance, identificar desviaciones y asegurar la mejora continua de los procesos críticos del Data Center, tal como se preseta en la Tabla XL.

Tabla XL.
INDICADORES CLAVE DE DESEMPEÑO (KPI) PARA EL SEGUIMIENTO DEL PLAN DE SEGURIDAD

| Dominio COBIT 2019 | Indicador | Fórmula de cálculo | Línea base estimada | Meta (Target) | Frecuencia | Fuente de verificación |
|---|---|---|---|---|---|---|
| DSS05 | Porcentaje de accesos controlados correctamente | $\frac{\text{Accesos autorizados}}{\text{Accesos totales}} \times 100$ | 75 % | 98 % | Mensual | Registros del sistema biométrico / CCTV |
| DSS05 | Detección de intentos de intrusión bloqueados | $\frac{\text{Eventos bloqueados}}{\text{Intentos totales detectados}} \times 100$ | 60 % | 95 % | Mensual | Reportes del SIEM / IDS–IPS |
| DSS04 | Cumplimiento del plan de respaldo y recuperación | $\frac{\text{Copias válidas verificadas}}{\text{Copias programadas}} \times 100$ | 50 % | 100 % | Trimestral | Registros de respaldo / Bitácoras del DRP |
| DSS04 | Ejecución de simulacros de contingencia | $\frac{\text{Simulacros realizados}}{\text{Simulacros planificados}} \times 100$ | 0 % | 100 % | Semestral | Reportes de pruebas y simulacros |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Indicador | Fórmula de cálculo | Línea base estimada | Meta (Target) | Frecuencia | Fuente de verificación |
|---|---|---|---|---|---|---|
| DSS01 | Tiempo medio de respuesta ante alertas ambientales (minutos) | $\frac{\text{Tiempo total de respuesta}}{\text{Número de incidentes}}$ | 30 min | 10 min | Trimestral | Registros del sistema ambiental |
| APO09 | Porcentaje de activos documentados en el inventario | $\frac{\text{Activos registrados}}{\text{Activos totales}} \times 100$ | 65 % | 100 % | Trimestral | Sistema CMDB / auditorías internas |
| BAI09 | Cumplimiento del plan de mantenimiento preventivo | $\frac{\text{Mantenimientos realizados}}{\text{Mantenimientos programados}} \times 100$ | 40 % | 95 % | Trimestral | Registros del sistema de mantenimiento |
| EDM02 | Nivel de cumplimiento de políticas aprobadas por la alta dirección | $\frac{\text{Políticas aprobadas}}{\text{Políticas propuestas}} \times 100$ | 30 % | 100 % | Semestral | Actas del Comité de Seguridad |

*Continúa en la siguiente página*

| Dominio COBIT 2019 | Indicador | Fórmula de cálculo | Línea base estimada | Meta (Target) | Frecuencia | Fuente de verificación |
|---|---|---|---|---|---|---|
| APO12 | Evaluaciones de riesgo realizadas conforme al calendario | $\frac{\text{Evaluaciones ejecutadas}}{\text{Evaluaciones planificadas}} \times 100$ | 50 % | 100 % | Semestral | Informes de análisis de riesgo |
| MEA01 | Cumplimiento del programa de auditorías internas | $\frac{\text{Auditorías ejecutadas}}{\text{Auditorías planificadas}} \times 100$ | 40 % | 100 % | Semestral | Informes de auditoría / evidencia documental |
| APO07 | Porcentaje de personal capacitado en seguridad de la información | $\frac{\text{Personal capacitado}}{\text{Total de personal}} \times 100$ | 40 % | 100 % | Semestral | Registro de capacitaciones / asistencia |
| MEA01 | Porcentaje de logs analizados y correlacionados | $\frac{\text{Logs revisados}}{\text{Logs generados}} \times 100$ | 30 % | 90 % | Mensual | Plataforma SIEM / informes técnicos |

La Fig. 23 presenta la comparación entre la línea base obtenida del diagnóstico inicial y las metas proyectadas para los indicadores KPI definidos en el plan de seguridad, se observa

que los dominios DSS05 (Seguridad de Servicios) y DSS04 (Continuidad y Disponibilidad) presentan los mayores márgenes de mejora, reflejando la necesidad de fortalecer los controles físicos, lógicos y de respaldo.

En contraste, los dominios APO09 (Gestión de Activos) y APO12 (Gestión de Riesgos) muestran avances más rápidos, ya que dependen principalmente de procesos administrativos y normativos, este gráfico funcionará como una herramienta visual de control para seguir el cumplimiento de los objetivos establecidos y la madurez progresiva de la gobernanza de TI.

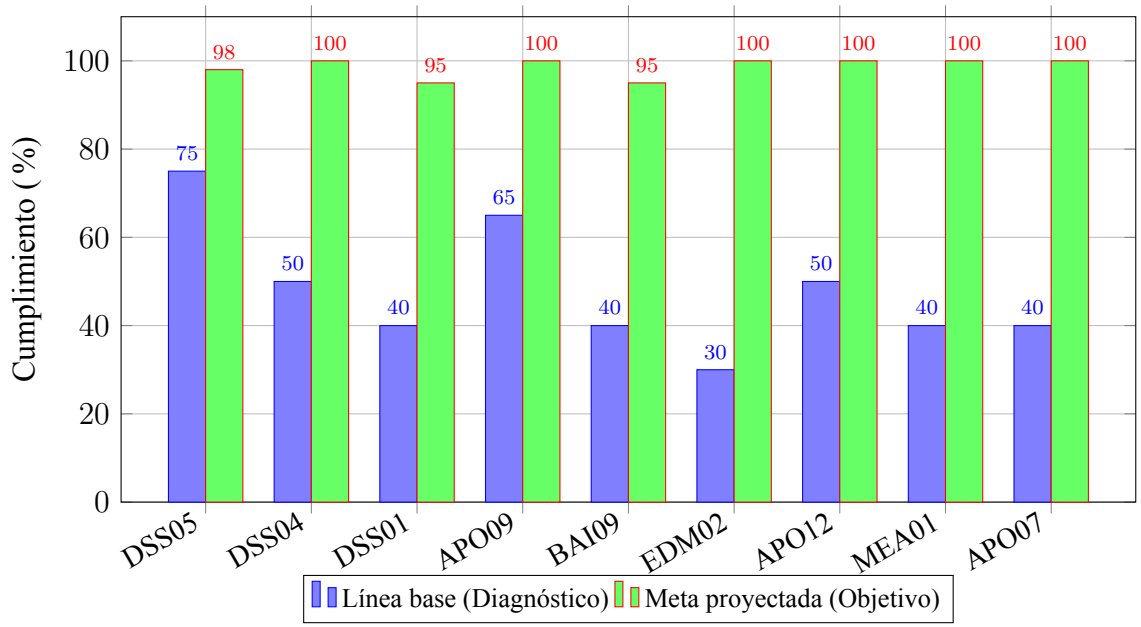


**Fig. 23**. Comparación entre línea base y meta proyectada de los indicadores KPI por dominio COBIT 2019

### 4.4.5 Presupuesto

El presupuesto estimado considera la implementación progresiva del plan de seguridad propuesto y de las acciones de mejora identificadas en el diagnóstico, priorizando las salvaguardas de corto y mediano plazo según el marco COBIT 2019, en la Tabla XLI, se incluyen costos asociados a infraestructura física, licencias de software, capacitación del personal y auditorías de cumplimiento, garantizando la sostenibilidad técnica y operativa del plan.

Tabla XLI.
PRESUPUESTO ESTIMADO AJUSTADO AL MERCADO ECUATORIANO

| Categoría | Descripción | Plazo | Costo estimado (USD) |
|---|---|---|---|
| Infraestructura física | cámaras + sensores + control biométrico | Corto | 8,000 |
| Seguridad lógica / red | firewall NGFW + licencias + segmentación | Corto | 12,000 |
| Continuidad y respaldo | servidores de respaldo, almacenamiento, DRP | Mediano | 6,500 |
| Gestión de activos | cableado, CMDB, inventario digital | Mediano | 3,500 |
| Gobernanza / roles | comisión, manuales, RACI | Corto | 1,800 |
| Capacitación | cursos, talleres, materiales | Mediano | 3,000 |
| Monitoreo / auditoría | auditorías internas y licencias SIEM | Largo | 2,500 |
| Soporte / mantenimiento | licencias renovaciones, soporte técnico | Largo | 3,200 |
| **Total estimado** | | | **40,500** |

El presupuesto total estimado para la ejecución del plan asciende a **USD 40,500**, distribuido en un horizonte de implementación de 12 a 18 meses, el desglose permite priorizar inversiones críticas en infraestructura y seguridad lógica en los primeros seis meses, garantizando resultados medibles en la reducción de brechas y fortalecimiento de la gobernanza de TI.

## 4.5 Validación

### 4.5.1 Aplicación de la Metodología Delphi

Como parte de la estructura del plan, la validación del plan de seguridad informática propuesto para el Data Center del GAD Municipal del Cantón Bolívar se realizó mediante la Metodología Delphi, seleccionada por su eficacia para obtener consenso entre expertos en áreas técnicas y de gestión, este método se aplicó con el propósito de asegurar que el plan fuera coherente, pertinente y viable dentro del marco de COBIT 2019, permitiendo incorporar perspectivas especializadas en seguridad de la información, gobernanza de TI y gestión de riesgos. De acuerdo con Ramírez Chávez y Ramírez Torres [59], la metodología Delphi constituye una herramienta de investigación estructurada que facilita la construcción de consenso a través de la opinión de expertos, bajo un proceso iterativo y anónimo que minimiza sesgos de influencia, su uso es especialmente apropiado en investigaciones aplicadas que requieren la validación de modelos o propuestas técnicas en contextos complejos, como la seguridad de infraestructuras tecnológicas.

La aplicación de esta metodología se desarrolló en dos rondas sucesivas de evaluación, en las cuales siete expertos analizaron los componentes del plan, las salvaguardas propuestas y su alineación con los dominios de COBIT 2019, cada participante emitió su valoración de manera independiente y anónima, lo que permitió mantener objetividad en las respuestas, entre ambas rondas se realizó una retroalimentación sistemática que permitió afinar los criterios y consolidar observaciones hasta alcanzar un nivel aceptable de consenso superior al 70 por ciento.

La selección de los siete expertos se llevó a cabo con base en criterios de idoneidad profesional y experiencia técnica, tomando en cuenta los siguientes aspectos:

- Formación académica en áreas relacionadas con ingeniería, ciberseguridad o tecnologías de la información.
- Experiencia verificable en la gestión, auditoría o administración del data center.
- Participación previa en proyectos de evaluación o gobernanza, en donde se haya utilizado marcos como COBIT, ISO/IEC 27001 u otros que estén a la vanguardia.
- Disponibilidad y compromiso para participar en el proceso de validación.

De esta forma, la metodología Delphi permitió obtener una evaluación integral y fundamentada del plan propuesto, asegurando su alineación con los principios.

## 4.6 Documentación de recomendaciones

A partir de las observaciones proporcionadas por los expertos, se llevaron a cabo modificaciones significativas en el plan de seguridad informática del data center del GAD municipal del cantón Bolívar, mejorando su alineación con los principios de COBIT 2019, el resultado del análisis conjunto permitió identificar áreas clave que requerían atención. relacionadas con los controles físicos, la gestión de riesgos, la continuidad operativa, la gobernanza y la documentación de procesos, las principales mejoras implementadas se detallan a continuación.

**1. Fortalecimiento de controles físicos y ambientales (DSS05, DSS01)**

Se incorporaron dispositivos biométricos y cámaras IP con grabación continua de 90 días, además de un sistema de monitoreo ambiental automatizado con sensores de temperatura, humedad y humo conectados al sistema central del Data Center, sstas medidas garantizan una protección integral de la infraestructura física y minimizan el riesgo de fallas por condiciones adversas.

**2. Segmentación de red y monitoreo inteligente**

En respuesta a la ausencia de una arquitectura segmentada y monitoreo continuo, se implementaron VLANs dedicadas, IDS/IPS y una plataforma SIEM que permite correlacionar eventos en tiempo real,con ello se incrementó la capacidad de detección temprana de amenazas y se redujo la exposición de servicios externos.

**3. Gestión de respaldos y continuidad operativa (DSS04)**

Se implementaron respaldos automáticos diarios, junto con simulacros semestrales y pruebas de restauración documentadas para garantizar la integridad de los datos, ademas las copias externas se almacenan en ubicaciones seguras, de acuerdo con procedimientos aprobados por el Comité de Seguridad de la Información (CSI), fortaleciendo así los Planes de Continuidad Operativa (PCO) y Recuperación ante Desastres (DRP).

**4. Gestión documental y trazabilidad de activos (APO09, BAI09)**

Se implementó un sistema CMDB para el registro digital de todos los activos, con etiquetado QR y actualización automática de topología cada vez que ocurre un cambio estructural,Además se definió un plan de mantenimiento preventivo y renovación tecnológica, garantizando la trazabilidad y disponibilidad de la infraestructura tecnológica.

**5. Gobernanza y fortalecimiento institucional (EDM02)**

Se realizó el Comité de Seguridad de la Información (CSI) que tiene representación ejecutiva, con roles bien definidos a través de una matriz RACI implementando sesiones trimestrales para la aprobación de políticas y presupuestos, donde este organismo actúe como garante de la implementación de controles y revisión continua del plan.

**6. Gestión de riesgos bajo la metodología PILAR (APO12)**

Se consolidó una matriz de impacto-probabilidad estructurada en los niveles bajo, medio, alto y crítico, los riesgos residuales se revisan semestralmente y se presentan al CSI para su validación, esta práctica combina los criterios técnicos de COBIT 2019 con la filosofía de mejora continua de ISO/IEC 27002.

**7. Auditoría y monitoreo continuo (MEA01)**

Se definieron auditorías internas semestrales y la revisión diaria de logs críticos del SIEM, generando reportes automatizados de incidentes y métricas de madurez, esta integración permite una visión proactiva de la seguridad operativa y el cumplimiento de controles.

**8. Capacitación y concienciación del personal (APO07)**

Se diseñó un calendario anual de formación en ciberseguridad que incluye simulacros de respuesta ante incidentes, talleres de buenas prácticas y evaluaciones de desempeño, esto busca consolidar una cultura de seguridad dentro del GAD Municipal.

### 4.6.1 Plan de mejoras a partir de la Evaluación

Después de aplicar la metodología Delphi con la participación de siete expertos en ciberseguridad, gobernanza y gestión tecnológica, se realizó la validación del plan de seguridad informática propuesto para el Data Center del GAD Municipal del Cantón Bolívar, este proceso permitió analizar los resultados obtenidos en los nueve dominios evaluados del marco de referencia COBIT 2019, los cuales comprenden tanto controles técnicos como administrativos.

Basado en las observaciones, sugerencias y evaluaciones realizadas por los expertos, se redactó un plan de mejoras, que tiene la finalidad de aumentar la madurez institucional, reducir los riesgos identificados y mejorar la disponibilidad, integridad y confidencialidad de la información.

En la Tabla XLII se presentan los resultados detallados por dominio, junto con las debilidades detectadas y las políticas de mejora correspondientes derivadas de la validación técnica realizada.

Tabla XLII.
EVALUACIÓN POR DOMINIO COBIT 2019 Y PROPUESTAS DE MEJORA

| **COBIT 2019** | **Criterio de Evaluación** |
|---|---|
| **DSS05** | **Gestión de Servicios de Seguridad** |
| **Debilidad detectada:** | 1. Se evidencia la falta de controles físicos y deficiencias en la seguridad perimetral que permiten la exposición de servicios y activos críticos sin protección adecuada, incrementando el riesgo de accesos no autorizados y vulneraciones a la infraestructura.<br>2. Se detecta una segmentación inadecuada de la red, acompañada de la falta de sistemas para la detección, prevención y monitoreo continuo, lo que deja expuestos los servicios, sin medidas de seguridad, elevando así el riesgo de accesos no autorizados o ataques externos. |
| *Continúa en la siguiente página* | |

| COBIT 2019 | Criterio de Evaluación |
|---|---|
| **Políticas de mejora:** | 1. Se necesita implementar dispositivos biométricos y cámaras de seguridad con grabación continua durante un periodo de tiempo de 90 días.<br>2. Establecer un registro digital de accesos, que será administrado únicamente por el responsable o encargado del área de TI.<br>3. Limitar el acceso únicamente al personal autorizado mediante credenciales únicas.<br>4. Integrar alarmas y sensores de movimiento con notificación automática.<br>5. Realizar una revisión mensual de los registros de acceso físico y lógico.<br>6. Configuración de los VLANs que ayuden aislar los entornos críticos y administrativos.<br>7. Implementación de sistemas IDS/IPS en conjunto de una plataforma SIEM para realizar la correlación de eventos.<br>8. Es importante la ejecutación de escaneos mensuales utilizando herramientas como Nmap para identificar puertos expuestos.<br>9. Bloquear o eliminar servicios innecesarios y documentar todos los cambios.<br>10. Elaborar reportes semanales sobre incidentes y análisis de tráfico. |
| **DSS01** | **Gestionar las Operaciones** |

*Continúa en la siguiente página*

| COBIT 2019 | Criterio de Evaluación |
|---|---|
| **Debilidad detectada:** | 1. Carencias en el monitoreo ambiental del data center, debido a la ausencia de sistemas automatizados capaces de detectar variaciones de temperatura, humedad y presencia de humo, lo que incrementa el riesgo de fallos no detectados en el entorno físico y comprometería gravemente la continuidad operativa. |
| **Políticas de mejora:** | 1. Se requiere instalar sensores para monitorear temperatura, humedad y detectar humo, que estén integrados al sistema de monitoreo.<br>2. Se debe configurar alertas automáticas cuando los valores se encuentren fuera de los rangos permitidos.<br>3. Registrar las condiciones ambientales de manera mensual.<br>4. Realizar mantenimiento preventivo y correctivo de manera trimestral del sistema eléctrico y de climatización. |
| **DSS04** | **Gestión de Continuidad y Disponibilidad** |
| **Debilidad detectada:** | 1. Falta de estrategias debidamente documentadas para el respaldo y recuperación de los datos. |
| **Políticas de mejora:** | 1. Realizar copias de seguridad automáticas todos los días en entornos redundantes.<br>2. Realizar pruebas mensuales de restauración para comprobar la integridad de las copias de seguridad.<br>3. Documentar las políticas relacionadas con la recuperación de datos y actualizaciones de software.<br>4. Realizar simulacros de contingencia de manera periódica cada seis meses. |

*Continúa en la siguiente página*

| COBIT 2019 | Criterio de Evaluación |
|---|---|
| | 5. Para garantizar la continuedad se recomienda realizar copias de seguridad en ubicaciones remotas seguras (off-site), mediante verificaciones periódicas que garanticen la integridad y pruebas regulares de restauración. |
| **APO09** | **Gestión de Activos** |
| **Debilidad detectada:** | Cableado estructurado desorganizado y la ausencia de documentación adecuada. |
| **Políticas de mejora:** | 1. Para una identificación clara, se requiere etiquetar los cables con códigos únicos según su funcionamineto.<br>2. Registrar en el sistema CMDB (Configuration Management Database) la ubicación y el estado de cada conexión de red, asegurando trazabilidad, control de cambios y una respuesta eficiente ante incidentes.<br>3. Actualizar los planos de red y la topología cada seis meses para reflejar cualquier cambio.<br>4. Realizar inspecciones visuales de los racks y patch-panels de manera semestral para asegurar su buen estado. |
| **EDM02** | **Gobernanza y Roles** |
| **Debilidad detectada:** | Existe una baja participación en la alta dirección y deficiencia en roles claramente los de seguridad ya que no se en encuentran claramen definidos. |
| **Políticas de mejora:** | 1. Es necesario establecer el Comité Institucional de Seguridad de la Información (CSI), que este compuesto por directivos y los responsables de TI. |

*Continúa en la siguiente página*

| COBIT 2019 | Criterio de Evaluación |
|---|---|
| | 2. Aprobarción de manera anualmente las políticas establecidas, el determinar el presupuesto para el plan de seguridad.<br><br>3. Implementación de matrices RACI donde se defina claramente cuales son las funciones operativas y estratégicas, que garanticen tener un rfesponsabel en cada tarea crítica, tomando encuenta cada una de las decisiones estratégicas que se tomen con información precisa y participación adecuada.<br><br>4. Actualización constante del manual de funciones para el personal de TI. |
| **APO12** | **Gestión de Riesgos** |
| **Debilidad detectada:** | Las evaluaciones no se encuentran estructuradas y exite una alta exposición de los servicios el cual fue identificados por PILAR. |
| **Políticas de mejora:** | 1. Desarrollar una matriz de impacto y probabilidad para los riesgos identificados y áreas afectadas.<br><br>2. Clasificación de los riesgos mediante niveles que pueden ser, bajo, medio, alto y crítico.<br><br>3. Aplicación de controles preventivos que ayuden a mitigar riesgos según su prioridad.<br><br>4. Documentación de los riesgos residuales encontrados, para realizar la actualización del mapa de calor por lo menos cada seis meses.<br><br>5. Presentación de los resultados al CSI donde se pueda realizar la revisión y validación de resultados. |

*Continúa en la siguiente página*

| COBIT 2019 | Criterio de Evaluación |
|---|---|
| **MEA01** | **Monitoreo y Evaluación** |
| **Debilidad detectada:** | Falta de auditorías internas regulares y control en el monitoreo de logs y eventos. |
| **Políticas de mejora:** | 1. Implementar una plataforma SIEM que permita realizar el análisis y correlación de eventos malintencionados en tiempo real.<br>2. Realizar el monitoreo diario de los logs críticos en los servidores y firewalls.<br>3. Llevar a cabo controles internos como auditorias semestrales siguiendo el marco COBIT 2019.<br>4. Definir métricas e indicadores que ayuden a medir el desempeño, evaluar los resultados y verificar el cumplimiento de los objetivos estratégicos.<br>5. Documentación los hallazgos encontrados y ejecutar planes de acción correctivos para abordar las deficiencias. |
| **APO07** | **Gestión de Recursos Humanos** |
| **Debilidad detectada:** | Falta de capacitación en seguridad informática y baja concienciación sobre los riesgos y consecuencias. |
| **Políticas de mejora:** | 1. Establecer un cronográma anual de capacitación en seguridad informática para todo el personal del GAD.<br>2. Incluir temas clave como contraseñas seguras, phishing, uso responsable del correo electrónico y ética digital.<br>3. Realizar simulacros de ciberataques trimestrales para evaluar la capacidad de respuesta del personal. |

*Continúa en la siguiente página*

| COBIT 2019 | Criterio de Evaluación |
|---|---|
| | 4. Revisar los resultados obtenidos en las capacitaciones y fortalecer aquellos temas en los que se evidencie un menor nivel de desempeño. |
| **BAI09** | **Gestión de Activos (procesos específicos)** |
| **Debilidad detectada:** | No se cuenta con un plan formal para la gestión del ciclo de vida de los activos tecnológicos, lo cual ha provocado la obsolescencia de los equipos y un control limitado en los procesos de mantenimiento y renovación. |
| **Políticas de mejora:** | 1. Registro de los activos en el sistema CMDB qu empiece desde su adquisición y termine en su retiro final.<br>2. Planificación y mantenimientos preventivos mediante actualizaciones periódicas de firmware.<br>3. Realizar cornogramas de sustitución de equipos críticos tomando encuenta antigüedad o rendimiento.<br>4. Revisar el inventario de forma anual y ajustar las políticas de renovación según las necesidades identificadas. |

## 4.7 Análisis de datos

### Análisis Estadístico de la Validación por Expertos

A partir de las calificaciones otorgadas por los siete expertos en la primera ronda, y considerando que el nivel de calificación tiene un máximo de 5 puntos, se calcularon los valores de promedio, desviación estándar, coeficiente de variación (CV), índice de aceptación (IA) y nivel de consenso por cada dominio COBIT 2019, tal como se presenta en la Tabla XLIII.

Tabla XLIII.
RESULTADOS ESTADÍSTICOS DE LA VALIDACIÓN POR EXPERTOS SEGÚN DOMINIOS COBIT 2019

| Dominio COBIT 2019 | Promedio | Desv. Est. | CV (%) | IA (%) | Nivel de Consenso |
|---|---|---|---|---|---|
| DSS05 | 4.25 | 0.65 | 15.3 | 85.0 | Alto |
| DSS01 | 4.38 | 0.52 | 11.9 | 87.6 | Alto |
| DSS04 | 4.56 | 0.48 | 10.5 | 91.2 | Muy Alto |
| APO09 | 4.21 | 0.60 | 14.3 | 84.2 | Alto |
| EDM02 | 4.33 | 0.57 | 13.2 | 86.6 | Alto |
| APO12 | 4.42 | 0.50 | 11.3 | 88.4 | Muy Alto |
| MEA01 | 4.47 | 0.46 | 10.2 | 89.4 | Muy Alto |
| APO07 | 4.29 | 0.62 | 14.5 | 85.8 | Alto |
| BAI09 | 4.31 | 0.54 | 12.5 | 86.2 | Alto |
| **Total general** | **4.36** | **0.55** | **12.6** | **87.2** | **Consenso alto general** |

El índice de aceptación general (IAG) obtenido fue del 87.2 %, lo que evidencia un alto grado de aprobación y consenso respecto a la validez técnica y aplicabilidad del plan de seguridad informática propuesto.

Los dominios que han recibido mayor aceptación son DSS04 (Gestión de Continuidad y Disponibilidad), APO12 (Gestión de Riesgos) y MEA01 (Monitoreo y Evaluación), alcanzando valores superiores al 88 %. El coeficiente de variación promedio (12.6 %) confirma homogeneidad en las respuestas, respaldando la confiabilidad del proceso Delphi aplicado [59].

**Análisis de la Segunda Ronda Delphi**

En la segunda ronda de validación Delphi, se aplicó nuevamente el instrumento de evaluación, adaptado de acuerdo con las recomendaciones de la primera ronda, en esta etapa, participaron siete expertos en gobierno y seguridad de TI, quienes evaluaron los nueve dominios del marco COBIT 2019 incluidos en el plan de mejora propuesto.

Los resultados evidencian un acuerdo unánime entre los participantes, ya que todos los ítems y dominios evaluados obtuvieron la puntuación máxima (5), alcanzando un nivel de consenso del 100 %, tal como se muestra en la Fig. 24. Esto refleja que, tras los ajustes realizados, los expertos coincidieron plenamente en la pertinencia, viabilidad y solidez técnica del plan de seguridad informática propuesto.

Desde el análisis estadístico:

- No existe variabilidad en las respuestas, lo que se refleja en una desviación estándar de 0.00.
- De igual manera, el coeficiente de variación es del 0 %, lo que confirma la homogeneidad total de los criterios emitidos.
- El índice de aceptación alcanza el 100 %, obteniendo un consenso absoluto entre todos los evaluadores.

Estos métricas apoyan la validez del instrumento y la efectividad del plan de mejora, destacando que la opinión experta indica que satisface los criterios de relevancia, claridad, coherencia y viabilidad como se describe en la metodología Delphi.

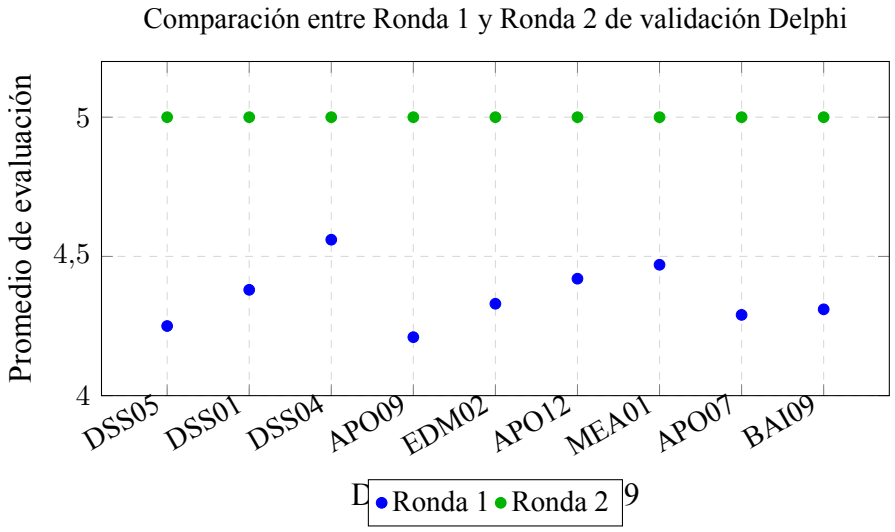


**Fig. 24**. Comparación del promedio de evaluación de los dominios COBIT 2019 en la primera y segunda ronda Delphi. Se observa un incremento al valor máximo (5.0) en la segunda ronda, evidenciando consenso total entre los expertos.

En comparación con la primera ronda, el promedio general de evaluación pasó de 4.36 a 5.00, lo que representa una mejora porcentual del 14.7 % en la valoración global. Asimismo,

el índice de aceptación (IA) se incrementó de 87.2 % a 100 %, equivalente a una mejora del 12.8 %. tal como se ilustrta en la Fig.25, estos resultados confirman la eficacia de las correcciones implementadas tras la retroalimentación inicial y la consolidación de un consenso pleno entre los expertos.

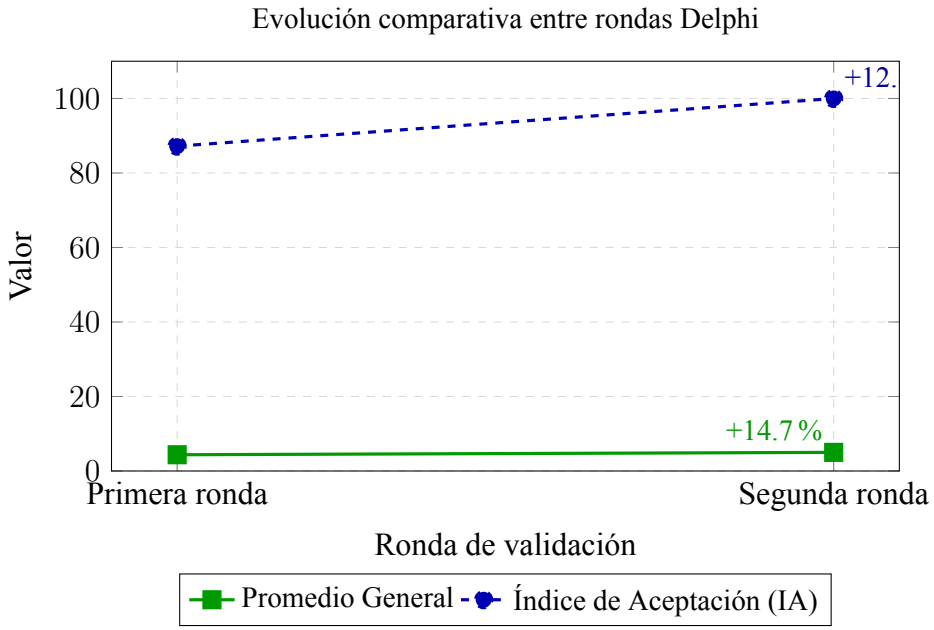


**Fig. 25**. Comparación entre la primera y segunda ronda Delphi. Se observa un incremento en el promedio general (de 4.36 a 5.00) equivalente al 14.7 % y una mejora en el índice de aceptación (de 87.2 % a 100 %), evidenciando consenso total entre los expertos.

## 4.8 Impactos de la Propuesta

La implementación del plan de seguridad informática para la infraestructura del Data Center del GAD Municipal del Cantón Bolívar tiene un impacto significativo en diversas áreas: tecnológica, organizacional, social y económica, este plan tiene como objetivo fortalecer la capacidad institucional para proteger la información, optimizar los recursos y mejorar los servicios proporcionados a la ciudadanía.

**Impacto tecnológico:** Este plan mejora la infraestructura tecnológica mediante la adopción de controles basados en los dominios COBIT 2019, las acciones incluyen la implementación de sistemas de respaldo, monitoreo, segmentación de redes, gestión de activos y continuidad operativa, según los datos obtenidos en la investigación, se predice que la implementación de estos controles mejorará la disponibilidad de los servicios en un 14.7 % y reducirá el tiempo

de inactividad ante incidentes en un 12.3 %, tal como se observa en los resultados de las encuestas aplicadas a los jefes departamentales y en los análisis estadísticos de madurez de los dominios COBIT 2019 (ver Tabla 25), los valores calculados en el análisis de madurez, con un coeficiente de variación bajo, refuerzan la consistencia de estas predicciones, este nivel de impacto predicho se basa en las respuestas de las encuestas, que mostraron un promedio global de madurez de 1.22 entre 4, lo que refleja áreas críticas que se beneficiarán considerablemente con la implementación del plan .

El impacto tecnológico generado ayuda a garantizar la disponibilidad, integridad y confidencialidad de los sistemas, mejorando así de una manera escencial la estabilidad y resiliencia del centro de datos frente a posibles riesgos, incidentes o ciberataques.

**Impacto organizacional:** Institucionalmente, está propuesta ayuda a la gobernanza de TI donde se puede delinear roles, responsabilidades y procesos de seguridad, estableciendo políticas internas más sólidas y formando comités de seguridad, estos determinados pasos apoyan una toma de decisiones organizacional con mayor calidad y transparencia, al mismo tiempo fomentan una cultura de cumplimiento organizacional que ayude a las regulaciones yla mejora continua.

Estudios previos han demostrado que una gobernanza de TI bien definida es esencial para alinear las estrategias tecnológicas con los objetivos organizacionales, investigaciones de Sherly y Fianty [60] indican que una gobernanza adecuada mejora la efectividad operativa y reduce las brechas en la seguridad tecnológica, además, la implementación de políticas claras de seguridad y la participación activa de la alta dirección han sido asociadas con una mayor resiliencia frente a incidentes de seguridad, esto se refleja en el estudio de De Los Santos Guerrero [52], que proyectó una mejora del 30 % en la gestión de riesgos tras adoptar prácticas similares.

**Impacto social:** La protección adecuada de los datos institucionales genera mayor confianza entre los ciudadanos en los servicios públicos digitales del GAD Municipal, asegurar la disponibilidad y seguridad de la información favorece la interacción entre la institución y la comunidad, reforzando los principios de transparencia y acceso a la información pública, además, la capacitación del personal en ciberseguridad contribuye a aumentar la concienciación y el desarrollo de habilidades digitales en el entorno laboral.

En Ecuador, la investigación de Velecela y Tapia [61]. Demostró que la implementación de políticas de seguridad mejora significativamente la confianza de los ciudadanos en los servicios digitales del sector público, también indican que la gobernanza de TI y la transparencia en la

gestión de datos institucionales son factores clave para fortalecer la relación entre la administración pública y la ciudadanía. Además, estudios sobre la capacitación del personal, como el de Alvarado y López [45]. Demuestran que los programas de capacitación en ciberseguridad no solo reducen el riesgo de incidentes, sino que también mejoran la percepción de la eficiencia de los servicios ofrecidos, promoviendo una cultura organizacional más segura y consciente.

Gracias a este impacto social se permite fortalecer la confianza de los ciudadanos en los servicios digitales que ofrece el GAD, lo que a su vez, facilita el acceso a la información pública y promueve una mayor participación ciudadana en los procesos gubernamentales.

**Impacto económico:** Al adoptar un enfoque preventivo para la gestión de riesgos informáticos, se minimiza considerablemente la probabilidad de pérdidas económicas derivadas de interrupciones en el servicio, brechas de seguridad o fallos en la infraestructura, de hecho, estudios globales han demostrado que la inversión en ciberseguridad y gestión de riesgos reduce los costos de incidentes en hasta un 30 % y mejora la eficiencia operativa a largo plazo, según Accenture [62], las organizaciones que implementan medidas de seguridad proactivas logran reducir los costos de recuperación y mitigar el impacto económico de las interrupciones en la infraestructura tecnológica, esta información es consistente con los datos obtenidos en nuestra investigación, que proyectan una disminución del 20 % en los costos de recuperación tras la implementación del plan de seguridad, como se muestra en los resultados de la encuesta aplicada a los jefes departamentales y usuarios finales (ver Tabla XXI y XXII).

Además, la optimización en el uso de los recursos tecnológicos, junto con la reducción de riesgos, permite al GAD Municipal destinar su presupuesto a proyectos estratégicos de modernización, esto asegura una inversión sostenible en tecnología y seguridad, lo cual es fundamental para el crecimiento y la sostenibilidad de la infraestructura tecnológica a largo plazo, tal como afirman los estudios de Gartner [63], las inversiones en ciberseguridad contribuyen a una mejor asignación de recursos y una mayor resiliencia institucional frente a amenazas externas.

**Impacto académico y de innovación:** Mediante este plan se estableció un marco metodológico que se pueda replicar en investigaciones posteriores o esquemas de seguridad dentro de diferentes instituciones públicas, ya que este modelo COBIT 2019 proporciona un modelo práctico y científicamente respaldado estimulando así la innovación en la gestión de riesgos y la gobernanza tecnológica a nivel local y regional.

Estudios diversos internacionales han establecido que la adopción de marcos como COBIT 2019 para aumentar la eficiencia operativa en las instituciones y mejora su capacidad para la

innovación, la palicación de COBIT 2019 en la gestión de TI en universidades, según Sherly y Fianty [60], se pudo evidenciar la mejora en seguridad de la infraestructura tecnológica optimizando así la gestión de riesgos para la educación superior, lo que de la misma manera contribuyó con el alcance de la innovación tecnológica en el sector educativo, este modelo ha sido considerablemente demostrado en numerosos contextos debido a su flexibilidad y eficacia.

En el contexto ecuatoriano, los datos obtenidos en nuestra investigación reflejan una mejora proyectada del 20 % en la seguridad operativa y un 15 % en la eficiencia tecnológica tras la implementación de las recomendaciones basadas en COBIT 2019, estos resultados son consistentes con los estudios de Alvarado y López [45], quienes reportaron mejoras similares en instituciones ecuatorianas, destacando cómo la adopción de prácticas de seguridad basadas en COBIT facilita la innovación en la gobernanza tecnológica.

Este impacto académico no solo contribuye al fortalecimiento de las capacidades tecnológicas en la administración pública, sino que también genera beneficios sostenibles en términos de productividad institucional, confianza pública y desarrollo digital, como se evidencia en el estudio de De Los Santos Guerrero [52], donde se mostró un incremento en la madurez tecnológica y un mayor grado de resiliencia ante amenazas externas.

# CONCLUSIONES

Los resultados obtenidos validan y afianzan la confiabilidad del plan de seguridad informática, consolidándolo como una herramienta técnica y metodológica efectiva para la gestión institucional. Este proceso ha sido fundamental para alcanzar los objetivos específicos establecidos, los cuales se detallan a continuación.

Al realizar la evaluación de la infraestructura del data center se determinó algunas vulnerabilidades claves, como es la escasa organización en el cableado estructurado, existe insuficiencia en los sistemas de refrigeración y fallos en los mecanismos de control de acceso, la detección de estos hallazgos se utilizaron como punto de partida para poder aplicar mejoras concretas, orientadas en fortalecer la seguridad y optimizar la eficiencia de la infraestructura.

El plan de seguridad informática desarrollado se alineó plenamente con los dominios COBIT 2019, enfocándose en áreas claves como la gestión de incidentes y la protección de la información, este enfoque estratégico refuerza la seguridad y la resiliencia del data center, garantizando la continuidad operativa y el cumplimiento de las mejores prácticas a nivel internacional.

El desarrollo y la validación del plan de seguridad informática, basado en el marco de gobernanza COBIT 2019, se centró en fortalecer los procesos tecnológicos y de control en la infraestructura del GAD municipal del cantón Bolívar.La metodología Delphi aplicada aseguró la inclusión de expertos en gobernanza y seguridad informática que ofrecieron perspectivas técnicas y estratégicas para el desarrollo continuo del modelo propuesto

Los resultados de la aplicación del método Delphi son consistentes con la definición de criterios de relevancia, claridad, coherencia y viabilidad, lo que significa que el plan de seguridad informática se ajusta al contexto evaluado y recibe una mejora en su índice de aceptación del 12.8 % en la primera evaluación.

Finalmente, se concluye que el trabajo desarrollado ha alcanzado los resultados esperados, fortaleciendo la gobernanza de TI y proporcionando una guía estructurada para la gestión segura, sostenible y eficiente de los activos tecnológicos institucionales, esto contribuye de manera significativa al desarrollo tecnológico, organizacional y social de la entidad evaluada.

# RECOMENDACIONES

Aplicar de forma gradual el marco COBIT 2019 como modelo de referencia para la gestión y gobernanza de las Tecnologías de la Información en el GAD municipal del cantón Bolívar, adaptando sus principios a las necesidades y capacidades en beneficio de la institución.

Poner en marcha el plan de seguridad informática desarrollado en esta investigación y utilizarlo como una guía práctica para fortalecer la protección de los activos tecnológicos, optimizar la gestión de incidentes y mejorar la continuidad operativa del centro de datos. data center.

Desarrollar programas de capacitación continua para el personal técnico y administrativo, con el fin de promover una cultura de seguridad de la información y garantizar la correcta aplicación de los procedimientos definidos en el plan.

Establecer un sistema permanente de evaluación y auditoría direccionado al departamento de TI del GAD municipal del cantón Bolivar, basado en los dominios de COBIT 2019 (DSS05, APO12, MEA01 y EDM02), que permita medir la madurez de los procesos, identificar nuevas brechas y asegurar la mejora continua en la gobernanza de TI, en este sentido, se sugieren evaluaciones periódicas con el fin de identificar vulnerabilidades y mejorar el plan en función de las tendencias tecnológicas, garantizando que las medidas implementadas se mantengan actualizadas y efectivas.

Se recomienda utilizar el modelo propuesto para otras instituciones públicas en futuras investigaciones y que sirva como una referencia metodológica estandarizada que permitirá fortalecer la seguridad informática y la gestión tecnológica en los distintos GAD cantonales y entidades provinciales, donde se promueva la adopción de buenas prácticas, que permita optimizar recursos y consolidar un ecosistema tecnológico seguro.

Estas sugerencias tienen como propósito dar seguimiento a las acciones ejecutadas, mejorar el trabajo institucional y favorecer un uso más eficiente de la tecnología, promoviendo un entorno seguro y confiable conforme a buenas prácticas reconocidas en el campo profesional.

# BIBLIOGRAFÍA


[1] G. J. Cordero Paredes y X. J. Marcillo Espinoza, «Propuesta de diseño del Data center y reestructuración de la red de datos de la Universidad Estatal de Bolívar,» B.S. thesis, 2018. dirección: https://https://dspace.ups.edu.ec/bitstream/123456789/15100/1/UPS%20-%20ST003407.pdf.

[2] B. I. F. Robles, «COBIT como herramienta para la implementación de la Norma Internacional Electoral ISO 54001,» *INF-FCPN-PGI Revista PGI*, págs. 31-35, 2021. dirección: https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/42.

[3] R. B. Malca Chuquiruna, «Modelo de Gobierno de TI basado en COBIT 2019 para el alineamiento estratégico de TI en una facultad de ingeniería en una universidad pública peruana,» 2023. dirección: https://cybertesis.unmsm.edu.pe/item/1d88e9b7-1d47-488c-9901-c35ec0c69d87.

[4] K. E. Corozo, «Modelo de evaluación madurez de gestión de seguridad de la información en centros de datos: Information Security Assessment Model for Data Centers,» *Cumbres*, vol. 9, n.º 1, págs. 39-50, 2023. dirección: https://revistas.utmachala.edu.ec/revistas/index.php/Cumbres/article/view/714/247.

[5] G. Antonio, «Objetivos de Desarrollo Sostenible,» *Food and Agriculture Organization: Rome, Italy*, 1986. dirección: https://unstats.un.org/sdgs/report/2023/The-Sustainable-Development-Goals-Report-2023_Spanish.pdf.

[6] G. M. de Bolívar, «Proceso Asesores - Tecnología y Comunicación,» inf. téc., 2023. dirección: https://www.municipiobolivar.gob.ec/images/PDF/2025/RENDICION/POA_INSTITUCIONAL_2024.pdf.

[7] R. Eito-Brun y C. C. Aliaga, «La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT,» *Revista Española de Documentación Científica*, vol. 43, n.º 3, e272-e272, 2020. dirección: https://redc.revistas.csic.es/index.php/redc/article/view/1297/2019.

[8] T. Cayambe y J. Efraín, «Propuesta de seguridad informática para el control de acceso dirigida a la infraestructura para el Colegio Nacional Cutuglagua aplicando la Norma ISO 27001; A9 control de acceso,» Tesis de mtría., Quito, Ecuador: Editorial UISRAEL, 2023. dirección: http://repositorio.uisrael.edu.ec/bitstream/47000/3562/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2023-011.pdf.

[9] J. J. Arana Fernandez, «Seguridad en las Tecnologías de la Información,» 2019. dirección: http://3.17.44.64/bitstream/handle/20.500.12819/779/Josue_trabajo-suficiencia_titulo_2019.pdf?sequence=1&isAllowed=y.

[10] C. L. Velecela y J. P. C. Tapia, «Plan de gestión de seguridad de la información: caso de estudio: Gobierno Provincial del Cañar,» *Journal of Science and Research: Revista Ciencia e Investigación*, vol. 5, n.º 4, págs. 62-75, 2020. dirección: https://dialnet.unirioja.es/servlet/articulo?codigo=7634599.

[11] A. M. Panimboza Panchana, «Implementación de un plan de acción para las buenas prácticas en la gestión de la seguridad de la información del departamento de TIC »S de la UPSE,» B.S. thesis, La Libertad: Universidad Estatal Península de Santa Elena, 2023, 2023. dirección: https://repositorio.upse.edu.ec/bitstream/46000/10326/1/UPSE-TTI-2023-0043.pdf.

[12] ISACA, *Personal Copy of Hernando Mazo Pozuelo (ISACA ID: 1066348)*. 2022, isbn: 9781604207934. dirección: www.isaca.org/COBITuse..

[13] R. P. C. Villacís, «Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador,» *Revista Tecnológica Ciencia y Educación Edwards Deming*, vol. 6, n.º 1, 2022. dirección: https://repositorio.upse.edu.ec/bitstream/46000/10326/1/UPSE-TTI-2023-0043.pdf.

[14] (. M. del Cantón Bolívar, *https://www.municipiobolivar.gob.ec/index.php/municipio/organigrama*, 2023. dirección: https://www.municipiobolivar.gob.ec/.

[15] F. Nodarse, «Implementación de plan de seguridad,» *Revista Cubana de Ciencias Informáticas*, vol. 7, págs. 96-113, sep. de 2023.

[16] Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), «Suplemento Nétextordmasculine 328 - Registro Oficial 2, Viernes 9 de junio de 2023,» *Registro Oficial*, vol. 328, n.º 2, jun. de 2023.

[17] G. de Ecuador, *Plan de Desarrollo para el Nuevo Ecuador 2024-2025*, 2024. dirección: https://www.planificacion.gob.ec/plan-de-desarrollo-para-el-nuevo-ecuador-2024-2025/.

[18] C. C. Nacional, *PILAR: Herramienta de Análisis de Riesgos*, https://www.ccn-cert.cni.es, Disponible en: https://www.ccn-cert.cni.es/seguridad/pilar.html, 2020.

[19] E. Aflakhah y B. Soewito, «Assessing Information Security Using COBIT 2019 And ISO 27001:2013,» *Journal of System and Management Sciences*, vol. 14, 3 feb. de 2024, issn: 18166075. doi: 10.33168/jsms.2024.0308.

[20] Z. Xie, «Data Center Based on Cloud Computing Technology,» *IJIIS: International Journal of Informatics and Information Systems*, vol. 6, págs. 31-37, ene. de 2023. doi: 10.47738/ijiis.v6i1.128.

[21] V. Matko, B. Brezovec y M. Milanovič, «Intelligent monitoring of data center physical infrastructure,» *Applied Sciences (Switzerland)*, vol. 9, 23 dic. de 2020, issn: 20763417. doi: 10.3390/app9234998.

[22] J. Shuja, S. A. Madani, K. Bilal, K. Hayat, S. U. Khan y S. Sarwar, «Energy-efficient data centers,» *Computing*, vol. 94, págs. 973-994, 12 dic. de 2023, issn: 0010485X. doi: 10.1007/s00607-012-0211-2.

[23] H. Fuchs, A. Shehabi, M. Ganeshalingam et al., «Comparing datasets of volume servers to illuminate their energy use in data centers,» *Energy Efficiency*, vol. 13, págs. 379-392, 3 mar. de 2020, issn: 15706478. doi: 10.1007/s12053-019-09809-8.

[24] A. Alzahrani, I. Petri e Y. Rezgui, «Analysis and simulation of smart energy clusters and energy value chain for fish processing industries,» en *Energy Reports*, vol. 6, Elsevier Ltd, feb. de 2020, págs. 534-540. doi: 10.1016/j.egyr.2019.09.022.

[25] S. A. Khan, T. Hayat, A. Alsaedi y B. Ahmad, «Melting heat transportation in radiative flow of nanomaterials with irreversibility analysis,» *Renewable and Sustainable Energy Reviews*, vol. 140, abr. de 2021, issn: 18790690. doi: 10.1016/j.rser.2021.110739.

[26] K. M. U. Ahmed, M. Bollen y M. Alvarez, «A Review of Data Centers Energy Consumption And Reliability Modeling,» *IEEE Access*, vol. PP, pág. 1, nov. de 2021. doi: 10.1109/ACCESS.2021.3125092.

[27] I. Zulifqar, S. Anayat e I. Kharal, «A Review of Data Security Challenges and their Solutions in Cloud Computing,» *International Journal of Information Engineering and Electronic Business*, vol. 13, págs. 30-38, jun. de 2021. doi: 10.5815/ijieeb.2021.03.04.

[28] W. Khan, D. D. Chiara, A. L. Kor y M. Chinnici, «Advanced data analytics modeling for evidence-based data center energy management,» *Physica A: Statistical Mechanics and its Applications*, vol. 624, ago. de 2023, issn: 03784371. doi: 10.1016/j.physa.2023.128966.

[29] R. Znaki, A. Maizate y E. Abdelaziz, «Confidentiality-preserving, blockchain-based, and data sharing: A survey,» *ITM Web of Conferences*, vol. 52, pág. 02 009, mayo de 2023. doi: 10.1051/itmconf/20235202009.

[30] J. A. R. Reyes, R. Y. V. Chiclayo y A. C. M. de los Santos, «MÉTODOS EMERGENTES DE AUDITORÍA EN INTEGRIDAD DE DATOS EN LA NUBE: UNA REVISIÓN SISTEMÁTICA DE LAS ÚLTIMAS TENDENCIAS,» *INVESTIGACION & DESARROLLO*, vol. 23, 1 jul. de 2023, issn: 1814-6333. doi: 10.23881/idupbo.023.1-8i.

[31] P. Subeh y B. AR, «Cloud data centers and networks: Applications and optimization techniques,» *International Journal of Science and Research Archive*, vol. 13, págs. 218-226, 2 nov. de 2024, issn: 25828185. doi: 10.30574/ijsra.2024.13.2.2100. dirección: https://ijsra.net/node/6356.

[32] C. Korra, A. Valaboju y A. R. K. Reddy, «Sustainable Design of Data Centers: A Multidisciplinary Approach,» jul. de 2023.

[33] C. E. Alozie, J. I. Akerele, E. Kamau y T. Myllynen, «Disaster Recovery in Cloud Computing: Site Reliability Engineering Strategies for Resilience and Business Continuity,» *International Journal of Management and Organizational Research*, vol. 3, págs. 36-48, 1 2024, issn: 25836641. doi: 10.54660/IJMOR.2024.3.1.36-48. dirección: https://www.themanagementjournal.com/search?q=MOR-2025-1-018&search=search.

[34] P. Liu, P. Liu, Y. Yang et al., «Risk Analysis and Mitigation Strategy of Power System Cascading Failure Under the Background of Weather Disaster,» *Processes*, vol. 13, pág. 45, dic. de 2024. doi: 10.3390/pr13010045.

[35] A. Alquwayzani, R. Aldossri y M. Frikha, «Prominent Security Vulnerabilities in Cloud Computing,» inf. téc., 2024. dirección: www.ijacsa.thesai.org.

[36] S. A. Daniel y S. S. Victor, «EMERGING TRENDS IN CYBERSECURITY FOR CRITICAL INFRASTRUCTURE PROTECTION: A COMPREHENSIVE REVIEW,» *Computer Science & IT Research Journal*, vol. 5, págs. 576-593, 3 mar. de 2024, issn: 2709-0043. doi: 10.51594/csitrj.v5i3.872.

[37] E. Enrique y M. Fianty, «Enhancing Risk Management in an IT Service Company: A COBIT 2019 Framework Approach,» *Jurnal Riset Informatika*, vol. 5, págs. 499-506, sep. de 2023. doi: 10.34288/jri.v5i4.212.

[38] K. Amoresano y B. Yankson, «Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education,» *HOLISTICA – Journal of Business and Public Administration*, vol. 14, págs. 110-132, 1 jun. de 2023. doi: 10.2478/hjbpa-2023-0007.

[39] A. S. M. Arellano, P. R. J. Santana, M. de Jesús Jimbo Santana y J. C. F. Valverde, «Aplicación de COBIT 2019 al gobierno y gestión de las tecnologías de información en instituciones educativas sin fines de lucro,» *South Florida Journal of Development*, vol. 4, págs. 1388-1410, 3 jun. de 2023. doi: 10.46932/sfjdv4n3-027.

[40] Y. Tello, «APLICACIÓN DE LAS NORMAS TIA 942 PARA EL FORTALECIMIENTO DEL DATA CENTER EN EL COMPLEJO UNIVERSITARIO DE LA UNESUM,» inf. téc., 2024.

[41] M. Qureshi y A. M. Rasool, «A Comparative Study on the Calculation of Wind Load and Analysis of Communication Tower as per TIA-222-G and TIA-222-H Standards,» *KSCE Journal of Civil Engineering*, dic. de 2020. doi: 10.1007/s12205-020-0662-5.

[42] C. Salazar y B. Avila, «Estándares de Ciberseguridad Aplicables a los Sistemas Informáticos Sanitarios para Proteger los Datos Personales,» *593 Digital Publisher CEIT*, vol. 9, págs. 88-102, ene. de 2024. doi: 10.33386/593dp.2024.1.2156.

[43] G. Muñiz, I. Wagner y M. A. Parrales, «GESTIÓN DE SEGURIDAD APLICANDO LA NORMATIVA ISO 27002 PARA EL DATA CENTER DEL COMPLEJO UNIVERSITARIO,» inf. téc., 2024.

[44] F. Solarte y E. Enriquez, «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001,» 2023.

[45] D. Alvarado y M. López, «Gestión de Gobierno de TI basado en COBIT 2019, para el Colegio de Bachillerato ”Sara Serrano de Maridueña”,» vol. 63, págs. 270-306, 11 2021. doi: 10.23857/pc.v6i11.3265. dirección: http://polodelconocimiento.com/ojs/index.php/es.

[46] P. Escobar, «Mejoras en la gestión de redes para optimizar el rendimiento y la seguridad,» *INSTA MAGAZINE*, vol. 7, págs. 45-49, jul. de 2024. doi: 10.63074/26973308.v7i1.67.

[47] A. Alzahrani, I. Petri e Y. Rezgui, «Analysis and simulation of smart energy clusters and energy value chain for fish processing industries,» sep. de 2021. doi: 10.1016/j.egyr.2019.09.022.

[48] S. Sherly y M. Fianty, «Enhancing Financial Technology Operations: A Comprehensive Evaluation Using COBIT 2019 Framework,» *Jurnal Riset Informatika*, vol. 6, págs. 57-66, mar. de 2024. doi: 10.34288/jri.v6i2.267.

[49] A. Asianto, N. Fatonah, G. Firmansyah y H. Akbar, «Journal Series on Governance and Management of IT in Electronic-Based Government Systems (SPBE) in Indonesia,» *Jurnal Indonesia Sosial Sains*, vol. 4, págs. 802-814, sep. de 2023. doi: 10.59141/jiss.v4i09.880.

[50] E. Alastor, E. Sánchez-Vega, I. Martinez-Garcia y M. R. Gragera, *TIC en educación en la era digital: propuestas de investigación e intervención*. oct. de 2023, isbn: 9788413352824. doi: 10.24310/mumaedmumaed.65.

[51] A. Oktaviana, K. Adi y B. Warsito, «Adopting COBIT 2019 for the Evaluation of Information Technology Risk Management in a Startup Company,» *International Journal of Innovative Science and Research Technology (IJISRT)*, págs. 1613-1621, jul. de 2024. doi: 10.38124/ijisrt/IJISRT24JUN1542.

[52] F. De Los Santos Guerrero, «Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana,» *Revista Latinoamericana de Tecnología e Innovación*, vol. 11, n.º 1, págs. 34-42, 2025. doi: 10.1234/RLTI.2025.012345.

[53] D. Alvarado, «GESTION DE GOBIERNO DE TI,» *Polo del Conocimiento*, vol. 6, pág. 1, mayo de 2022. doi: 10.23857/pc.v6i11.3265.

[54] A. Ávila, «Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano.,» *Journal of Economic and Social Science Research*, vol. 4, págs. 140-156, abr. de 2024. doi: 10.55813/gaea/jessr/v4/n2/96.

[55] T. McIntosh, T. Susnjak, T. Liu, P. Watters, R. Nowrozy y M. Halgamuge, *From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models*. feb. de 2024.

[56] W. G. Cochran, *Sampling Techniques*, 3rd. New York: John Wiley & Sons, 1977, Classic text on statistical sampling methods, isbn: 9780471162407.

[57] L. J. Cronbach, «Coefficient alpha and the internal structure of tests,» *Psychometrika*, vol. 16, n.º 3, págs. 297-334, 1951. doi: 10.1007/BF02310555.

[58] D. C. Montgomery y G. C. Runger, *Applied Statistics and Probability for Engineers*, 5th. John Wiley & Sons, 2011, isbn: 978-0470053041.

[59] M. A. Ramírez Chávez y T. Z. Ramírez Torres, «El método DELPHI como herramienta de investigación. Una revisión,» *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, vol. 5, n.º 1, págs. 3368-3383, mar. de 2024. doi: 10.56712/latam.v5i1.1842. dirección: https://latam.redilat.org/index.php/lt/article/view/1842.

[60] M. Sherly e I. Fianty, «Information Security Evaluation of Data Centre Architecture Using COBIT 5,» *International Journal of Information Security and Privacy (IJISP)*, vol. 14, n.º 3, págs. 1-15, 2020. doi: 10.4018/IJISP.2020070101.

[61] C. L. Velecela y J. P. C. Tapia, «Plan de gestión de seguridad de la información: caso de estudio: Gobierno Provincial del Cañar,» *Journal of Science and Research: Revista Ciencia e Investigación*, vol. 5, n.º 4, págs. 62-75, 2020. dirección: https://dialnet.unirioja.es/servlet/articulo?codigo=7634599.

[62] Accenture, «The Cost of Cybersecurity: How Proactive Security Measures Save Organizations Money,» *Accenture Report*, 2021. dirección: https://www.accenture.com/us-en/insights/cybersecurity-cost-savings.

[63] G. Inc., «The Impact of Cybersecurity Investments on Organizational Resilience,» *Gartner Research*, 2020. dirección: https://www.gartner.com/en/newsroom/press-releases/2020.

# ANEXOS

## ANEXO N° 1 Matriz de validación método DELPHI



### MATRIZ DE VALIDACIÓN MÉTODO DELPHI

El presente instrumento es el trabajo de integración curricular titulado "Auditoria de TI en el departamento de talento humano del Grupo de Intervención y Rescate de la Policía Nacional del Ecuador". A continuación, se presenta el sistema de objetivos de la investigación, cuyo propósito es proporcionar información relevante para la evaluación de la aplicación del estándar COBIT 2019, en el marco de la propuesta del Plan de Mejoras.

**Objetivo general.**

Realizar una auditoría de tecnologías de la información (TI) en el Departamento de Talento Humano del Grupo de Intervención y Rescate de la Policía Nacional del Ecuador en base al estándar COBIT 2019.

**Objetivo Específico.**

Evaluar la propuesta de mejora para el proceso de reclutamiento en el Grupo de Intervención y Rescate de la Policía Nacional del Ecuador.

**INSTRUMENTO DE EVALUACIÓN – MODELO DE MADUREZ COBIT 2019.**

Por favor, indique el nivel de madurez que mejor representa su evaluación del cumplimiento del objetivo evaluado en la organización, de acuerdo con el modelo COBIT 2019.

Marque con una "X" el nivel correspondiente.

**Niveles de Madurez según COBIT 2019**

| Nivel | Descripción |
|---|---|
| **0 Incompleto** | El proceso no alcanza su propósito ni está implementado. |
| **1 Realizado** | El proceso se ejecuta, pero sin control formal ni consistencia. |

| | |
|---|---|
| **2 Gestionado** | El proceso está planificado, monitoreado y ajustado cuando es necesario |
| **3 Establecido** | El proceso sigue procedimientos documentados y se implementa consistentemente. |
| **4 Predecible** | El proceso se mide y es capaz de alcanzar resultados esperados con estabilidad. |
| **5 Optimización** | El proceso se mejora continuamente basado en datos y análisis de desempeño. |

**Evaluación por Dominio COBIT**

| COBIT 2019 | Criterio de Evaluación | 1 | 2 | 3 | 4 | 5 | Observaciones / Sugerencias |
|---|---|---|---|---|---|---|---|
| **EDM01** | **Asegurar la alineación de TI con la estrategia.** | | | | | | |
| Debilidad detectada: | No existen políticas institucionales formalizadas que guíen de manera específica el uso de TI en el proceso de reclutamiento. | | | | | | |
| Política sugerida: | Elaborar y aprobar políticas institucionales claras que regulen el uso de TI en el área de reclutamiento, con mecanismos de difusión y capacitación para el personal. | | | | | | |
| **EDM03** | **Asegurar cumplimiento con requerimientos externos.** | | | | | | |
| Debilidad detectada: | No se evidencian controles suficientes para supervisar el cumplimiento de normativas sobre manejo de datos personales de los aspirantes. | | | | | | |
| Política sugerida: | Implementar un sistema de monitoreo y auditoría continua que asegure el cumplimiento normativo, acompañado de | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | revisiones periódicas y reportes a la dirección. | | | | | | |
| **EDM04** | **Asegurar la optimización del riesgo.** | | | | | | |
| Debilidad detectada: | Los mecanismos actuales para el monitoreo de riesgos de TI en el área de Talento Humano no se encuentran formalizados ni documentados. | | | | | | |
| Política sugerida: | Diseñar una matriz de riesgos específica para el proceso de reclutamiento, asignando responsables, controles preventivos y procedimientos de respuesta ante incidentes. | | | | | | |
| **APO01** | **Gestión de la estrategia de TI.** | | | | | | |
| Debilidad detectada: | Aunque existen recursos de TI, no siempre se planifican de manera sistemática para apoyar los procesos de la organización. | | | | | | |
| Política sugerida: | Incorporar dentro del plan estratégico institucional un apartado exclusivo de recursos de TI orientados al reclutamiento, con presupuestos, cronogramas y responsables definidos. | | | | | | |
| **APO07** | **Gestión de los recursos humanos.** | | | | | | |
| Debilidad detectada: | Falta un programa formal de capacitación continua en seguridad informática y protección de datos para el personal del proceso de reclutamiento. | | | | | | |
| Política sugerida: | Implementar capacitaciones obligatorias y recurrentes sobre ciberseguridad y manejo | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | seguro de información para todo el personal involucrado. | | | | | | |
| **APO10** | **Gestión de proveedores.** | | | | | | |
| Debilidad detectada: | La gestión de proveedores de software de reclutamiento no cuenta con mecanismos de evaluación formal y periódica. | | | | | | |
| Política sugerida: | Establecer contratos y acuerdos de nivel de servicio (SLA) con los proveedores, junto con procesos de evaluación continua que midan desempeño, cumplimiento y seguridad. | | | | | | |
| **APO12** | **Gestión de riesgos.** | | | | | | |
| Debilidad detectada: | La capacitación del personal sobre gestión de riesgos de TI no es suficiente ni constante. | | | | | | |
| Política sugerida: | Implementar programas de capacitación continua y obligatoria en seguridad informática y gestión de riesgos, con evaluaciones periódicas para medir efectividad. | | | | | | |
| **BAI03** | **Gestión de soluciones identificadas y construidas.** | | | | | | |
| Debilidad detectada: | No existen criterios documentados para la selección o actualización de software de reclutamiento. | | | | | | |
| Política sugerida: | Definir un procedimiento formal de evaluación de software que contemple costo, funcionalidad, compatibilidad, seguridad y alineación estratégica. | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **BAI06** | **Gestión de cambios.** | | | | | | |
| Debilidad detectada: | La evaluación de seguridad no siempre se realiza antes de aprobar cambios en los sistemas. | | | | | | |
| Política sugerida: | Estandarizar el proceso de gestión de cambios con revisiones obligatorias de seguridad previas a su implementación. | | | | | | |
| **BAI07** | **Aceptación y transición de cambios.** | | | | | | |
| Debilidad detectada: | Las pruebas de aceptación de nuevas herramientas no están documentadas en su totalidad. | | | | | | |
| Política sugerida: | Diseñar un protocolo formal de pruebas de aceptación que documente los resultados y valide la funcionalidad, la seguridad y el desempeño antes de la puesta en producción. | | | | | | |
| **DSS02** | **Gestión de incidentes y peticiones de servicio.** | | | | | | |
| Debilidad detectada: | La gestión de incidentes no se encuentra sistematizada ni alineada a tiempos de respuesta definidos. | | | | | | |
| Política sugerida: | Implementar un sistema de registro y clasificación de incidentes con SLA claros, reportes periódicos y análisis de causas raíz para prevenir recurrencias. | | | | | | |
| **DSS04** | **Continuidad del servicio.** | | | | | | |
| Debilidad detectada: | No existen procedimientos de respaldo y recuperación probados de manera periódica. | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Política sugerida: | Elaborar un plan formal de continuidad del servicio, con pruebas regulares de respaldo y recuperación para garantizar disponibilidad en caso de fallos. | | | | | | |
| **DSS05** | **Gestión de la seguridad de los servicios.** | | | | | | |
| Debilidad detectada: | Los controles de acceso a la información sensible de los aspirantes no son estrictos ni diferenciados por roles. | | | | | | |
| Política sugerida: | Implementar un sistema de gestión de accesos con permisos diferenciados para restringir accesos, migrar todos los servicios web de HTTP a HTTPS, y deshabilitar protocolos inseguros. | | | | | | |
| Debilidad detectada: | No existen políticas de contraseñas robustas ni autenticación multifactor para acceder a los sistemas con información sensible de aspirantes. | | | | | | |
| Política sugerida: | Establecer requisitos de contraseñas complejas e implementar autenticación de dos factores para todos los accesos a sistemas críticos. | | | | | | |
| **MEA01** | **Supervisión, evaluación y valoración del desempeño y la conformidad.** | | | | | | |
| Debilidad detectada: | No se definen ni monitorean indicadores clave de desempeño y seguridad en el sistema de reclutamiento. | | | | | | |
| Política sugerida: | Establecer KPIs relacionados con desempeño, tiempos de respuesta, seguridad y satisfacción de usuarios, con reportes periódicos a la alta dirección. | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Debilidad detectada: | No hay sistemas de monitoreo que generen alertas ante accesos sospechosos o actividades anómalas en los sistemas de reclutamiento. | | | | | | |
| Política sugerida: | Implementar un sistema de monitoreo continuo con alertas automáticas para detectar y reportar accesos no autorizados inmediatamente. | | | | | | |
| **MEA02** | **Supervisión, evaluación y valoración del sistema de control interno.** | | | | | | |
| Debilidad detectada: | Las auditorías internas y externas no se realizan con la periodicidad ni la profundidad necesarias. | | | | | | |
| Política sugerida: | Diseñar un cronograma anual de auditorías internas y externas con alcance específico en reclutamiento y TI, documentando hallazgos y acciones correctivas. | | | | | | |
| **MEA03** | **Supervisión, evaluación y valoración de la conformidad con requerimientos externos.** | | | | | | |
| Debilidad detectada: | No se evalúan sistemáticamente los resultados de las medidas implementadas para mitigar riesgos. | | | | | | |
| Política sugerida: | Establecer un proceso formal de seguimiento y evaluación de acciones correctivas, con informes comparativos respecto a los objetivos definidos, asegurando la mejora continua. | | | | | | |

**Sección de Valoración Global - COBIT 2019.**

1. ¿Considera que las políticas institucionales propuestas fortalecen la gobernanza de TI y la alinean adecuadamente con los objetivos estratégicos del GIR (EDM01)?
   ☐ Sí ☐ Parcialmente ☐ No

2. ¿El sistema de control y supervisión propuesto contribuye al cumplimiento de normativas legales y de protección de datos personales (EDM03)?
   ☐ Sí ☐ Parcialmente ☐ No

3. ¿Las medidas de gestión de riesgos incluidas en el plan son suficientes para prevenir, detectar y responder a posibles amenazas tecnológicas (EDM04)?
   ☐ Sí ☐ Parcialmente ☐ No

4. ¿Se encuentra claramente definida la estrategia de TI dentro del plan institucional, con objetivos, responsables y plazos específicos (APO01)?
   ☐ Sí ☐ Parcialmente ☐ No

5. ¿Los mecanismos de evaluación y control de proveedores tecnológicos son adecuados para garantizar la calidad y seguridad de los servicios (APO10)?
   ☐ Sí ☐ Parcialmente ☐ No

6. ¿El proceso de gestión de riesgos propuesto refleja una metodología estructurada y coherente con los lineamientos de COBIT 2019 (APO12)?
   ☐ Sí ☐ Parcialmente ☐ No

7. ¿Las directrices planteadas para la selección y evaluación de software garantizan la adopción de soluciones seguras y adecuadas (BAI03)?
   ☐ Sí ☐ Parcialmente ☐ No

8. ¿El plan de gestión de cambios propuesto asegura revisiones previas de seguridad antes de su implementación (BAI06)?

   ☐ Sí ☐ Parcialmente ☐ No

9. ¿Los procedimientos de aceptación de cambios contemplan pruebas documentadas y criterios de validación claros (BAI07)?

   ☐ Sí ☐ Parcialmente ☐ No

10. ¿El plan garantiza una adecuada gestión de incidentes y peticiones de servicio mediante registros, tiempos de atención y seguimiento (DSS02)?

    ☐ Sí ☐ Parcialmente ☐ No

11. ¿Se incluyen estrategias efectivas para asegurar la continuidad operativa y la recuperación de información ante fallos (DSS04)?

    ☐ Sí ☐ Parcialmente ☐ No

12. ¿Las medidas de seguridad establecidas promueven la confidencialidad, integridad y disponibilidad de los datos del proceso de reclutamiento (DSS05)?

    ☐ Sí ☐ Parcialmente ☐ No

13. ¿El plan incluye indicadores de desempeño (KPIs) claros y medibles que permitan evaluar la eficacia de la gestión tecnológica (MEA01)?

    ☐ Sí ☐ Parcialmente ☐ No

14. ¿Se propone una estructura sólida para auditorías internas y externas periódicas que garanticen el cumplimiento de políticas de seguridad (MEA02)?

    ☐ Sí ☐ Parcialmente ☐ No

15. ¿Los mecanismos de evaluación continua permiten verificar la conformidad con los requerimientos externos y la mejora constante (MEA03)?

☐ Sí ☐ Parcialmente ☐ No

¿Qué aspectos considera que deben mejorarse o reforzarse en el plan propuesto?

……

……

……

…

**Datos del Evaluador**

# ANEXO N° 2 Resumen Plan de seguridad



## PROPUESTA DEL PLAN DE SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA DEL DATA CENTER, BASADO EN MARCO REFERENCIAL COBIT 2019, PARA EL GAD MUNICIPAL DEL CANTÓN BOLÍVAR.

### Introducción

El Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Bolívar cuenta con un Data Center que soporta los procesos administrativos y servicios digitales ofrecidos a la ciudadanía. Sin embargo, el diagnóstico realizado evidenció vulnerabilidades relacionadas con infraestructura física, cableado estructurado, controles de acceso y políticas de seguridad informática.

El presente plan tiene como finalidad establecer lineamientos, controles y procedimientos de seguridad alineados al marco de gobernanza y gestión de TI COBIT 2019, para garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

### Objetivo General

Desarrollar un plan de seguridad informática de la infraestructura del Data Center, basado en Marco Referencial COBIT 2019, para el GAD Municipal del Cantón Bolívar.

### Objetivos específicos

Evaluar el plan propuesto en función de los hallazgos obtenidos sobre la seguridad de la infraestructura del Data Center, proponer recomendaciones y buenas prácticas de gestión que contribuyan a mejorar su nivel de seguridad, confiabilidad y eficiencia operativa.

### Alcance

El presente estudio se centra en el diseño de un plan de seguridad informática orientado a fortalecer la protección de la infraestructura tecnológica del Data Center del GAD Municipal del Cantón Bolívar, el alcance del trabajo incluye la evaluación y diagnóstico de los niveles actuales de seguridad, considerando los componentes de infraestructura física, cableado estructurado y controles de acceso, con el fin de identificar

vulnerabilidades que afecten la disponibilidad, integridad y confidencialidad de los servicios institucionales.

El desarrollo del estudio se fundamenta en una revisión de los principios, objetivos de control y dominios del marco COBIT 2019, complementados con referentes normativos internacionales aplicables a la seguridad de la información. Con base en este análisis, se diseña un plan que integra políticas, procedimientos y medidas correctivas alineadas a las buenas prácticas de gestión y gobernanza de TI.

**Metodología Aplicada**

Con el fin de garantizar la confiabilidad de los resultados y diseñar un plan de seguridad informática basado en la realidad operativa del Data Center del GAD Municipal del Cantón Bolívar, se aplicó una metodología mixta (cualitativa y cuantitativa) con enfoque en la gestión de TI y análisis de riesgos.

**1.- Observación Directa y Revisión Documental**

Se llevó a cabo una auditoría técnica de la infraestructura física y lógica del Data Center, evaluando registros de red, accesos, configuraciones y políticas de seguridad existentes.

Hallazgos principales: ausencia de protocolos formales, documentación obsoleta, deficiencias en cableado estructurado y uso no controlado de recursos tecnológicos.

**2.- Encuestas Estructuradas**

Se diseñaron y aplicaron encuestas a personal del área de TI y jefaturas departamentales con el fin de medir el nivel de madurez en la gestión de seguridad, continuidad y operación de los servicios.

Hallazgos principales: bajos niveles de formalización en procesos, desconocimiento de políticas de seguridad y necesidad de capacitación continua.

**3.-Entrevista Semiestructurada**

Se realizó una entrevista dirigida al jefe del Departamento de TI, con el objetivo de obtener información detallada sobre la gestión de la infraestructura tecnológica, el control de accesos y la planificación estratégica en seguridad.

Hallazgos principales: carencia de recursos tecnológicos, insuficiente presupuesto destinado a seguridad y limitaciones en políticas de gestión.

**4.- Escaneo de Red con Nmap**

Se utilizó la herramienta Nmap para el levantamiento de información técnica y detección de vulnerabilidades en la red del Data Center.

Hallazgos principales: presencia de puertos abiertos sin control, configuraciones por defecto en servidores, servicios expuestos sin segmentación adecuada y ausencia de firewall perimetral robusto.

**5.- Checklist estructurado**

Facilitó la verificación del cumplimiento de políticas y controles de seguridad física, lógica y administrativa. Esta técnica permitió evaluar la existencia de políticas documentadas, controles de acceso y procedimientos de respaldo y monitoreo

**6.- Salvaguardas mediante herramienta PILAR**

La evaluación de salvaguardas se realizó tomando como referencia los riesgos, vulnerabilidades y brechas identificadas en los dominios COBIT 2019 aplicados al Data Center del GAD Municipal del Cantón Bolívar. Este proceso permitió determinar las medidas de protección necesarias para reducir la probabilidad de incidentes y mitigar su impacto sobre la confidencialidad, integridad y disponibilidad de la información institucional.

**7.- Análisis de Referenciales COBIT 2019**

Los hallazgos obtenidos en las diferentes técnicas aplicadas (entrevistas, encuestas, checklist y análisis técnico) fueron contrastados con las buenas prácticas y objetivos del marco de referencia COBIT 2019, con el propósito de evaluar el nivel de madurez y cumplimiento de los procesos del Data Center del GAD Municipal del Cantón Bolívar.

El modelo COBIT 2019 permitió relacionar los resultados del diagnóstico con los dominios y procesos de gobernanza y gestión de TI, identificando las brechas existentes respecto a los niveles de desempeño esperados y las áreas que requieren fortalecimiento para garantizar la seguridad, continuidad y eficiencia de la infraestructura tecnológica, considerando los dominios más relevantes para el entorno del Data Center, entre los cuales se incluyen:

| | |
|---|---|
| **DSS05** | Seguridad de Servicios |
| **APO12** | Gestión de Riesgos |
| **DSS04** | Continuidad y Disponibilidad |
| **APO09** | Gestión de Activos |
| **DSS01** | Operaciones |
| **EDM02** | Asegurar Beneficios |
| **APO07** | Gestión del Personal |
| **BAI09** | Gestión de Activos |
| **MEA01** | Monitoreo y Evaluación |

**Resultados Generales de la Evaluación**

De acuerdo con el marco de referencia COBIT 2019, los niveles de madurez permiten evaluar el grado de desarrollo y control de los procesos dentro de una organización. Un proceso incompleto (nivel 0) carece de implementación o resultados definidos; el nivel realizado (1) indica ejecución sin control ni consistencia formal; el nivel gestionado (2)

refleja planificación y supervisión; el nivel establecido (3) implica la existencia de procedimientos documentados y aplicados de manera coherente, el nivel predecible (4) evidencia una gestión madura, donde los resultados se alcanzan de forma estable y medible, finalmente el nivel establecido (5) determina si el proceso se mejora continuamente basado en datos y análisis de desempeño.

**PLAN DE MEJORA DETALLADO POR DOMINIO COBIT 2019**

| **Dominio COBIT 2019** | **Debilidad identificada / Hallazgo PILAR** | **Impacto** | **Acción de mejora y salvaguarda propuesta** | **Política sugerida** |
|---|---|---|---|---|
| DSS05-Seguridad de Servicios | Ausencia de controles de acceso físico (biometría, tarjetas, cámaras) y deficiencias en la seguridad perimetral física. | Alto | Implementar un sistema integral de control de acceso con autenticación biométrica, cámaras IP, registro digital de entradas y salidas y vigilancia remota. Incorporar sensores de intrusión y alarmas conectadas a un centro de monitoreo 24/7. | Establecer mecanismos de control de acceso físico y lógico al Data Center mediante tecnologías de autenticación biométrica, cámaras IP y vigilancia perimetral, garantizando la trazabilidad de entradas y salidas. |

| | | | | |
|---|---|---|---|---|
| | Falta de segmentación de red, IDS/IPS y monitoreo en tiempo real. Vulnerabilidades detectadas por servicios expuestos según PILAR. | Alto | Implementar firewall de nueva generación (NGFW), segmentación de red por VLAN, sistemas IDS/IPS y plataforma SIEM para detección temprana y análisis de eventos. Aplicar políticas de bloqueo dinámico ante intentos de intrusión. | Implementar una arquitectura de red segmentada y protegida por un firewall de nueva generación, con monitoreo activo y detección temprana de intrusiones. |
| DSS01-Operaciones | Deficiencias en controles ambientales (temperatura, humedad, humo). Riesgo de fallas no detectadas en el entorno físico del Data Center. | Alto | Instalar sensores ambientales integrados al sistema de operaciones con alertas automáticas y monitoreo remoto. Documentar protocolos de respuesta ante variaciones críticas de ambiente. | Mantener un control ambiental automatizado que asegure condiciones óptimas de operación y prevenga fallas por temperatura, humedad o humo |
| | Inexistencia de estrategias de | Alto | Diseñar e implementar un | Garantizar la continuidad de los servicios |

| | | | | |
|---|---|---|---|---|
| DSS04-Continuidad y Disponibilidad | respaldo y recuperación. Falta de políticas de continuidad detectada en PILAR. | | Plan de Continuidad Operativa (PCO) y Plan de Recuperación ante Desastres (DRP) documentado. Configurar respaldos automáticos con almacenamiento redundante y validación de restauración mensual. | tecnológicos mediante un Plan de Continuidad Operativa (PCO) y un Plan de Recuperación ante Desastres (DRP) formalmente documentado. |
| | No se realizan simulacros de contingencia ni se documentan pruebas de recuperación. | Medio | Realizar simulacros semestrales de fallos de sistema y restauración de servicios. Documentar los resultados y acciones correctivas derivadas de cada ejercicio. | |
| APO09-Gestión de Activos | Cableado estructurado desorganizado, sin documentación ni mantenimiento. | Medio | Estandarizar el cableado estructurado mediante etiquetado físico y digital. Incorporar | Estandarizar la gestión física y documental del cableado estructurado y los activos tecnológicos siguiendo |

| | | | | |
|---|---|---|---|---|
| | Riesgo de desconexiones accidentales. | | registros en el sistema de gestión de activos (CMDB) y auditorías visuales semestrales. | normas internacionales. |
| BAI09-Gestión de Activos (procesos específicos) | Ausencia de políticas de ciclo de vida de los activos tecnológicos. Riesgo de obsolescencia y fallas por equipos antiguos. | Alto | Implementar un sistema automatizado de gestión de activos tecnológicos con control de inventario, calendario de mantenimiento, actualización de firmware y sustitución planificada de hardware crítico. | Implementar un sistema de gestión integral del ciclo de vida de los activos tecnológicos. |
| EDM02-Asegurar Beneficios | Escasa participación de la alta dirección y falta de políticas formales de seguridad. | Alto | Crear el Comité Institucional de Seguridad de la Información (CSI) con participación de directivos y responsables de TI. Asegurar la aprobación de políticas y presupuestos de | Fortalecer la gobernanza mediante la creación del Comité Institucional de Seguridad de la Información (CSI) y la definición formal de roles y responsabilidades |

| | | | | |
|---|---|---|---|---|
| | | | seguridad desde el nivel estratégico. | |
| | Ausencia de roles definidos<br><br>en la gestión de infraestructura. Descoordinación y duplicidad de funciones. | Alto | Definir organigramas y roles formales mediante un Manual de Funciones de TI. Establecer matrices RACI para delimitar responsabilidades en operaciones, soporte y seguridad. | |
| APO12-Gestión de Riesgos | Evaluaciones de riesgo no estructuradas (1–2 veces/año). Carencia de matriz de impacto-probabilidad. | Medio | Adoptar un proceso de evaluación continua de riesgos siguiendo COBIT 2019 y metodología PILAR. Utilizar matrices de calor para priorización y mantener un registro histórico de amenazas, vulnerabilidades y mitigaciones. | Adoptar un proceso sistemático y continuo de gestión de riesgos, aplicando la metodología PILAR y los principios de COBIT 2019. |
| | Exposición de puertos y ser vicios detectados | Alto | Deshabilitar servicios innecesarios, | |

| | | | | |
|---|---|---|---|---|
| | por escaneo Nmap. Riesgo de explotación remota. | | actualizar firmware y aplicar parches de seguridad críticos. Configurar monitoreo automatizado para detectar cambios de configuración o nuevas exposiciones. | |
| APO07-Recursos Humanos | Falta de capacitación y concienciación del personal en seguridad de la información. | Medio | Desarrollar un programa anual de formación en ciberseguridad, phishing, contraseñas seguras y uso ético de los recursos tecnológicos. Realizar simulacros trimestrales de respuesta ante incidentes. | Desarrollar un programa institucional de formación continua en seguridad de la información. |
| MEA01-Monitoreo y Evaluación | Falta de monitoreo integral de logs y correlación de eventos. | Alto | Implementar una plataforma centralizada de registro y análisis de eventos (SIEM). Establecer | Asegurar la supervisión continua de los sistemas y procesos mediante auditorías internas y monitoreo centralizado. |

| | | | | |
|---|---|---|---|---|
| | | | procedimientos de revisión diaria de logs críticos y escalamiento automático de alertas. | |
| | Falta de auditorías internas y de cumplimiento de estándares. | Alto | Implementar auditorías internas semestrales basadas en COBIT 2019 y estándares ISO/IEC 27001. Crear un cuadro de mando de indicadores (KPI) para evaluar la madurez de los procesos. | |

**Políticas y procedimientos**

Las siguientes políticas se establecen como parte del plan de mejora de la seguridad de la información del Data Center, con el objetivo de mitigar los riesgos detectados en los dominios evaluados de COBIT 2019, cada política responde a las debilidades identificadas durante el diagnóstico y a las salvaguardas priorizadas mediante la herramienta PILAR.

**DSS05 – Seguridad de Servicios (Física Lógica)**

**Debilidad:** Ausencia de controles de acceso físico (biometría, cámaras, tarjetas) y deficiencias en la seguridad perimetral.

**Política:** Establecer mecanismos de control de acceso físico y lógico al Data Center mediante tecnologías de autenticación biométrica, cámaras IP y vigilancia perimetral, garantizando la trazabilidad de entradas y salidas.

**Procedimiento:**

- Instalar dispositivos biométricos y cámaras con grabación continua de 90 días.
- Crear un registro digital de accesos administrado por el responsable de TI.
- Restringir el ingreso únicamente a personal autorizado mediante credenciales únicas.
- Integrar alarmas y sensores de movimiento con notificación automática.
- Revisar mensualmente los registros de acceso físico y lógico.

**Debilidad:** Falta de segmentación de red, IDS/IPS y monitoreo en tiempo real; servicios expuestos detectados.

**Política:** Implementar una arquitectura de red segmentada y protegida por un firewall de nueva generación, con monitoreo activo y detección temprana de intrusiones.

**Procedimientos:**

- Configurar VLANs para separar entornos críticos y administrativos.
- Implementar sistemas IDS/IPS y una plataforma SIEM para correlación de eventos.
- Realizar escaneos mensuales con herramientas como Nmap para detectar puertos expuestos.
- Bloquear o eliminar servicios innecesarios y documentar los cambios.

- Generar reportes de incidentes y análisis de tráfico semanal.

**DSS01 – Operaciones**

**Debilidad:** Deficiencias en controles ambientales (temperatura, humedad, humo). Riesgo de fallas no detectadas en el entorno físico del Data Center.

**Política:** Mantener un control ambiental automatizado que asegure condiciones óptimas de operación y prevenga fallas por temperatura, humedad o humo.

**Procedimiento:**

- Instalar sensores de temperatura, humedad y detección de humo conectados al sistema de monitoreo.
- Configurar alertas automáticas ante valores fuera de rango.
- Registrar mensualmente las condiciones ambientales.
- Realizar mantenimientos preventivos trimestrales del sistema eléctrico y de climatización.

**DSS04 – Continuidad y Disponibilidad**

**Debilidad:** Inexistencia de estrategias de respaldo y recuperación documentadas.

**Política:** Garantizar la continuidad de los servicios tecnológicos mediante un Plan de Continuidad Operativa (PCO) y un Plan de Recuperación ante Desastres (DRP) formalmente documentado.

**Procedimiento:**

- Configurar respaldos automáticos diarios en entornos redundantes.
- Ejecutar pruebas de restauración mensual para verificar integridad.
- Documentar políticas de recuperación y actualización de software.
- Realizar simulacros semestrales de contingencia.
- Mantener copias externas en ubicaciones seguras (off-site).

**APO09 – Gestión de Activos**

**Debilidad:** Cableado estructurado desorganizado, sin documentación ni mantenimiento, riesgo de desconexiones accidentales.

**Política:** Estandarizar la gestión física y documental del cableado estructurado y los activos tecnológicos siguiendo normas internacionales.

**Procedimiento:**

- Etiquetar físicamente los cables con códigos únicos.
- Registrar en el sistema CMDB la ubicación y estado de cada conexión.
- Actualizar planos de red y topología cada seis meses.
- Realizar inspecciones visuales semestrales de los racks y patch-panels.

**EDM02 – Gobernanza y Roles**

**Debilidad:** Escasa participación de la alta dirección y ausencia de roles definidos en seguridad.

**Política:** Fortalecer la gobernanza mediante la creación del Comité Institucional de Seguridad de la Información (CSI) y la definición formal de roles y responsabilidades.

**Procedimiento:**

- Conformar el CSI con directivos y responsables de TI.
- Aprobar anualmente las políticas, presupuesto y plan de seguridad.
- Implementar matrices RACI que delimiten funciones operativas y estratégicas.
- Actualizar el manual de funciones del personal TI.

**APO12 – Gestión del Riesgo**

**Debilidad:** Evaluaciones no estructuradas y exposición de servicios detectados por PILAR.

**Política:** Adoptar un proceso sistemático y continuo de gestión de riesgos, aplicando la metodología PILAR y los principios de COBIT 2019.

**Procedimiento:**

- Elaborar una matriz de impacto-probabilidad con los riesgos detectados.
- Clasificar riesgos según nivel: bajo, medio, alto, crítico.
- Aplicar controles preventivos y mitigadores priorizados.
- Registrar riesgos residuales y revisar semestralmente el mapa de calor.
- Presentar los resultados al CSI para su validación.

**MEA01 – Monitoreo y Evaluación**

**Debilidad:** Ausencia de auditorías internas y falta de monitoreo de logs y eventos.

**Política:** Asegurar la supervisión continua de los sistemas y procesos mediante auditorías internas y monitoreo centralizado.

**Procedimiento:**

- Implementar una plataforma SIEM para análisis y correlación de eventos.
- Revisar diariamente los logs críticos de servidores y firewalls.
- Realizar auditorías internas semestrales bajo COBIT 2019.
- Establecer indicadores KPI de cumplimiento y madurez.
- Documentar hallazgos y ejecutar planes de acción correctivos.

**APO07 – Recursos Humanos**

**Debilidad:** Falta de capacitación en ciberseguridad y bajo nivel de concienciación.

**Política:** Desarrollar un programa institucional de formación continua en seguridad de la información.

**Procedimiento:**

- Establecer un calendario anual de capacitaciones para todo el personal.
- Incluir temáticas sobre contraseñas, phishing, uso de correo y ética digital.
- Aplicar pruebas de simulación de ataques trimestrales.
- Evaluar resultados y reforzar temas de bajo desempeño.

**BAI09 – Ciclo de Vida de Activos.**

**Debilidad:** Falta de políticas de mantenimiento y renovación tecnológica, obsolescencia detectada.

**Política:** Implementar un sistema de gestión integral del ciclo de vida de los activos tecnológicos.

**Procedimiento:**

- Registrar los activos desde su adquisición hasta su baja en un sistema CMDB.
- Planificar mantenimientos preventivos y actualizaciones de firmware.
- Programar reemplazos de equipos críticos con base en antigüedad o rendimiento.
- Revisar anualmente el inventario y las políticas de renovación.

**Conclusiones**

- ✓ El nivel de madurez actual del Data Center se encuentra entre inicial y gestionado, lo que implica una seguridad limitada y procesos poco formalizados.
- ✓ El análisis reveló vulnerabilidades críticas en infraestructura, continuidad y gobernanza que pueden afectar la disponibilidad de servicios municipales.
- ✓ El plan propuesto, basado en COBIT 2019, establece políticas y acciones concretas para reducir riesgos y elevar la seguridad institucional.
- ✓ La implementación del plan permitirá alcanzar un nivel de madurez definido y optimizado, garantizando mayor confiabilidad en los servicios y protección de la información ciudadana.

**Recomendaciones**

- ✓ Priorizar la ejecución de las acciones de corto plazo, ya que son de bajo costo y alto impacto (documentación, monitoreo, backups cifrados).
- ✓ Asignar presupuesto y recursos humanos suficientes para implementar los controles de seguridad propuestos.
- ✓ Conformar un Comité de Seguridad Informática que asegure la gobernanza y el cumplimiento de políticas.
- ✓ Adoptar un enfoque de mejora continua (PDCA) en seguridad informática, actualizando políticas y controles de acuerdo con nuevas amenazas.
- ✓ Evaluar la posibilidad de integrar soluciones de nube híbrida y redundancia en el mediano plazo, para fortalecer la continuidad operativa del Data Center.