AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA GESTIÓN DE LOS CENTROS DE DATOS DE JASEC

INFORME DE AUDITORÍA FINAL

ATO-029-2024

CONTENIDO:

SIGLAS Y ABREVIATURAS

A continuación, se detalla las siglas y abreviaturas utilizadas en este informe:

SIGLAS/ ABREVIATURAS	SIGNIFICADO
ANSI	American National Standards Institute
BCMS	Sistema de Gestión de Continuidad del Negocio
BCP	Business Continuity Plan o Plan de Continuidad de las operaciones
CD / CPD	Centro de Datos o Centro Procesamiento de Datos
CGR	Contraloría General de la República
DRP	Plan de recuperación ante desastres
GAC	Gestión de la Arquitectura y Comunicaciones
GCR	Gestión de Calidad y Riesgos
ISO	Organización Internacional de Normalización o Estandarización
JASEC	Junta Administrativa del Servicio Eléctrico de Cartago
LGCI	Ley General de Control Interno
LOG	Registro de Eventos de tipo Logaritmo (Bitácora, Registro o Historial)
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
MTPD	Período máximo tolerable de interrupción
NAS	Network Attached Storage (Almacenamiento en la red local)
NGASP	Normas Generales de Auditoría para el Sector Público
NIST	Instituto Nacional de Estándares y Tecnología de los Estados Unidos
NOC	Centro de la Operación de la red
PATI	Proceso de Tecnología de Información (JASEC)
RPO	Objetivo de punto de recuperación
RTO	Objetivo de tiempo de recuperación
SAC	Sistema de Apertura de Cajas
SAN	Storage Area Network (Red local de Almacenamiento)
SGSI	Sistema de Gestión de Seguridad de la Información
TI	Tecnología de Información
TIA	Telecommunications Industry Association
TIC	Tecnologías de Información y Comunicaciones

Fuente: Elaboración propia Auditoría Interna, 2025

RESUMEN EJECUTIVO

¿Qué examinamos?

Se examinó el plan de continuidad de la plataforma tecnológica aplicada a los tres Centros de Procesamiento de Datos de JASEC, verificándose que estuviera alineado y conforme al Marco normativo aplicable (Marco Normativo Gobierno y Gestión TI v2 2022 del MICITT, ISO/IEC 27001 gestión de la seguridad de la información, ISO 22301 gestión de la continuidad del negocio y ANSI/TIA 945).

¿Por qué es importante?

Un plan de continuidad actualizado garantiza que los servicios críticos de tecnología puedan mantenerse o restaurarse rápidamente ante incidentes e interrupciones, disminuyendo el tiempo de inactividad y reduciendo costos con posibles pérdidas, ya que apegarse a un plan de mantenimiento actualizado; fortalece la confianza ante los clientes y la integridad de la empresa, permitiendo estar preparados para una recuperación rápida y eficiente, y minimizando impactos operativos y financieros.

En la actualidad, las empresas corporativas de interés público enfrentan constantes amenazas de posibles ataques cibernéticos, lo que compromete la seguridad de la información y la ciberseguridad de sus datos. Por tanto, es esencial que los Centros de Procesamiento de Datos de JASEC fortalezcan continuamente los mecanismos de continuidad e inspecciones en sus centros de datos, con el objetivo de mantener siempre actualizado el plan de continuidad y gestión de riesgos, esto por cuanto un plan de continuidad asegura que, en caso de un ataque cibernético o una falla del sistema, el centro de datos pueda recuperarse rápidamente y minimizar el tiempo de inactividad, lo cual es crucial para mantener la confianza de los clientes y la integridad de los datos, así como salvaguardar el patrimonio de la institución y reducir costos ante pérdidas potenciales causadas por un ataque cibernético.

¿Qué encontramos?

La evaluación realizada ha revelado que el marco normativo de tecnologías de información actualmente vigente se encuentra desactualizado, además no se ajusta a los estándares de gobernanza, ni a la gestión tecnológica establecidos por el MICITT para la gestión de los Centros de Procesamiento de Datos de JASEC.

Asimismo, se identificaron oportunidades de mejora en cuanto al contenido, gestión y actualización de los inventarios de equipo de cómputo de los centros de datos, así como las condiciones de seguridad, físicas, técnicas y ambientales de estos centros; aunado a la ausencia de una estructura organizacional clara que garantice la aplicación de los controles necesarios para la recuperación de posibles desastres que pueden afectar los servicios actuales de JASEC, los cuales se resguardan en los equipos de cómputo en los Centros de Datos.

¿Qué sigue?

De acuerdo con los resultados obtenidos, se emiten recomendaciones dirigidas a las jefaturas de los Departamentos de Gestión de la Arquitectura y Comunicaciones, y Operación de la Red e Infocomunicaciones, las cuales están orientadas en fortalecer el proceso de renovación de los Planes de Continuidad de la plataforma tecnológica de los tres Centros de Datos de JASEC, cuyo plazo de implementación comprende el periodo de mayo a noviembre del 2025.

9 de abril de 2025

INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

La auditoría a que se refiere el presente informe se efectuó en cumplimiento a los Planes Anuales de Trabajo de la Auditoría Interna del 2024 -2025, a los resultados obtenidos en el análisis sobre la viabilidad, al nivel de riesgo y la importancia relativa para la operatividad de la JASEC.

OBJETIVO GENERAL

Verificar si JASEC aplica los mecanismos de control de alta disponibilidad y recuperación de desastres en sus Centros de Datos, de acuerdo con la normativa técnica y legal aplicable.

ALCANCE

La auditoría se desarrolló en los Centros de Procesamiento de Datos de JASEC (ubicados en el Edificio Central de JASEC, Centro de Control de la red o NOC El Bosque y Centro de Operaciones de Infocomunicaciones), evaluando los controles aplicados a la alta disponibilidad y recuperación de desastres disponibles (Sistema de Gestión de Continuidad del Negocio BCMS y plan de continuidad BCP). El período evaluado comprende de setiembre del 2024 a diciembre del 2024, ampliándose a febrero del 2025.

METODOLOGÍA

1.1.1.Declaratoria de cumplimiento de las normas

La auditoría fue realizada de conformidad con las Normas Generales de Auditoría para el Sector Público y las Normas para el Ejercicio de la Auditoría Interna en el Sector Público, ambas emitidas por la CGR, con el Reglamento de Organización y funcionamiento de la Auditoría Interna y según lo respaldan los resultados del Programa de aseguramiento y mejora de la calidad de la actividad de esta Auditoría, así como la demás normativa de auditoría de aplicación y aceptación general.

1.1.2.Metodología de auditoría

La auditoría aplica la metodología para proyectos de aseguramiento de control interno de la Auditoría Interna de JASEC, la cual contempla 4 actividades, a saber: I- Planificación, II-Examen, III-Comunicación de Resultados y IV-Seguimiento.

1.1.3.Criterios de Auditoría

La comunicación de los criterios de auditoría aplicados se remitió al jefe de Departamento de Gestión de la Arquitectura de Comunicaciones (GAC), al Jefe de Departamento de Operación de la Red de Fibra, y a la Jefa de Departamento de Operación de la Red mediante el oficio AUDI-310-2024; el día 24 de octubre de 2024, los cuales se detallan a continuación:

- Normas técnicas para la gestión y el control de las Tecnologías de Información 2021
- MICITT - Marco Normativo Gobierno y Gestión TI 2022
- MICITT - Perfil de la Gestión de TI - Matriz 2021
- MICITT - Código Nacional de Tecnologías Digitales 2024
- MICITT - Normas Portafolio de Riesgos TI
- NSI/TIA-942-2005 - Estándar de infraestructura de telecomunicaciones para centros de datos
- MICITT - Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información 2022
- Normas de Control Interno para el Sector Público, (N-2-2009-CO-DFOE)
- Norma ISO/IEC 27001:2022 3a Ed

Además, asimismo, durante en el desarrollo de la auditoria se amplió, debido a la ampliación del alcance de las pruebas, lo cual permitió evaluar el cumplimiento de se consideraron los siguientes criterios:

- Gestión de las Tecnologías de Información y Comunicación – PATI
- Plan Estratégico para la Función Informática – PATI.PR1.NR7
- Marco Normativo de la Política de Seguridad de la Información – PATI.PR1.NR5
- Plan de Continuidad de la Plataforma Tecnológica – PATI.PR2.NR5
- MICITT: Plan general de la emergencia ciberataques, Decreto: N°43542-MP-MICITT 2022.

- COBIT 2019 Objetivos de gobierno y gestión.
- NIST SP 800-53 v.4
- ISO/IEC 22301:2019
- ISO_IEC_FDIS_27002_(E)

1.1.4.Proceso Administrativo analizado

En la auditoría se analizaron los procesos administrativos sobre los controles aplicados a la alta disponibilidad y recuperación de desastres de los tres Centros de Procesamiento de Datos de JASEC, basándose en los procedimientos de BCP descritos anteriormente, los cuales fueron comparados y analizados de conformidad con el marco normativo nacional e internacional aplicable.

ANTECEDENTES ACERCA DE LO AUDITADO

En el periodo 2018, esta Auditoría Interna mediante el servicio ATI-R-02-2018 denominado "Evaluación de los planes de continuidad del negocio y recuperación ante desastres de los procesos críticos de TI", se determinó que el Plan de Continuidad de la Plataforma Tecnológica de JASEC, fue elaborado en 2014 y no había sido actualizado desde entonces, además de que las revisiones se realizaban a criterio de la jefatura del Área de TIC sin procedimientos formalizados, aunque la planificación asignaba responsables de la actualización y pruebas de los planes de continuidad a las distintas Áreas de Negocio.

Asimismo, en el periodo 2024, la Auditoria Interna desarrolló la auditoria ATO-019-2024 *"Auditoria de Carácter Especial sobre el estado de la gestión de la seguridad de la información y la ciberseguridad"*[1]. Mientras que la Auditoría externa, mediante las cartas a la gerencia emitidas por el Despacho MOORE - AGC (Asesores Gerenciales Corporativos); "Controles Generales del Computador, al 31 de diciembre de 2023" y "Controles Generales del Computador, al 31 de diciembre de 2024". En estas se concluye que el Marco Normativo de Gobierno y Gestión de TI no ha estado alineado conforme lo solicitado por el MICITT, por lo que se recomendó actualizar normas, procedimientos y realizar cambios, necesarios para coordinar el desarrollo del Marco Normativo de TI conforme a lo requerido.

COMUNICACIÓN PRELIMINAR

En cumplimiento a los artículos 35 de la Ley General de Control Interno, 30[2] y 31[3] del Reglamento de Organización y funcionamiento de la Auditoría Interna, se tiene que:

1.6.1 El borrador del presente informe fue remitido a la Dirección Comercial, Área de Tecnologías de Información y Comunicación, al Departamento de Gestión de la Arquitectura de Comunicaciones y al Departamento de Operación de la Red en un plazo de 1 día hábil, mediante el oficio AUDI-088-2025, el 18 de marzo 2025, con el propósito de que en la conferencia final se formularan las consulta y/u observaciones que se consideraran pertinentes sobre su contenido. Al respecto, se recibieron observaciones al borrador de este informe mediante el oficio SUBG-TIC-GAC-097-2025, el 25 de marzo 2025, las cuales fueron documentadas y analizadas en el **Apéndice N°1**.

1.6.2 La comunicación preliminar de los resultados, producto de la auditoria que alude este informe, se llevó a cabo el 19 de marzo 2025, por medio de la plataforma Teams, con la participación de las siguientes personas: Rodolfo Sanabria Hernández, Director Comercial, Osvaldo Navarro Navarro, Jefe de Área Tecnologías de Información y Comunicación, Mario Jiménez Brenes, Jefe de Área Distribución, Julio Quesada Garita Jefe de Departamento de Gestión de la Arquitectura de Comunicaciones, y María del Milagro Villalta Romero, Jefa de Departamento Operación de la Red. Al respecto, se recibieron observaciones al borrador de este informe, las cuales fueron documentadas y analizadas en el **Apéndice N°1**.

[1] Comunicada mediante los oficios: AUD-317/318-2024 y AUD-073/074-2025

[2] **Comunicación de resultados:** De previo a la comunicación oficial del informe, se expondrá en una conferencia final con las personas funcionarias a las que se les dirigió, con el propósito de retroalimentarse respecto a los resultados. / De no haberse llegado a una conciliación del informe en la conferencia, el o los responsables de las recomendaciones comunicarán por escrito, en el plazo definido por el titular de la Auditoría Interna, las observaciones al borrador del informe, con el debido sustento. /Las observaciones serán analizadas por la Auditoria Interna y de ser aceptadas se contemplarán en el respectivo informe de auditoría. A partir de estas observaciones, la Auditoría Interna podrá variar su criterio y, si es del caso, modificar el contenido de su informe, cuando así se le demuestre con razones fundadas y a su entera satisfacción. El análisis de tales observaciones se incorporará como un apéndice al informe final. /En el caso de resultados de los que pueden derivarse eventuales responsabilidades, la comunicación debe realizarse observando la normativa específica emitida por la Contraloría General de la República.

3 Informes parciales y definitivos: La Auditoría Interna, de acuerdo con su criterio, podrá emitir informes parciales durante el desarrollo de sus auditorías, los cuales serán expuestos los resultados del servicio de auditoría en la conferencia final, analizadas y revisadas las observaciones al informe borrador, el titular de la Auditoría Interna deberá comunicar a los titulares subordinados correspondientes, los resultados definitivos mediante un Informe Final, a efecto de que se implementen las recomendaciones y sus planes de acción dentro del plazo acordado.

RESULTADOS

Durante el desarrollo de los objetivos de esta auditoría y de conformidad con el alcance de este, se determinaron los hallazgos que se describen a continuación.

2.1. Implementación de controles de inspección

Criterio N°1: Matriz Guía, Implementación Buenas Prácticas Basadas en *COBIT 2019:* Marco de referencia para el gobierno y la gestión de la información y la tecnología, dirigido a toda la empresa. (MICITT) "Dominio: Alinear, Planificar y Organizar, Objetivo de gestión: APO12—Gestionar el riesgo Descripción, Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa. Propósito Integrar la gestión del riesgo empresarial relacionado con la I&T con la gestión del riesgo empresarial global (ERM), y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con las I&T".

El Departamento de Gestión de la Arquitectura de Comunicaciones (GAC), gestiona la alta disponibilidad de los centros de procesamiento de datos con un porcentaje de **56%** del marco normativo desactualizado respecto con al Marco Normativo Gobierno y Gestión TI del MICITT, identificándose además que el **18%** de la normativa interna de JASEC no tienen en su contenido lo solicitado por el Marco Normativo Gobierno y Gestión TI del MICITT, tal situación se detectó en los lineamientos de: arquitectura de la información, gestión de la calidad y activos de TIC; modelo de servicios de TI, gestión de proveedores de TI, gestión del desarrollo de aplicaciones y tecnologías, gestión de la continuidad y disponibilidad de los servicios de TIC, lo que conlleva a no disponer de un Plan de Continuidad de TI.

Ahora bien, sobre los diferentes listados para el inventario de equipo, a continuación, se presenta una tabla con la condición de cada Centro de Datos de JASEC:

Tabla N° 1
Listado de los inventarios centros de datos
-A octubre de 2024-

LISTADOS	EDIFICIO CENTRAL	EL BOSQUE	INFOCOMUNICACIONES
SERVIDORES EN EL CENTRO DE DATOS	-Cuenta con inventarios parciales pues no incluyen: actualizaciones, equipos nuevos, localización, números de activo incompletos.	-No contiene los servidores mencionados en los listados de GAC, a excepción de SCADA. -Únicamente se menciona qué es el activo, no hay más información.	Cuenta con la información suficiente.
EQUIPO DE RED	-Está desactualizado, los equipos mencionados son muy antiguos, ya no están conectados según se indica en el listado. -No incluye sistemas instalados a partir del 2022. -Los datos no coinciden con otros listados del mismo centro de datos o están desactualizados.	-En el listado solo se menciona qué es el activo de red y dirección IP, no hay más información que permita localizar el activo y saber su ubicación física.	Cuenta con la información suficiente. (actualizado y completo, los sistemas generan reportes y éstos pueden integrar suficiente información del activo, cuenta con control de direcciones IP, etiquetado para gestión autónoma o interna)
EQUIPO DE CÓMPUTO	-Se encuentra incompleto el inventario de equipamiento del empleado, pues hay personal nuevo que no está incluido.	-No, indica los equipos del NOC o del DC, señalados como existentes en listados de GAC.	-Carece de información sobre el dueño del equipo de cómputo.
SOFTWARE	-Del "Inventario de equipamiento del empleado", esta desactualizado los softwares de cada equipo de las personas colaboradoras -No hay inventarios exclusivos de software.	-el inventario de software está incompleto, solo se enlistan los sistemas de uso habitual (FONT, SCADA, ICCP, NOJA), además no hay información en qué equipos están instalados.	-No hay información.
OTROS COMPONENTES EXTERNOS COMO CABLEADO Y OTROS DISPOSITIVOS.	-No se tienen identificados, a excepción de los electrógenos y aires acondicionados. -No hay un sistema de identificación de periféricos.	-No se tienen identificados, a excepción de los electrógenos y aires acondicionados. -No hay un sistema de identificación de periféricos	-No hay un sistema de identificación de periféricos

Fuente: Elaboración propia.

El Departamento de GAC no demuestra la existencia de acciones específicas para desarrollar la documentación de riesgos en el SEVRI e implementar el Marco de MICITT, así como identificar los riesgos en relación con el gobierno y gestión de TI, lo que impide o posterga la planificación y desarrollo de planes estratégicos y procedimientos de continuidad necesarios para actualizar las normas internas, además de que carece de personal específicamente delegado y capacitado para dar soporte a la calidad del marco normativo PATI.

El no cumplimiento de la normativa para la gestión de riesgo de los equipos de alta disponibilidad, expone la continuidad de los negocios JASEC (disrupción de las operaciones), afectando tanto clientes internos como externos (pérdida de reputación y pérdida de clientes),

exponiéndose además a riesgos tecnológicos como amenazas y ataques cibernéticos, costos de recuperación, así como subestimar riesgos críticos en la operativa del negocio, como omisiones operativas por no mantener actualizado el marco normativo de TI, afectando la calidad en la atención a clientes y los servicios de TI, brindados a la organización.

2.2. Gestión de Continuidad de Negocio

Criterio N°2: ISO/IEC 22301:2019: "Seguridad y resiliencia -Continuidad del negocio, sistemas de gestión -Requisitos": *"La organización debe implementar y mantener una estructura que permita la advertencia y la comunicación oportunas a las partes interesadas relevantes y proporcionar planes y procedimientos para administrar la organización durante una interrupción. Los planes y procedimientos se utilizarán cuando sea necesario para ejecutar soluciones de continuidad del negocio."*

Los Centros de Datos del Edificio Central y el Bosque no cuentan con inventario de activos que contengan: plan de gestión de la obsolescencia, información detallada de proveedores de servicios actualizado como plan de mantenimiento y soporte, control de localización de los respaldos físicos y redundancia para garantizar la contingencia de los sistemas de cómputo, así como inventarios de accesorios y periféricos de respaldo para los sistemas. Caso contrario, el Centro de Datos de Infocomunicaciones cuenta con inventarios de algunos equipos y componentes de la red, pero deben ser mejorados en cuanto a la valoración del activo e información del ciclo de vida como coste de obtención, análisis de obsolescencia o curva de depreciación y garantías, así como información del soporte (empresa/operario responsable y sus datos de contacto). Además, JASEC no cuenta para sus tres centros de datos con planes de infraestructura e inversiones que permitan proyectar los requerimientos y mantenimiento de infraestructura tecnológica (preventiva, por obsolescencia, mejora).

La jefatura del Departamento del GAC señala que no existen planes e inventarios actualizados en el Centro de Datos del Edificio Central, pues se carece de la planificación de continuidad adecuada debido a la falta de personal para realizarlo, sin embargo, poseen de la información necesaria para realizar los inventarios, tales como: el cómo número de activo, manuales técnicos, documentación de proveedores, descripción de los dispositivos y reportes de soporte.

En cuanto al Centro de Datos de Centro de Control el Bosque, no existe una retroalimentación, registro y comunicación constante entre el encargado del Centro de Datos con los operarios, pues estos últimos son quienes realizan el mantenimiento y poseen la información para realizar y actualizar los inventarios, sin embargo, es un levantamiento que puede realizarse puesto que poseen la información necesaria.

No contar con inventarios y planes actualizados expone a JASEC a gastos adicionales cuando se requiera sustituir equipo sin previa planificación, además, no contar con inventarios detallados, compromete al riesgo de no controlar a qué sistemas deben ejecutarse las actividades de respaldo durante una contingencia, con prioridad, lo que puede llevar a excesos de inversión de tiempo y posibles filtraciones de datos a personal no autorizado, incluso a configuraciones incorrectas o descontrol afectando la exactitud y aprovechamiento de los sistemas. Asimismo, sin información actualizada, es complicado gestionar con rapidez el soporte de RTO y RPO, lo que puede llevar a fallos inesperados y tiempos de inactividad prolongados.

2.3. Infraestructura de los centros de datos y seguridad perimetral

Criterio N°3: ANSI/TIA-942 – 2005: "Estándar de infraestructura de telecomunicaciones para centros de datos".

El Centro de Datos del Edificio Central presenta las siguientes condiciones: el acceso al edificio cuenta con guardas de seguridad, pero el ingreso al centro de datos se realiza de manera convencional (carece de dispositivos biométricos o cierre electrónico con RFID), no posee sensores de apertura con alerta, ni cerraduras con sensor por lo que su apertura y cierre es con llave, sin generar alertas o notificar ingresos. En cuanto a la señalización, el centro carece de señales de salida y luces de emergencia en caso de apagón, manuales técnicos o de soporte de emergencia. Además, este centro carece de herramientas que permitan supervisar, analizar y responder a alertas de aplicaciones, redes e infraestructuras, además de que no se están generando históricos de registros y los sistemas de monitoreo no generen alertas, lo cual derivó a que el 18 de enero del 2025, se tardara más tiempo en responder a la pérdida de energía ocurrida en el Centro.

En relación con el Centro de Datos del Bosque se determinó que la entrada al Edificio cuenta con cerradura electrónica y sensor tipo RFID, sin embargo, se constató que las cámaras de seguridad no tienen cobertura integral del ingreso al Centro de Datos, y la iluminación requiere mantenimiento, además se encontró que, el uso de bitácora de acceso no se utiliza más que para el acceso de terceros para

mantenimiento. Este centro carece de un Higrómetro[4], que permita un mejor aprovechamiento de los aires acondicionados de tipo Split[5]. En la inspección realizada el 18 de diciembre del 2024 se verificó que un aire acondicionado se encontraba dañado, la infraestructura física tiene hongos en cielo raso, y la iluminación del Centro de Datos presenta algunos tubos fluorescentes dañados.

Por el contrario, el Centro de Datos de Infocomunicaciones cuenta con mejores condiciones de infraestructura, acceso y ambientales que los otros centros, sin embargo; cuenta con problemas de dispersión del aire por todo el espacio físico por lo que se acude a ventiladores.

Las condiciones del Centro de Datos del Edificio Central se deben, a que según menciona el jefe del Departamento GAC se ha solicitado los recursos para las mejoras, pero no han sido otorgados, se solicitó más información, pero no se encontró documentación que respalde la petición de mejoras.

En cuanto a la caída de dos sistemas de servidor de virtualizado y bases de datos sistema SAC Sistema de Cobro afectando a GCR (Departamento de Gestión de Calidad y Riesgo) por casi 8 horas en el Centro de Datos en el Edificio Central, se debió a que una celda del tendido eléctrico ubicado en paraíso, fue dañado por fauna y esto generó a que las Oficinas del Edificio Central (donde está ubicado el Centro de Datos) se quedara sin electricidad por al menos 4 horas y 22 minutos, provocando que una de las UPS que soportan el sistema de SAC debido a que no contaba con la capacidad de carga suficiente para mantener activos los equipos de cómputo el tiempo suficiente hasta activar apropiadamente el generador auxiliar (el cual si se activó poco después para los demás equipos con la otra unidad), esto se debió a que no se retomó el mantenimiento de las UPS trifásicas, debido a la postergación de su reemplazo a marzo 2025 en la contratación 2024LD-000113-0018300001 “Adquisición de dos Sistemas de Alimentación Ininterrumpida para el Centro de Datos Principal” responsable de Julio Enrique Quesada Garita Jefe de GAC.

Ante esta situación, JASEC se expone al acceso de personal no autorizado a los Centros de Datos, lo que aumenta el riesgo de robo, sabotaje o manipulación de equipos y datos, en cuanto a las condiciones ambientales se expone al riesgo de daños o mal funcionamiento del equipo, deterioro del equipo (corrosión), lo que conlleva al aumento de costos operativos para reemplazarlo o repararlo. Asimismo, y ante la condición de la omisión de mantenimiento, se materializó el riesgo de la caída de dos sistemas: Virtualizado y de Bases de Datos, lo cual afectó en la paralización de servicios de facturación, Gestión de Calidad y Riesgo (GCR) y así como labores administrativas que requieren el uso de las bases de datos del sistema financiero, tal como el Sistema de Apertura de Cajas y cobros (SAC).

2.4. Matriz Guía de Implementación de Prácticas de Gobierno y Gestión

Criterio N°4: MICITT: Marco Normativo de Gobierno y Gestión de las Tecnologías de Información: “Para asegurar la disponibilidad del Marco de Gestión de Tecnología de Información Institucional, la institución debe establecer los procesos al nivel de Tecnologías de información, que permitan brindar servicios efectivos para mantener la operativa institucional, salvaguardar los datos que se capturan, procesan, organizan, distribuyen y resguardan.”.

A partir del análisis de la alineación de la normativa interna con la normativa gubernamental (Marco Normativo Gobierno y Gestión TI v2 2022), que evalúa la gestión estratégica de gobierno y operativa de las TIC mediante la herramienta del MICITT, “*Perfil de la Gestión de Tecnologías de la Información”,* se identificó que los componentes de las normas a evaluar se dividen en **90 “procesos”** basados en normas ISO27001 y COBIT 2019, de los cuales JASEC cubre el **60%** para el Nivel de Gestión, cuyo estado de definición en el que se encuentra el proceso corresponde al siguiente:

- Pendiente **60%:** No se ha documentado ni ejecutado.
- En Proceso **34%:** Se están realizando y formalizando acciones.
- Finalizado **6%:** Se cuenta con un proceso formal asociado y se aplica en forma adecuada y consistente.

El detalle de estos resultados se expone en el Anexo N°1, en el cual se muestra que la ejecución de los procesos: dependen del personal, sus competencias y su conocimiento, se obtiene una calificación de **58%**, mientras que el **34%** de éstos aún requieren del personal, pero “cumple con lo mínimo requerido” por contar con formularios, mientras que el **8%** son actualizados, medibles y controlados constantemente.

El nivel de gestión y el estado de definición del proceso documental de la JASEC, según los parámetros del modelo de madurez por etapas establecido por el MICITT, se encuentra en nivel “bajo”, por cuanto **“se depende del personal**”, ya que se carece de procesos documentados y actualizados, por lo que la institución en su gestión de TIC depende del conocimiento del personal que lo ejecuta. Sobre

[4] Dispositivo diseñado para poder medir tanto la temperatura como la humedad del aire, instrumento para comprobar las condiciones climatológicas en almacenes y salas de computadoras.
[5] Divide su sistema en dos unidades: una unidad exterior (el condensador) y otra unidad interna (el evaporador) donde ambos aparatos están comunicados mediante tubos, hay de dos tipos con inverter o convencional.

el particular, el jefe del Departamento GAC señala que con el recurso humano actual no es posible gestionarlo, pues no hay tiempo disponible para dar soporte a la actualización constante que requiere la documentación.

Lo expuesto anteriormente, podría exponer a la JASEC a los riesgos de incumplimiento de las estrategias gubernamentales para el sector público, eventuales sanciones por incumplimiento, perdida de imagen y reputación ante las regulaciones del gobierno, ya que la normativa emitida del MICITT es de acatamiento obligatorio para las instituciones y órganos sujetos a la fiscalización de la Contraloría General de la República, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable. Además, la eventual dependencia del personal para la operativa de las TIC y que esto no esté debidamente documentado acorde con la normativa supra citada puede exponerse al riesgo de erróneas ejecuciones del proceso por malas interpretaciones, duplicidad o pérdida de la información.

2.5. Inventarios del Plan de continuidad de TI.

Criterio N°5: PATI.PR2.NR5, Plan de continuidad de la plataforma tecnológica: "Inventario de ambiente de seguridad, Inventario de comunicaciones, Inventario de centrales telefónicas, Inventario de servidores físicos, inventario de servidores virtuales, Inventario de aplicaciones, Virtualización y SAN".

PATI.PR1.NR5, Marco normativo de la política de seguridad de la información: *3.6 Clasificación de los Activos "Deberán generarse los inventarios de los activos para garantizar la vigencia de una protección eficaz de los recursos. Estos inventarios de activos son fuente de información para la administración de riesgos, dado que con éstos se identifican los activos y el valor relativo e importancia de los mismos. Todo componente del inventario al menos debe tener una clasificación por la importancia hacia los sistemas de aplicación y la seguridad, adicionalmente es importante destacar su propietario y la ubicación". 5.9 Procedimientos de vigilancia/monitoreo "Seguridad Informática deberá realizar un inventario de todos los recursos informáticos de la organización que sean asignados a los empleados para el cumplimiento de sus funciones (ej. laptops, computadoras personales, etc.). Este inventario debe mantenerse actualizado y en éste se debe identificar el tipo de equipamiento entregado y los datos del empleado responsable del mismo".*

ISO/CEI 27002:2022(E) - 5.9 Inventario de información y otros activos asociados: "La organización debería identificar su información y otros activos asociados y determinar su importancia en términos de seguridad de la información. La documentación debe mantenerse en inventarios dedicados o existentes, según corresponda".

MICITT CNTD 2024: p.83, Controles para protección de equipos: "La arquitectura de ciberseguridad debe de contar con procedimientos para levantar y mantener un inventario de activos digitales necesarios para la operación de la organización".

En los inventarios se registran equipos claves como switches, firewalls y servidores, la información es dispersa, desactualizada y carece de detalles, además, se determinaron inconsistencia en datos como números de serie, placas, niveles de criticidad, configuraciones de hardware y software, fechas de adquisición y contratos de mantenimiento.

Por otra parte, el Área de Infocomunicaciones dispone de inventarios detallados y actualizados de sus equipos, incluyendo hardware, software, redes y sistemas de respaldo de bases de datos, sin embargo, es necesario desarrollar inventarios orientados a garantizar la continuidad en caso de incidentes, esto debido a que estos permiten planificar y ejecutar acciones de recuperación ante desastres de manera más eficiente.

Para el listado gestionado por el Departamento GAC, se determinó lo siguiente:

a. No se ha implementado una solución de gestión de contraseñas centralizada, lo que resulta en la reutilización de credenciales en múltiples sistemas y el almacenamiento inseguro de contraseñas en documentos compartidos Excel, contraviniendo los principios de seguridad establecidos en ISO 27002.
b. El alcance de los inventarios de activos de TI es incompleto y desactualizado, lo que impide una gestión efectiva de los mismos y la evaluación de riesgos asociados.
c. Faltan registros detallados sobre los planes de mantenimiento, inversiones y contactos de soporte contratado, lo que compromete la disponibilidad y el rendimiento de los sistemas.

Asimismo, hay ausencia de procesos robustos y políticas para la administración de inventarios de estos activos.

Los listados del Centro de Control del Bosque solo registran la presencia de los sistemas, sin proporcionar detalles esenciales como ubicación, número de serie o características técnicas, lo anterior compromete la calidad de la información de los inventarios, ya que no incluye datos fundamentales como: responsable del equipo, estado actual, proveedores, servicios asociados, configuración de hardware, fecha de adquisición y registro de mantenimiento.

Esta situación podría limitar la gestión eficiente de los activos, la evaluación de riesgos y la planificación orientada a la continuidad de las operaciones, por lo que carecen de referencias a procedimientos de recuperación e identificación de RPO y RTO, así como a alternativas para operar en caso de que las instalaciones principales resulten dañadas.

La condición se debe a que existe una gestión descentralizada y no estandarizada de los inventarios de equipo de cómputo de los Centros de Procesamiento de Datos de JASEC, además, existe la delegación de la gestión de activos críticos (servidores, aplicaciones, etc.) a contratistas externos bajo servicios tercerizados.

Al no disponer de inventarios actualizados de los activos del equipo de cómputo de los Centros de Procesamiento de Datos de JASEC, la institución se expone al riesgo de ineficiente gestión e información no integrada, información poco confiable al no cumplir con los estándares establecidos para garantizar la continuidad operativa. Además, al presentar información como contraseñas, representan un riesgo crítico para la seguridad y ciberseguridad. Por otro lado, el desconocimiento de la vigencia de los activos, o la información de cuándo corresponde su mantenimiento pondría en riesgo el activo de quedar en abandono, o que no se incluya en planes de soporte o actualización.

Asimismo, la gestión de los servidores, aplicaciones y otros componentes bajo el servicio OneWay Technologies, Applied y Electrotécnica, limitan la visibilidad de necesidad de soporte y control por parte de la institución, junto con el hecho que el contenido de los inventarios presentan las citadas debilidades de control, exponen a la JASEC al riesgo de falta de planificación del RPO o RTO y omiten información crítica para la continuidad operativa al tratarse de un servidor de respaldo de algún sistema, su localización y manuales de operación.

2.6. Perfiles de puestos con funciones de planificar la continuidad

Criterio N°6: ISO/IEC 22301:2019 Seguridad y resiliencia, continuidad del negocio, sistemas de gestión, requisitos: “Este documento especifica la estructura y los requisitos para implementar y mantener un sistema de gestión de la continuidad del negocio (BCMS) eficaz.”.

Del análisis realizado al Manual descriptivo de los puestos de Jefe del Departamento GAC, Profesional Nivel 2 de Comunicaciones TI, Profesional Nivel 2 Seguridad de la Informática, Jefe Departamento de Operación de la Red se determina que las actividades ahí descritas permiten garantizar la continuidad de los centros de datos y los sistemas alojados en ellos, no obstante, se ha identificado la ineficiente ejecución de las siguientes actividades:

a. La gestión, comunicación y repartición de actividades para renovar o actualizar el marco normativo de TI para demostrar esfuerzos por cumplir con las expectativas del MICITT.
b. Las actividades de formalizar la gestión de inventarios y detallar la información para el control de los activos para establecer y mantener el alineamiento de éstos respecto a BCMS.
c. Planificar la continuidad mediante un enfoque colaborativo con otros departamentos, incluyendo el análisis de riesgos y la capacitación del personal para enfrentar diversas amenazas.

No contar con personal que ocupe los puestos de Profesional Nivel 2 Seguridad Informática, que se encuentra vacante desde abril 2024 y el Profesional Nivel 2 Comunicaciones, vacante desde noviembre 2024 y el Asistente Técnico Nivel 1, que está vacante desde hace 8 años, afecta las actividades diarias de la gestión de tecnologías y el cumplimiento al marco normativo PATI.PR1.NR5 Marco normativo de la política de seguridad de la información, el cual no se ha actualizado desde Julio del 2021.

Ante la condición expuesta, JASEC se expone a la disminución de la eficiencia en la operativa del Departamento GAC para garantizan la continuidad de los centros de datos y los sistemas alojados en ellos, el aumento de costos ante la falta de personal y la necesidad de resolver problemas de manera reactiva pueden generar costos adicionales, así como incidentes y la incapacidad para responder de manera efectiva que pueden dañar la imagen de la organización contribuyendo a la falta de resiliencia organizacional.

CONCLUSIONES

Una vez efectuada la auditoría se evidencian oportunidades de mejora para corregir una serie de debilidades de control significativas que inciden sobre los mecanismos de control de alta disponibilidad y recuperación de desastres en los Centros de Procesamiento de Datos de JASEC, de acuerdo con la normativa técnica y legal aplicable, concluyéndose de manera específica en lo siguiente:

a. Existe un rezago significativo respecto al cumplimiento del marco normativo de la política de seguridad de la información, a nivel de gobierno y gestión, pues no se evidencian esfuerzos sustanciales en curso para la implementación y cumplimiento del marco requerido por el MICITT, por lo que los mecanismos de control de alta disponibilidad de los sistemas del Centro de Datos no se ajustan a las normativas técnicas posibles de aplicar en la actualidad.

b. Se deben desarrollar o completar los inventarios de equipo de cómputo de los centros de datos y prepararlos para su uso en la planificación de la continuidad de operaciones , también se deben mejorar las condiciones físicas y ambientales que garanticen la seguridad de estos centros y la continuidad de la operativa de los negocios, asimismo y ante la ausencia de recuro humano en la estructura de GAC para puestos clave, se ha identificado la desactualización de normativa que define y regula controles esenciales para la recuperación de posibles desastres que pueden afectar los servicios actuales de JASEC, los cuales se resguardan en los equipos de cómputo en los Centros de Datos.

RECOMENDACIONES

De conformidad con las competencias asignadas en el artículo 22 y el artículo 12 inciso c), ambos de la Ley General de Control Interno, se emiten las siguientes recomendaciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello; una vez que transcurra el plazo establecido en el artículo 36 y 37, en caso de que proceda, el artículo 38 de ese mismo cuerpo normativo; por lo que su incumplimiento no justificado constituye causal de responsabilidad (artículo 39 de la LGCI).

Esta Auditoría Interna se reserva la verificación, por los medios que considere pertinentes, la efectiva implementación de las recomendaciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales recomendaciones.

A LA PERSONA QUE OCUPA EL PUESTO DE JEFE DE INFOCOMUNICACIONES, O EN SU CASO AL DIRECTOR COMERCIAL

4.1. Oficializar y coordinar para verificar que se incluya en los inventarios, la información de los sistemas de cómputo que se custodian en el Centro de procesamiento de Datos de Infocomunicaciones, la cual debe contener, al menos lo siguiente: **(Véase criterio No.2)**

a. Etiqueta de activos, marca, modelo y serie
b. Nivel de criticidad y prioridad
c. Sistemas o software integrados al equipo (si aplica, en caso de servidores propios de Jasec)
d. Localización del activo (ubicación física)
e. Dirección IP en la red
f. Información de dueño y usuario experto o a cargo
g. Información de mantenimiento por fechas de soportes próximos
h. Información de empresa soporte (datos de contacto de empresa contratada)

Plazo de implementación: Mayo, 2025

Nivel de criticidad: MEDIO

4.2. Documentar la información necesaria para notificar, atender y prevenir incidentes que pueden representar riesgo para los sistemas y equipos de cómputo del Centro de procesamiento de Datos de Infocomunicaciones, conteniendo al menos: **(Véase criterio No.5)**

a. Información específica que permita localizar el activo
b. Localización, dirección IP y detalles de respaldos o BackUps (si existen, RPO)
c. Equipo de electrógenos correspondiente
d. Resultado del análisis de riesgo y análisis de criticidad
e. Registros de eventos e históricos de incidentes
f. Localización de manuales, configuraciones y demás documentación que permita reactivar el sistema.
g. Ciclo de vida del activo, valoración y análisis de obsolescencia (para planificación oportuna de cambios)
h. Información de dueño y usuarios expertos especificando comunicación
i. Datos de contacto de empresa de soporte contratada y nombre encargado directo
j. (Deseable) Registros de promedio de la duración de las actividades de mantenimiento y soporte (RTO)

Plazo de implementación: Mayo, 2025

Nivel de criticidad: MEDIO

A LA PERSONA QUE OCUPA EL PUESTO DE JEFE DEL DEPARTAMENTO DE GESTION DE LA ARQUITECTURA Y COMUNICACIONES (GAC)

4.3. Priorizar, coordinar e implementar para que se desarrolle el Marco normativo de la política de seguridad de la información alineado al Marco Normativo de Gobierno y Gestión de TI del MICITT, considerando para ello, los resultados de nivel de gestión y el estado de definición del proceso documental que se expone en el **Anexo N°1** de este informe. **(Véase criterio No.1, No.4)**

Plazo de implementación: Junio, 2025

Nivel de criticidad: ALTO

4.4. Desarrollar e implementar un plan de continuidad de la plataforma tecnológica (BCP) para los servicios de TI (BCMS), que contemple, al menos, la definición de tiempos de recuperación (RTO), puntos de recuperación (RPO), reporte de incidentes, planificando pruebas periódicas y planes de comunicación, anticipando su posible uso en capacitaciones, alinearlo a la estructura actual de JASEC. **(Véase criterio No.1, No.2, No.4 y No.5)**

Plazo de implementación: Noviembre, 2025

Nivel de criticidad: ALTO

4.5. Actualizar, implementar y divulgar la información de los inventarios de los sistemas de cómputo que se custodian en el centro de datos en el Edificio Central, indicando al menos, lo siguiente: **(Véase criterio No.2)**

a. Etiqueta de activos, marca, modelo y serie
b. Nivel de criticidad y prioridad
c. Sistemas o software integrados al equipo (si aplica, en caso de servidores propios de Jasec)
d. Localización del activo (ubicación física)
e. Dirección IP en la red
f. Información de dueño y usuario experto o a cargo
g. Información de mantenimiento por fechas de soportes próximos
h. Información de empresa soporte (datos de contacto de empresa contratada)

Plazo de implementación: Junio, 2025

Nivel de criticidad: MEDIO

4.6. Documentar, gestionar y divulgar la información necesaria para notificar, atender y prevenir incidentes que pueden representar riesgo para los sistemas y equipos de cómputo del Centro de Procesamiento de Datos del Edificio Central, conteniendo al menos, lo siguiente: **(Véase criterio No.5)**

a. Información específica que permita localizar el activo
b. Localización, dirección IP y detalles de respaldos o BackUps (si existen, RPO)
c. Equipos de electrógenos correspondientes
d. Resultados del análisis de riesgo y análisis de criticidad
e. Registros de eventos e históricos de incidentes y los Logs
f. Información de manuales, configuraciones y demás documentación que permita reactivar el sistema.
g. Ciclo de vida del activo, valoración y análisis de obsolescencia (para planificación oportuna de cambios)
h. Información de dueño y usuarios expertos especificando contacto y teléfono personal (con motivo de contactar al personal con disponibilidad cuando éste se requiera para atender emergencias).
i. Datos de contacto de empresa de soporte contratada y encargado directo
j. (Deseable) Registrar el promedio de la duración de las actividades de mantenimiento y soporte (RTO)
k. Documentar con detalle todo incidente ocurrido, cuando éstos han causado alguna afectación.
l. Mantener un registro de reportes del dispositivo como Logs, alertas e incidentes.
m. Las labores de mantenimiento según lo planificado para los activos, aun cuando éstos tienen planificado su reemplazo a corto plazo, si por alguna razón el reemplazo del activo se atrasa, se debe retomar el soporte y mantenimiento con normalidad, para garantizar la efectividad durante todo el proceso operativo

Plazo de implementación: Noviembre, 2025

Nivel de criticidad: MEDIO

4.7. Documentar, oficializar e implementar el proceso para la administración eficiente de inventarios de los activos de TI a nivel general de JASEC, definiendo para ello plazos y responsables para la implementación de buenas prácticas de seguridad e inventariado (COBIT 2019), considerando al menos, lo siguiente: **(Véase criterio No.1, No.2 y No.4)**

a. Recomendar la precaución de no exponer información confidencial como usuarios y contraseñas de equipo de la red en los inventarios.
b. Implementar gestores de contraseñas con autenticación de múltiple factor para gestionar los activos y otros accesos.
c. Integrar información de contactos de soporte, cronogramas de mantenimiento, planes de sustitución y renovación, garantías, entre otras especificaciones propias de los activos.
d. Documentar todo el proceso de configuración del firewall y demás equipos que fueron necesarios para poder implementar en el Plan de Continuidad de las Operaciones de TI.

Plazo de implementación: Mayo, 2025

Nivel de criticidad: MEDIO

4.8. Implementar, en coordinación con la dependencia pertinente, la ejecución de lo siguiente: **(Véase criterio No.3)**

a. Se instalen luces de emergencia en la posición más adecuada dentro de recinto de equipo de cómputo.
b. Se instaure señalización de seguridad y precaución en los equipos delicados o de riesgo de electrocución.
c. Se instaure señalación de salida de emergencia en los pasillos, que concuerde con el resto del edificio.
d. Se planifique la instalación de sistemas de seguridad tipo RFID y se implementen alarmas de apertura en las puertas de acceso al recinto con tarjetas HID.

Plazo de implementación: Junio, 2025

Nivel de criticidad: MEDIO

4.9. Implementar y emitir las gestiones con el Departamento de Talento Humano para el reclutamiento y selección de personal, paralelamente, se deberá diseñar e implementar un plan de capacitación integral dirigido al funcionariado de esa unidad, con el fin de habilitarlos para instruir al personal por ingresar de GAC y TIC. **(Véase criterio No.6)**

Plazo de implementación: Julio, 2025

Nivel de criticidad: ALTO

A LA PERSONA QUE OCUPA EL PUESTO DE JEFE DEL DEPARTAMENTO DE OPERACIÓN DE LA RED

4.10. Emitir, divulgar e implementar las gestiones necesarias para asegurar el adecuado acceso al Centro de Procesamiento de Datos del Bosque, así como su seguridad perimetral, considerando al menos, lo siguiente: **(Véase criterio No.3)**

a. Que el sistema RFID de acceso al edificio registre quien entra y sale, comprobar el registro HID.
b. Verificación de puntos ciegos a las cámaras de seguridad y coordinar mantenimiento de luminarias.
c. Mantenimiento y pruebas a los sensores de alarmas, activación de alerta de incendios, entre otros.

Plazo de implementación: Junio, 2025

Nivel de criticidad: MEDIO

4.11. Implementar, coordinar y divulgar, lo que corresponda, para inventariar todos los sistemas de cómputo que se custodian en el centro de datos localizado en el Bosque, cuyo levantamiento y registro debe contener al menos, lo siguiente: **(Véase criterio No.2)**

a. Etiqueta de activo, marca, modelo y serie
b. Nivel de criticidad y prioridad
c. Sistemas o software integrados al equipo (si aplica en caso de servidores pertenecientes a Jasec)
d. Localización del activo (ubicación física)

e. Dirección IP en la red
f. Información de dueño y usuario experto o a cargo
g. Información de mantenimiento por fechas de soportes próximos
h. Información de empresa soporte (datos de contacto de empresa contratada)

Plazo de implementación: Junio, 2025

Nivel de criticidad: MEDIO

4.12. Implementar, documentar y divulgar la información necesaria para notificar, atender y prevenir incidentes que pueden representar riesgo para los sistemas de cómputo y equipos del Centro de Procesamiento de Datos del Bosque, conteniendo al menos, lo siguiente: **(Véase criterio No.5)**

a. Información específica que permita localizar el activo
b. Localización, dirección IP y detalles de respaldos o BackUps (si existen, RPO)
c. Equipo de electrógenos correspondiente
d. Resultado del análisis de riesgo y análisis de criticidad
e. Registros de eventos e históricos de incidentes
f. Localización de manuales, configuraciones y demás documentación que permita reactivar el sistema.
g. Ciclo de vida del activo, valoración y análisis de obsolescencia (para planificación oportuna de cambios)
h. Información de dueño y usuarios expertos especificando comunicación
i. Datos de contacto de empresa de soporte contratada y nombre encargado directo
j. (Deseable) Registros de promedio de la duración de las actividades de mantenimiento y soporte (RTO)

Plazo de implementación: Agosto, 2025

Nivel de criticidad: MEDIO

4.13. Implementar una bitácora de ingreso al recinto del centro de computadores para que se lleve registro de las operaciones y personal de mantenimiento que ingresa a los sistemas en custodia, donde se indique al menos la siguiente información: **(Véase criterio No.3)**

a. Numero de caso (o código para registro)
b. Personal que aprueba o autoriza
c. Nombre de personas que ingresan
d. Fecha de ingreso
e. Hora de entrada
f. Hora de salida
g. Motivo de Ingreso y observaciones
h. Ingreso o salida de equipo

Plazo de implementación: Mayo, 2025

Nivel de criticidad: ALTO

WILLY ARNOLDO LEIVA LOPEZ (FIRMA)

Firmado digitalmente por WILLY ARNOLDO LEIVA LOPEZ (FIRMA)
Fecha: 2025.04.09 11:18:38 -06'00'

Elaborado por:
Willy Leiva Lopez
Profesional de Auditoría

AUDITORIA INTERNA
Marzo, 2025

APÉNDICE N°1.

Valoración de las observaciones realizadas al informe N° ATO-029-2024

RESULTADO, CONCLUSIÓN O RECOMENDACIÓN DE AI	OBSERVACIÓN DE LA ADMINISTRACIÓN	¿SE ACOGE? (SI, NO, PARCIAL)	JUSTIFICACIÓN AI
4.1. Oficializar y coordinar para verificar que se incluya en los inventarios, la información de los sistemas de cómputo que se custodian en el Centro de procesamiento de Datos de Infocomunicaciones, la cual debe contener, al menos lo siguiente: a. Etiqueta de activos, marca, modelo y serie b. Nivel de criticidad y prioridad c. Sistemas o software integrados al equipo (si aplica, en caso de servidores propios de Jasec) d. Localización del activo (ubicación física) e. Dirección IP en la red f. Información de dueño y usuario experto o a cargo g. Información de mantenimiento por fechas de soportes próximos h. Información de empresa soporte (datos de contacto de empresa contratada) **Fecha de Implementación: Abril, 2025**	En la conferencia final el Director Comercial solicita que la auditoría debe especificar el manejo de información sensible y cómo ésta debe tratarse respecto a los inventarios con activos privados. Se solicita ampliar el plazo de la recomendación a mayo 2025, debido a que se está en proceso de reclutamiento y selección del puesto de Jefe de Operación de la Red de Fibra Óptica, y se espera contar con dicho recurso para atender lo recomendado.	SI	Esta Auditoría tomará los lineamientos descritos en la normativa PATI.PR1.NR2- PATI.PR1.NR5 de JASEC, disponible en el SE-Suite, sin embargo, se aclara que no está dentro de la jurisdicción del auditor indicar el cómo se debe manipular la información. Considerando que el recurso está en proceso de reclutamiento, esta Unidad aprueba ampliar el plazo a Mayo, 2025.
4.2. Documentar la información necesaria para notificar, atender y prevenir incidentes que pueden representar riesgo para los sistemas y equipos de cómputo del Centro de procesamiento de Datos de Infocomunicaciones, conteniendo al menos: a. Información específica que permita localizar el activo b. Localización, dirección IP y detalles de respaldos o BackUps (si existen, RPO) c. Equipo de electrógenos correspondiente d. Resultado del análisis de riesgo y análisis de criticidad e. Registros de eventos e históricos de incidentes f. Localización de manuales, configuraciones y demás documentación que permita reactivar el sistema. g. Ciclo de vida del activo, valoración y análisis de obsolescencia (para planificación oportuna de cambios) h. Información de dueño y usuarios expertos especificando comunicación i. Datos de contacto de empresa de soporte contratada y nombre encargado directo j. (Deseable) Registros de promedio de la duración de las actividades de mantenimiento y soporte (RTO). **Fecha de Implementación: Mayo, 2025**	En la conferencia final el Director Comercial solicita ampliar el plazo de la recomendación a mayo 2025, debido a que se está en proceso de reclutamiento y selección del puesto de Jefe de Operación de la Red de Fibra Óptica, y se espera contar con dicho recurso para atender lo recomendado.	Si	Considerando que el recurso está en proceso de reclutamiento, esta Unidad aprueba ampliar el plazo a Mayo, 2025.
4.3. Priorizar, coordinar e implementar para que se desarrolle el Marco normativo de la política de seguridad de la información alineado al Marco Normativo de Gobierno y Gestión de TI del MICITT, considerando para ello, los resultados de nivel de gestión y el estado de definición del proceso documental que se expone en el Anexo N°1 de este informe.**Fecha de Implementación: Junio, 2025**	Mediante oficio SUBG-TIC-GAC-097-2025, el Jefe del Dpto. GAC señala lo siguiente: Mediante la solicitud realizada por esta auditoria la cual consiste en desarrollar el Marco normativo de la política de seguridad de la información alineado al Marco Normativo de Gobierno y Gestión de TI del MICITT, considerando para ello, los resultados de nivel de gestión y el estado de definición del proceso documental con un plazo a Junio de 2025, he de indicarle que en dicho plazo no vamos a poder satisfacer este requerimiento, dado el volumen de trabajo que tenemos y el poco personal con que se cuenta. Para dar una respuesta satisfactoria seria incluso tal vez necesario realizar una contratación que nos acompañe con la creación de dicho marco normativo, lo que nos llevaría a tener que solicitar recursos e incluirlos en el presupuesto del departamento, aunado al proceso de solicitud de recursos, estudios de mercado y proceso de contratación administrativa el plazo real para la entrega de este producto podría extenderse a junio del 2026 fecha que solicitamos se extienda el plazo sugerido por ustedes.	No	Es importante mencionar que dentro del servicio de autoría ATO-019-2024, en la recomendación 3.4 se indica lo siguiente: Implementación de las Normas para la gestión y el control de las TIC MICITT a nivel corporativo, el cual tiene fecha de implementación a Mayo 2025 y la recomendación 3.8 en dónde se recomienda emitir, divulgar e implementar un plan con responsables y actividades, para actualizar la documentación del proceso PATI, cuenta con una fecha de implementación a Marzo 2025. Es por lo que esta Auditoría no puede validar la ampliación de plazo a Junio 2026, siendo que hay recomendaciones que atienden parte de lo solicitado.

4.4. Desarrollar e implementar un plan de continuidad de la plataforma tecnológica (BCP) para los servicios de TI (BCMS), que contemple, al menos, la definición de tiempos de recuperación (RTO), puntos de recuperación (RPO), reporte de incidentes, planificando pruebas periódicas y planes de comunicación, anticipando su posible uso en capacitaciones, alinearlo a la estructura actual de JASEC. **Fecha de Implementación: Mayo, 2025**	Mediante oficio SUBG-TIC-GAC-097-2025, el Jefe del Dpto. GAC indica que mediante la solicitud realizada por esta auditoria la cual consiste en desarrollar e implementar un plan de continuidad de la plataforma tecnológica (BCP) para los servicios de TI (BCMS), que contemple, al menos, la definición de tiempos de recuperación (RTO), puntos de recuperación (RPO), reporte de incidentes, planificando pruebas periódicas y planes de comunicación, anticipando su posible uso en capacitaciones, alinearlo a la estructura actual de JASEC, con plazo de entrega para mayo 2025, le informo que este departamento en conjunto con la jefatura de Área de TI hemos estado implementando desde inicio de año una serie de soluciones como respaldo en la nube, hiperconvergencia, almacenamiento y sitio alterno las cuales vienen a brindarnos esa plataforma que se nos solicita, pero será hasta que los mismos estén implementados y en funcionamiento que se definirán los tiempos solicitados. Para este punto solicitamos extender el plazo indicado a noviembre de 2025 para contar con el tiempo suficiente para contar con una plataforma definida y estable.	Si	Es importante mencionar que dentro del servicio de autoría ATO-019-2024, se incorporaron recomendaciones N° 3.4, 3.6 y 3.8 que atienden parte de lo recomendado, con una fecha de implementación a junio 2025, sin embargo, al considerar el levantamiento de los inventarios que se requieren, esta Auditoría Interna, considera oportuno ampliar el plazo a Noviembre del 2025.
4.5. Actualizar, implementar y divulgar la información de los inventarios de los sistemas de cómputo que se custodian en el centro de datos en el Edificio Central, indicando al menos, lo siguiente: a. Etiqueta de activos, marca, modelo y serie b. Nivel de criticidad y prioridad c. Sistemas o software integrados al equipo (si aplica, en caso de servidores propios de Jasec) d. Localización del activo (ubicación física) e. Dirección IP en la red f. Información de dueño y usuario experto o a cargo g. Información de mantenimiento por fechas de soportes próximos h. Información de empresa soporte (datos de contacto de empresa contratada) **Fecha de Implementación: Abril, 2025**	Mediante oficio SUBG-TIC-GAC-097-2025, el Jefe del Dpto. GAC indica que mediante la solicitud realizada por esta auditoria la cual consiste en actualizar, implementar y divulgar la información de los inventarios de los sistemas que se custodian en el centro de datos en el Edificio Central con fecha de entrega para abril 2025, le indico que dado el poco personal con que se cuenta actualmente, la saturación de trabajo que tenemos y la implementación de varios proyectos no nos es posible cumplir con dicha fecha, solicitamos se pueda extender para junio del 2025 para poder satisfacer su requerimiento.	Si	En el servicio de autoría ATO-019-2024, se incorporaron recomendaciones 3.3, y 3.4 en dónde se recomienda la realización de inventarios, con una fecha de implementación a mayo 2025, sin embargo, al considerar el levantamiento de los inventarios, esta Auditoria considera oportuno ampliar el plazo a Junio del 2025.
4.6. Documentar, gestionar y divulgar la información necesaria para notificar, atender y prevenir incidentes que pueden representar riesgo para los sistemas y equipos de cómputo del Centro de Procesamiento de Datos del Edificio Central, conteniendo al menos, lo siguiente: a. Información específica que permita localizar el activo b. Localización, dirección IP y detalles de respaldos o BackUps (si existen, RPO)c. Equipos de electrógenos correspondientesd. Resultados del análisis de riesgo y análisis de criticidade. Registros de eventos e históricos de incidentes y los Logsf. Información de manuales, configuraciones y demás documentación que permita reactivar el sistema.g. Ciclo de vida del activo, valoración y análisis de obsolescencia (para planificación oportuna de cambios)h. Información de dueño y usuarios expertos especificando contacto y teléfono personal (con motivo de contactar al personal con disponibilidad cuando éste se requiera para atender emergencias).i. Datos de contacto de empresa de soporte contratada y encargado directoj. (Deseable) Registrar el promedio de la duración de las actividades de mantenimiento y soporte (RTO)k. Documentar con detalle todo incidente ocurrido, cuando éstos han causado alguna afectación.l. Mantener un registro de reportes del dispositivo como Logs, alertas e incidentes.m. Las labores de mantenimiento según lo planificado para los activos, aun cuando éstos tienen planificado su reemplazo a corto plazo, si por alguna razón el reemplazo del activo se atrasa, se debe retomar el soporte y mantenimiento con normalidad, para garantizar la efectividad durante todo el proceso operativo.**Fecha de Implementación: Mayo, 2025**	Mediante oficio SUBG-TIC-GAC-097-2025, el Jefe del Dpto. GAC indica que mediante la solicitud realizada por esta auditoria la cual consiste en documentar, gestionar y divulgar la información necesaria para notificar, atender y prevenir incidentes que pueden representar riesgo para los sistemas y equipos del Centro de Procesamiento de Datos del Edificio Central, con fecha de entrega a mayo 2025 le solicito ampliar dicho plazo para noviembre de 2025 dado que no contamos con el recursos humano con el suficiente tiempo para realizar esta documentación y procedimiento, se solicita plazo a noviembre de 2025 para poder brindar lo solicitado.	Si	En el servicio de autoría ATO-019-2024, se incorporaron recomendaciones 3.3, 3.4 y 3.6 en dónde se recomienda la realización de inventarios y divulgar planeación, con una fecha de implementación a mayo 2025 sin embargo al considerar el levantamiento de los inventarios y otros requerimientos como los análisis de riesgo, esta Auditoria considera oportuno ampliar el plazo a Noviembre del 2025.
4.7. Documentar, oficializar e implementar el proceso para la administración eficiente de inventarios de los activos de TI a nivel general de JASEC, definiendo para ello plazos y responsables para la implementación de buenas prácticas de seguridad e inventariado (COBIT 2019), considerando al menos, lo siguiente: a. Recomendar la precaución de no exponer información confidencial como usuarios y contraseñas de equipo de la red en los inventarios. b. Implementar gestores de contraseñas con autenticación de múltiple factor para gestionar los activos y otros accesos.c. Integrar información de contactos de soporte, cronogramas de mantenimiento, planes de sustitución y renovación, garantías, entre otras especificaciones propias de los activos.d. Documentar todo el proceso de configuración del firewall y demás equipos que fueron necesarios para poder implementar en el Plan de	Mediante oficio SUBG-TIC-GAC-097-2025, el Jefe del Dpto. GAC indica que mediante la solicitud realizada por esta auditoria la cual consiste en documentar, oficializar e implementar el proceso para la administración eficiente de inventarios de los activos de TI a nivel general de JASEC, definiendo para ello plazos y responsables para la implementación de buenas prácticas de seguridad e inventariado (COBIT 2019), con fecha de mayo 2025, le solicito ampliar dicho plazo para noviembre de 2025 dado que no contamos con el recursos humano con el suficiente tiempo para realizar esta documentación y procedimiento, se solicita plazo a noviembre de 2025 para poder brindar lo solicitado.	No	En el servicio de autoría ATO-019-2024, se incorporaron recomendaciones 3.2, en dónde se pide definir estrategias de Seguridad y Ciberseguridad, con una fecha de implementación a marzo 2025, y 3.4 en dónde se recomienda la realización de inventarios, planes de capacitación y planeación, con una fecha de implementación a mayo 2025 sin embargo al considerar el levantamiento de los inventarios, riesgos, clasificación de la información, entre otros, esta Auditoria considera oportuno ampliar el plazo a Noviembre del 2025.

Continuidad de las Operaciones de TI. **Fecha de Implementación: Mayo, 2025**			
4.8. Implementar, en coordinación con la dependencia pertinente, la ejecución de lo siguiente: a. Se instalen luces de emergencia en la posición más adecuada dentro de recinto de equipo de cómputo. b. Se instaure señalización de seguridad y precaución en los equipos delicados o de riesgo de electrocución. c. Se instaure señalación de salida de emergencia en los pasillos, que concuerde con el resto del edificio. d. Se planifique la instalación de sistemas de seguridad tipo RFID y se implementen alarmas de apertura en las puertas de acceso al recinto con tarjetas HID. **Fecha Implementación: Junio, 2025**	Mediante oficio SUBG-TIC-GAC-097-2025, el Jefe del Dpto. GAC indica que mediante la solicitud realizada por esta auditoria la cual consiste en implementar, en coordinación con la dependencia pertinente, la ejecución de instalar luces de emergencia en la posición más adecuada dentro de recinto de equipo de cómputo, se instaure señalización de seguridad y precaución en los equipos delicados o de riesgo de electrocución, se instaure señalación de salida de emergencia en los pasillos, que concuerde con el resto del edificio, se planifique la instalación de sistemas de seguridad tipo RFID y se implementen alarmas de apertura en las puertas de acceso al recinto con tarjetas HID, para dar una respuesta satisfactoria habría que realizar un estudio de mercado para la valoración de soluciones, luego de localizadas las posibles soluciones se debe solicitar los recursos para adquirirlas, lo que nos llevaría a tener que solicitar recursos e incluirlos en el presupuesto del departamento, aunado al proceso de solicitud de recursos, estudios de mercado y proceso de contratación administrativa el plazo real para la entrega de este producto podría extenderse a junio del 2026 fecha que solicitamos se extienda el plazo sugerido por ustedes.	No	Es de conocimiento de esta Auditoría Interna, que las gestiones para obtener recursos y contratar lo requerido requiere de colaboración y aprobación de otros departamentos para llevarse a cabo, sin embargo, el alcance de la recomendación se fundamenta en confeccionar un plan aprobado por la Gerencia General para implementar en el tiempo cada uno de los puntos descritos.
4.9. Implementar y emitir las gestiones con el Departamento de Talento Humano para el reclutamiento y selección de personal, paralelamente, se deberá diseñar e implementar un plan de capacitación integral dirigido al funcionariado de esa unidad, con el fin de habilitarlos para instruir al personal por ingresar de GAC y TIC. **Fecha Implementación: Julio, 2025**	Mediante oficio SUBG-TIC-GAC-097-2025, el Jefe del Dpto. GAC indica que mediante la solicitud realizada por esta auditoría la cual consiste en implementar y emitir las gestiones con el Departamento de Talento Humano para el reclutamiento y selección de personal, paralelamente, se deberá diseñar e implementar un plan de capacitación integral dirigido al funcionariado de esa unidad, con el fin de habilitarlos para instruir al personal por ingresar de GAC y TIC con fecha de julio 2025, para el cumplimiento de este punto debemos reunirnos con los compañeros de Talento Humano y llegar a un consenso con respecto a este tema, para lo cual la fecha de Julio 2025 no es factible dada la carga de trabajo que tenemos y el poco personal con que se cuenta, solicitamos ampliarla para noviembre de 2025.	No	En el servicio de auditoría ATO-019-2024, se incorporaron recomendaciones 3.4, 3.7 y 3.10 en las cuales requieren el realizar programas de capacitación, analizar los riesgos que limitan la contratación de personal y la realización de manuales de funciones, con fecha de implementación a marzo y mayo 2025, sin embargo, el alcance de la recomendación se fundamenta en confeccionar un plan consensado con el Dpto. de TH para atender lo requerido.

Fuente: F-EJE-081 Análisis de las observaciones de la Administración

AUDITORIA INTERNA
ABRIL, 2025