# INFORME DE AUDITORÍA INTERNA BASADA EN RIESGOS
## NIVEL CENTRAL
### OFICINA DE CONTROL INTERNO

| | | |
|---|---|---|
| **ÁREA AUDITADA**<br><br>Subgerencia de Protección Animal – Dirección Técnica de Inocuidad de Insumos Veterinarios | | |
| **UNIDAD AUDITABLE**<br>Procedimiento PRA-SPA-P-017 V.2 “Registro de Alimentos para Animales”, enfocando la evaluación en la línea de disponibilidad del Modelo de Seguridad y Privacidad de la Información (MSPI) | | |
| **TIPO DE AUDITORÍA:**<br>**Auditoría Interna _X___ Auditoría de Cumplimiento ___ Auditoría de seguimiento ____**<br>**Auditorías específicas: ____ Auditorías de sistemas o de TIC: ____¿Cuál? _____** | | |
| **LUGAR DE DESARROLLO DE LA AUDITORÍA**<br><br>**Oficinas Nacionales _X___ Gerencia Seccional ____ Oficina Local ____ PAPF ____ Otro ____ ¿Cuál?_____** | | |
| **FORMA DE DESARROLLO DE LA AUDITORÍA: Presencial ____ Remota ____ Mixta ___X_** | | |
| **VIGENCIA:** 2025 | | |
| **FECHA DE INICIO**:<br>09/11/2025 | **FECHA DE FINALIZACIÓN:**<br>09/12/2025 | |
| **TIPO DE INFORME:** | Preliminar ____ Definitivo __X___ | Fecha: 16/01/2026 |

## 1. OBJETIVO

Desarrollar la auditoría al procedimiento PRA-SPA-P-017 V.2 “Registro de Alimentos para Animales”, enfocando la evaluación en la línea de disponibilidad del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a lo dispuesto en el Anexo 1 de la Resolución 500 de 2021 y la Resolución 2277 de 2025 del MinTIC, que actualiza su marco normativo con base en la norma ISO/IEC 27001:2022.

El propósito de la auditoría es verificar la efectividad de los controles institucionales que garantizan la disponibilidad y continuidad del servicio tecnológico, asegurando que la plataforma SimplifICA 1.0 – Alimentos para Animales y los sistemas asociados al procedimiento se mantengan operativos, resilientes y trazables frente a incidentes, interrupciones o fallas de infraestructura.

Asimismo, se busca evaluar si la gestión de disponibilidad implementada por la Oficina de Tecnologías de la Información (OTI) y la Subdirección de Protección Animal cumple con los principios del MSPI y del Sistema de Gestión de Seguridad de la Información (SGSI) institucional, garantizando la existencia de mecanismos de monitoreo, respaldo, recuperación, redundancia y trazabilidad de eventos que permitan reconstruir y analizar la operatividad del sistema ante incidentes o afectaciones.

## 2. ALCANCE

La auditoría interna se desarrolló sobre el procedimiento PRA-SPA-P-017 V.2 “Registro de Alimentos para Animales”, focalizando la evaluación en el componente tecnológico que lo soporta, esto es, la plataforma SimplifICA 1.0 – Alimentos para Animales, en tanto herramienta utilizada para el registro y control de los trámites asociados. En consecuencia, el alcance comprendió la verificación de la línea de disponibilidad del MSPI aplicada al servicio tecnológico y, de manera complementaria, la revisión de los elementos de trazabilidad necesarios para reconstruir y analizar eventos que pudieran afectar la operación del sistema y el cumplimiento del procedimiento.

La unidad auditable correspondió a la Subgerencia de Protección Animal, en tanto responsable del procedimiento PRA-SPA-P-017 V.2 “Registro de Alimentos para Animales”. Para el cumplimiento del objetivo, el trabajo de auditoría comprendió la verificación de controles asociados a la disponibilidad (y la trazabilidad asociada) del MSPI/SGSI sobre la plataforma

SimplifICA 1.0 – Alimentos para Animales y su operación. En ese contexto, se revisaron evidencias y registros técnicos administrados por la Oficina de Tecnologías de la Información (OTI), en su calidad de área institucional que coordina y soporta la implementación/operación de prácticas y controles de seguridad de la información, incluyendo actividades orientadas a asegurar disponibilidad, respaldos y continuidad del servicio."



En términos de periodo evaluado (vigencia), el alcance cubrió la revisión de documentos y evidencias correspondientes al periodo 2024–2025, asociados al aseguramiento de disponibilidad del sistema (por ejemplo: respaldos, restauración/recuperación, monitoreo, registros de incidentes de indisponibilidad y registros técnicos de operación). En cuanto al periodo de ejecución de la auditoría, se desarrolló conforme al cronograma institucional definido para esta actividad (10 de noviembre a 9 de diciembre de 2025, según lo indicado en el anuncio/planeación de la auditoría).

Para el entendimiento del flujo y la operación del procedimiento en la plataforma (como insumo para evaluar disponibilidad y trazabilidad), se realizó una **sesión de trabajo** orientada a observar el recorrido funcional del trámite en el sistema. En dicha sesión se revisó el flujo de **registro de producto**, precisando dependencias funcionales previas (por ejemplo, la necesidad de contar con empresa registrada para adelantar el registro del producto), y se observó la interacción del usuario en el sistema durante el diligenciamiento y avance del trámite.

Adicionalmente, el alcance incluyó la validación del componente de trazabilidad operativa y de auditoría del sistema, considerando la existencia de mecanismos de registro de eventos/acciones (por ejemplo, bitácoras o logs funcionales del sistema) que permitieran identificar actividades realizadas (creación, envío, aceptación/rechazo y cambios de estado), así como su disponibilidad para consulta durante el ejercicio auditor. Lo anterior fue abordado expresamente en la sesión, la cual se estructuró en dos partes: una orientada al flujo del procedimiento y otra orientada a la trazabilidad/auditabilidad.

En cuanto a componentes y temas cubiertos dentro del marco de disponibilidad del MSPI, el alcance comprendió la revisión (con base en la evidencia disponible y allegada por las áreas) de aspectos como: monitoreo y disponibilidad del servicio, gestión de respaldos y recuperación, gestión de incidentes asociados a indisponibilidad, gestión de cambios con impacto potencial en continuidad, y gestión de registros/logs que soportaran la trazabilidad requerida para el análisis de afectaciones del servicio. Este enfoque se enmarcó en el procedimiento institucional de auditoría interna basada en riesgos, que contempla como unidades auditables, entre otras, procedimientos y sistemas de información

## 3. LIMITACIONES AL ALCANCE

Durante el desarrollo de la auditoría se presentaron limitaciones asociadas, principalmente, a la **completitud**, **periodicidad** y **trazabilidad** de la evidencia remitida para sustentar la línea de **disponibilidad** (y su trazabilidad asociada) del MSPI sobre el sistema SimplifICA 1.0 – Alimentos para Animales. En concordancia con el procedimiento institucional para el desarrollo de auditorías internas, cuando la información solicitada no se contó con soportes suficientes para su verificación, ello se consideró una limitación al alcance del trabajo de auditoría, en los términos previstos por el procedimiento CIG-OCI-P-002.

Las limitaciones de completitud, periodicidad y trazabilidad de la evidencia remitida se presentaron principalmente sobre información técnica bajo administración de la OTI; en consecuencia, dichas limitaciones afectaron la capacidad de la auditoría para emitir conclusiones integrales sobre la efectividad de los controles de disponibilidad y trazabilidad que soportaron la ejecución del procedimiento PRA-SPA-P-017 V.2 por parte de la Subgerencia de Protección Animal.

En lo referente a **evidencias de respaldo**, la OTI consolidó un documento descriptivo en el que señaló la existencia de "estadios" de respaldo y relacionó como evidencias archivos de programación y ejecución a nivel de sistema operativo (por ejemplo, cron.log) y reportes de trabajos (exportjobsreport) asociados a respaldos en Azure. No obstante, dentro del mismo

documento se indicó expresamente que los “logs de ejecución van en crudo” y que debían revisarse ejecuciones de ejecución a través de scripts (.sh) para corroborar la operación; en la evidencia recibida para este componente, dicha corroboración **no quedó sustentada** con artefactos completos o trazables (p.ej., scripts, bitácoras consolidadas de resultado por tarea, reportes de éxito/fallo por periodo), lo cual limitó la capacidad de verificar con suficiencia y de forma integral la ejecución y resultados de los respaldos frente al período solicitado 2024–2025.



Adicionalmente, respecto de la **verificación de respaldos y pruebas de restauración**, en el documento remisorio se describió que se realizaba verificación de los archivos dump comprobando “tamaño, contenido e integridad”; sin embargo, la evidencia suministrada para este punto **no se soportó** con actas, reportes formales de restauración (parcial o total) o resultados documentados que permitieran constatar, con criterios de auditoría, el éxito de pruebas de recuperación en las vigencias 2024–2025. Esta situación limitó el aseguramiento sobre la **efectividad** de la recuperación, más allá de la existencia de rutinas de respaldo.

En relación con el **procedimiento de recuperación ante desastres,** se recibió un documento denominado **“Estrategia DRP – ICA Preliminar”**; sin embargo, para el componente de **pruebas de DRP**, el documento remisorio listó el ítem, sin que quedara soportado con planes, cronogramas, reportes de ejecución y resultados de pruebas correspondientes a 2024–2025 (o, en su defecto, una constancia explícita de inexistencia). Lo anterior constituyó una limitación para concluir sobre la **capacidad probada** de recuperación frente a escenarios de indisponibilidad mayor.

Para el componente de **monitoreo, disponibilidad y desempeño del servicio)**, el documento remisorio enumeró los subnumerales 3.1 a 3.3 (manual/procedimiento de monitoreo; reportes de disponibilidad; bitácoras de alertas y monitoreo) sin que, dentro de la evidencia documental recibida para este bloque, se aportaran reportes formales y periódicos de disponibilidad (con porcentajes, tiempos de caída, causas y acciones) ni bitácoras consolidadas de alertamiento para el periodo solicitado, lo que limitó la evaluación de la operación de los controles de monitoreo como mecanismo preventivo y de detección (base para la disponibilidad).

En cuanto a la **trazabilidad y logs** el documento remisorio indicó que, para la base de datos de producción, los logs fueron “personalizados” por incidentes de espacio, “resguarda hasta 7 archivos” y “se rota cuando pesan 200M”, y que para la aplicación se mantenían configuraciones estándar. Esta condición de retención/rotación reportada limitó la disponibilidad histórica de registros para reconstrucción de eventos en horizontes amplios (como el periodo 2024–2025) cuando no se aportaron repositorios centralizados, exportaciones periódicas o mecanismos de conservación que permitieran asegurar trazabilidad completa para auditoría.

Finalmente, aunque se anexaron **extractos de logs** para evidenciar eventos (por ejemplo, syslogfe.log.txt con errores del 16 de octubre, incluyendo referencia a web_error.log-20251016, y mysqlerror.log con eventos fechados en 2025), la evidencia recibida para el periodo de análisis se concentró en **muestras puntuales** con fechas explícitas de 2025, sin que se contara con un repositorio o extracción integral que permitiera asegurar cobertura continua del periodo 2024–2025 solicitado en el requerimiento. Esto limitó la capacidad de realizar trazabilidad completa de incidentes y su correlación con respaldos/recuperaciones y con eventos de disponibilidad a lo largo del periodo total auditado.

## 4. CRITERIOS

Para el desarrollo de la auditoría, los criterios de evaluación se fundamentaron en el marco normativo y de buenas prácticas aplicable al Modelo de Seguridad y Privacidad de la Información (MSPI), así como en los lineamientos institucionales vigentes del ICA relacionados con la disponibilidad y la trazabilidad asociada (continuidad, respaldos, monitoreo, gestión de incidentes, gestión de cambios y gestión de registros). Estos criterios fueron utilizados para comparar la evidencia obtenida durante la auditoría frente a los requisitos definidos para el aseguramiento de la disponibilidad del sistema SimplifICA 1.0 – Alimentos para Animales y sus componentes tecnológicos asociados.

En el marco externo, se consideraron como criterio las disposiciones relacionadas con el MSPI adoptado como habilitador de la Política de Gobierno Digital, conforme al Anexo 1 de la Resolución 500 de 2021 y su actualización mediante la Resolución 2277 de 2025 del MinTIC, en concordancia con las buenas prácticas de la familia ISO/IEC 27000, particularmente la ISO/IEC 27001:2022 (referencia base del enfoque de controles del SGSI/MSPI). *Nota de trazabilidad documental:* en este numeral se citó el marco externo como criterio conforme al objeto y alcance aprobado; los apartes específicos de dichas resoluciones se desarrollaron a nivel de contraste con los instrumentos institucionales que las operacionalizan (SGSI/MSPI), en especial el Plan institucional y las Políticas internas.

En el marco interno del ICA, se aplicaron como criterios, principalmente:

- El Plan de Seguridad y Privacidad de la Información institucional (versión vigente aportada), el cual estableció lineamientos para la gestión de seguridad y privacidad, incorporó el enfoque de gestión del riesgo de seguridad y definió el marco de referencia aplicable, incluyendo NTC/ISO 27001:2022, GTC/ISO 27002:2022, NTC/ISO 27005:2022, NTC-ISO 31000:2011, y la referencia al Modelo de Seguridad y Privacidad de la Información (MSPI) y Política de Gobierno Digital como parte de los estándares/lineamientos aplicables.

- El Manual del Sistema de Gestión de Seguridad de la Información (SGSI) institucional, como documento marco del sistema de gestión, el cual definió el SGSI del ICA y su alineación con la familia ISO 27000 y el MSPI, constituyéndose en criterio para verificar la existencia y aplicabilidad de instrumentos institucionales del SGSI/MSPI frente a servicios y activos de información.

- El Manual de Políticas de Seguridad y Privacidad de la Información (ICA) (GIT-PTI-POL-001), como criterio normativo interno para la línea auditada, en especial: (i) Política de Copias de Respaldo, que estableció la realización de respaldos conforme a criticidad, así como la validación de resultados, el registro en bitácora y la realización de pruebas de restauración con periodicidad definida (trimestral), como elementos mínimos de control y evidencia;

(ii) lineamientos de continuidad / recuperación, que incluyeron la obligación de contar con DRP por servicio de alto impacto y la ejecución de pruebas periódicas con documentación (plan, periodicidad, resultados, lecciones aprendidas y acciones derivadas);

(iii) lineamientos de redundancia/alta disponibilidad para servicios de alto impacto, incluyendo la existencia de esquemas como redundancia, clustering y alta disponibilidad (como prácticas esperadas cuando aplique por criticidad);

(iv) lineamientos de registro, seguimiento y auditoría (logs), que establecieron la necesidad de que los registros de auditoría/eventos se generaran, se mantuvieran disponibles, y se protegieran contra alteraciones y accesos no autorizados, como criterio central para la trazabilidad verificable.

- El Procedimiento de Gestión de Incidentes de Seguridad de la Información (GIT-SOP-P-002), como criterio para la trazabilidad de incidentes que afectaran o pudieran afectar la disponibilidad; este procedimiento definió la seguridad de la información incluyendo expresamente disponibilidad y trazabilidad y estableció que, en la herramienta de Mesa de Servicio, debía documentarse toda la trazabilidad del incidente por los responsables, y que el registro/trazabilidad debía quedar en dicho aplicativo como repositorio para seguimiento y para auditorías/investigaciones.
- El Procedimiento de Gestión de Cambios (GIT-SOP-P-004), como criterio para validar la existencia de trazabilidad de cambios y su control respecto a la continuidad/estabilidad del servicio; dicho procedimiento definió como objetivo minimizar impactos negativos ante cambios y dispuso que los cambios aprobados debían quedar soportados mediante acta del comité para mantener la trazabilidad de lo aprobado y ejecutado.
- La Guía para la Administración de Riesgos de Seguridad Digital, como criterio para la identificación y tratamiento de riesgos asociados a seguridad digital, incluyendo explícitamente riesgos como la pérdida de disponibilidad de servicios digitales, y para

orientar la evaluación de controles en el componente de gestión del riesgo asociado a disponibilidad.
- Cuando aplicó por corresponder a servicios soportados en nube/proveedor, se tomó como criterio complementario el Contrato de Nivel de Servicio (SLA) para Servicios Online de Microsoft (documento aportado), particularmente las definiciones asociadas al porcentaje de disponibilidad/tiempo de actividad y su medición, como referencia para contrastar compromisos del proveedor frente a la disponibilidad del servicio.



Finalmente, como criterio de procedimiento del ejercicio auditor (planeación, obtención de evidencia y determinación de limitaciones), se aplicó el procedimiento institucional CIG-OCI-P-002 “Desarrollo de Auditoría Interna Basada en Riesgos”, el cual definió la auditoría como un proceso para evaluar el cumplimiento de criterios, y estableció que la revisión documental debía efectuarse según criterios, alcance y normatividad aplicable, así como el tratamiento de la limitación al alcance cuando la información solicitada no permitió verificación suficiente.

## 5. DESARROLLO DE LA AUDITORÍA

### 5.1 METODOLOGÍA

La auditoría se desarrolló como auditoría interna basada en riesgos, atendiendo el procedimiento institucional CIG-OCI-P-002 “Desarrollo de auditoría interna basada en riesgos”, el cual define la auditoría como un proceso sistemático, independiente y documentado orientado a obtener evidencia objetiva y evaluarla de forma imparcial frente a criterios establecidos. Asimismo, el procedimiento institucional enmarca el desarrollo del trabajo bajo el esquema de Planificación – Ejecución – Informe de auditoría.

Durante la ejecución se efectuó revisión documental y verificación de evidencias asociadas al procedimiento PRA-SPA-P-017 y a la operación del servicio SimplifICA. La obtención de evidencia incluyó información provista por la Subgerencia de Protección Animal y por la OTI, como área de apoyo responsable de custodiar y administrar registros técnicos relevantes para la disponibilidad y la trazabilidad (p. ej., respaldos, monitoreo, logs y continuidad).”

En coherencia con lo anterior, la metodología aplicada se orientó a verificar la existencia y efectividad de los controles relacionados con la disponibilidad (y su trazabilidad asociada), a partir de evidencia documental y técnica, y mediante la aplicación de técnicas de auditoría que permitieran sustentar las conclusiones del informe preliminar.

Identificación de la información: Para la obtención de evidencia se partió de la información requerida formalmente a la OTI y de los soportes remitidos para el periodo 2024–2025, específicamente en lo relacionado con respaldos, recuperación ante desastres, monitoreo/disponibilidad, trazabilidad y logs, y gestión de incidentes/cambios/SLA del sistema SimplifICA. En este componente, se revisó el documento remisorio de evidencias aportado por la OTI, en el cual se relacionaron archivos y fuentes de verificación, incluyendo referencias a cron.log y otros archivos de registro.

De igual forma, en el mismo documento se consignaron parámetros de operación relevantes para trazabilidad (por ejemplo, la indicación de que para base de datos los logs fueron “personalizados”, con retención/rotación limitada), los cuales se tomaron como insumo para orientar la verificación de trazabilidad y disponibilidad histórica de registros.

Adicionalmente, conforme al procedimiento institucional, se programaron y desarrollaron reuniones de trabajo cuando fue necesario para esclarecer inquietudes del proceso y precisar aspectos operativos, dejando el soporte correspondiente (listas de asistencia, cuando aplicó).

**Análisis y evaluación:** El análisis se realizó mediante la comparación estructurada entre: (i) los criterios de auditoría definidos en el plan (marco MSPI/SGSI y buenas prácticas ISO/IEC 27001), y (ii) la evidencia disponible remitida por las áreas y la obtenida durante las sesiones de entendimiento del procedimiento en el aplicativo. La evaluación consideró, para cada componente

revisado, atributos de evidencia relevantes para auditoría (pertinencia, consistencia, completitud, periodicidad y trazabilidad), y se focalizó en determinar si los controles se encontraban definidos y, especialmente, si su operación se encontraba demostrada y verificable dentro del periodo solicitado.

En línea con el procedimiento CIG-OCI-P-002, dentro de la ejecución se efectuó revisión documental según criterios, alcance y normatividad aplicable, y se soportó el análisis mediante la preparación de papeles de trabajo que evidenciaran la aplicación de técnicas de auditoría.



Cuando la evidencia remitida no permitió corroborar de manera suficiente el cumplimiento del criterio (por ausencia, incompletitud, falta de periodicidad o trazabilidad), dicha situación se trató metodológicamente como un elemento que incidía en la capacidad de verificación, en concordancia con el procedimiento institucional, el cual prevé la declaración de limitación al alcance ante ausencia de remisión de información en los tiempos o condiciones establecidas.

**Documentación de la información:** Los resultados de la verificación se documentaron en papeles de trabajo debidamente identificados y organizados, con trazabilidad a los numerales requeridos y a los soportes allegados (documentos, listados, registros, extractos y demás evidencias técnicas suministradas). Esta documentación se orientó a dejar evidencia suficiente sobre: qué se solicitó, qué se recibió, qué se verificó, contra qué criterio se evaluó y cuál fue la conclusión alcanzada para cada punto revisado, en consonancia con la exigencia institucional de que los papeles de trabajo evidencien el desarrollo de la auditoría y las técnicas utilizadas.

**Supervisión del trabajo:** La supervisión se atendió bajo el esquema institucional del procedimiento CIG-OCI-P-002, el cual contempla la revisión del informe preliminar y de los soportes de trabajo como parte del control de calidad previo a su comunicación formal, y la trazabilidad de los productos del ejercicio (incluido el informe preliminar en el formato aplicable).

### 5.2 MUESTRA

De conformidad con el procedimiento institucional CIG-OCI-P-002, durante la ejecución de la auditoría se analizó la documentación solicitada con el fin de determinar la muestra, cuando ello aplicó, atendiendo el enfoque de auditoría interna basada en riesgos y la disponibilidad/pertinencia de los soportes remitidos por la unidad auditable y la OTI.

En ese contexto, la muestra se definió como un censo de la evidencia documental efectivamente remitida por la Oficina de Tecnologías de la Información (OTI) para sustentar los componentes del requerimiento asociados a disponibilidad y trazabilidad del sistema SimplifICA 1.0 – Alimentos para Animales. Lo anterior, en razón a que el universo de soportes entregado para el período requerido (2024–2025) se concretó en un conjunto acotado de archivos, descripciones y extractos, por lo cual se revisó la totalidad de dichos insumos (sin que esto equivalga a revisar la totalidad de eventos operativos ocurridos en las vigencias 2024–2025, sino la totalidad de los soportes aportados para su verificación).

La muestra comprendió dos componentes complementarios:

**(i) Validación funcional del procedimiento en SimplifICA:** se desarrolló una sesión de trabajo orientada a comprender el flujo operativo del procedimiento PRA-SPA-P-017 V.2 en el aplicativo, con demostración del registro en el sistema y revisión del comportamiento funcional desde el punto de vista del usuario/proceso. En la transcripción de la sesión se evidenció que la validación se apoyó en la explicación paso a paso del registro y en un ambiente de pruebas para ilustrar el flujo y resolver dudas operativas.

**(ii) Revisión documental y técnica de la evidencia de controles (disponibilidad y trazabilidad):** se revisó el documento remisorio de evidencias preparado por la OTI, en el cual se describieron los mecanismos declarados para respaldos y se listaron artefactos asociados. Allí, por ejemplo, se describieron “estadios” de respaldo, frecuencias y retenciones, así como la referencia a evidencias técnicas tipo cron.log y reportes de trabajos exportjobsreport asociados a respaldos en Azure.

De manera específica, la evidencia técnica revisada dentro de la muestra incluyó, entre otros, los siguientes elementos (en la forma y alcance en que fueron entregados por la OTI):

- **Registros de programación/ejecución de tareas en sistema operativo** (cron): se revisaron extractos en los que se observó la ejecución programada de tareas relacionadas con rotación (logrotate) y ejecución de scripts de respaldo (por ejemplo, ejecución de /var/mariadb/backup.sh sobre el host referenciado), como parte del soporte a rutinas de respaldo.
- **Registros de auditoría** (audit): se revisaron extractos de auditoría del sistema asociados a sesiones ejecutadas bajo **terminal=cron**, como parte de la trazabilidad técnica remitida.
- **Logs de sistema/aplicación** (trazabilidad de eventos): se revisaron extractos con eventos/errores reportados para el servidor, evidenciándose, entre otros, referencias a eventos del 16 de octubre (syslog) y mensajes asociados a errores de aplicación.
- **Logs de base de datos**: se revisaron extractos con registros de error, observándose eventos fechados en 2025 (por ejemplo, julio y diciembre), tal como fue aportado por la OTI para soportar el numeral de logs de base de datos.

Adicionalmente, dentro de la muestra documental se consideró el contenido del mismo documento remisorio respecto a gestión de logs, en el cual se indicó que, para la base de datos de producción, los logs habían sido “personalizados” por incidentes de espacio, con retención limitada a hasta 7 archivos y rotación por tamaño (200M), así como la referencia a que para el servidor de aplicación se mantenían configuraciones estándar.

Para el componente de respaldos, el documento remisorio también dejó explícito que los “logs de ejecución van en crudo” y que se debía buscar la ejecución de scripts “.sh” para corroborar, aspecto que se tuvo en cuenta al definir el alcance verificable con la evidencia efectivamente aportada dentro del universo revisado.
Finalmente, se incluyeron en la muestra los documentos remitidos por la OTI para soportar elementos de continuidad/SLA, en particular: (a) el documento denominado **“Estrategia DRP – ICA”**, recibido como soporte del componente de recuperación ante desastres, cuyo objetivo general se orientó a presentar una estrategia de recuperación ante interrupción de servicios tecnológicos; y (b) el **SLA de Microsoft para servicios en línea** (diciembre de 2025), recibido como referente contractual de niveles de servicio para servicios online.

## 5.3 FORTALEZAS

Durante el desarrollo de la auditoría se evidenció que la Entidad contaba con un marco institucional documentado para la gestión de la seguridad y privacidad de la información, articulado con la Política de Gobierno Digital y el SGSI, el cual incorpora de forma expresa los componentes asociados a disponibilidad y continuidad del servicio. En particular, se revisó el Plan de Seguridad y Privacidad de la Información (versión 1.2), el cual se encontraba actualizado a junio de 2024 y aprobado por el Comité Institucional de Gestión y Desempeño (sesión ordinaria del 02 de julio de 2024), como instrumento vigente de planeación para el SGSI/MSPI institucional.

Así mismo, se constató que el alcance del SGSI declarado en dicho plan comprendía los procesos misionales, de apoyo, estratégicos y de evaluación que integran el mapa de procesos institucional, lo que resultó relevante para el objeto de auditoría, en tanto el procedimiento PRA-SPA-P-017 V.2 “Registro de Alimentos para Animales” y su soporte tecnológico (SimplifICA 1.0 – Alimentos para Animales) se enmarcaban dentro de un esquema institucional que definía la operación, verificación y mejora del SGSI.

Como fortaleza adicional, se identificó que el ICA disponía de políticas institucionales formalizadas que establecían lineamientos concretos sobre controles directamente relacionados con la línea de disponibilidad y trazabilidad, particularmente en materia de copias de respaldo y registro/seguimiento de eventos. En el Manual de Políticas de Seguridad de la Información se establecieron directrices tales como: la obligación de definir un procedimiento para actividades de backup considerando criticidad y necesidades de disponibilidad; la validación del resultado de ejecución de las copias y el registro de novedades en bitácora; la realización de pruebas de

restauración trimestrales; y la necesidad de que cada copia quedara registrada (logs en servidor o archivo externo) para estar disponible a controles o auditoría.

De igual forma, el mismo documento incorporó el deber de generar y mantener registros de auditoría sobre actividades de usuarios, excepciones y eventos de seguridad, y proteger dichos registros contra alteración o acceso no autorizado, lo cual constituyó un elemento de referencia positivo para la trazabilidad exigida en el marco del MSPI.



En el componente procedimental, se verificó la existencia de un procedimiento formal de gestión de incidentes de seguridad de la información, el cual definió canales institucionales de reporte (incluida la herramienta de Mesa de Servicio) y estableció expresamente que en dicha herramienta debía documentarse “toda la trazabilidad” del evento o incidente, indicando además que el registro y trazabilidad se realizaba allí como único lugar de almacenamiento, con el fin de soportar seguimiento, investigaciones o auditorías.

Esta formalización se consideró consistente con la necesidad de trazabilidad en la línea evaluada (disponibilidad y su trazabilidad asociada).

De manera complementaria, se constató que la Entidad contaba con un procedimiento de gestión de cambios para la formalización, aprobación y ejecución de cambios en la infraestructura y sistemas de información, incluyendo el uso de la Mesa de Ayuda como mecanismo de documentación y trazabilidad del cambio (por ejemplo, registro del cambio no aprobado y cierre del ticket), lo cual se alineaba con la necesidad de mantener control operacional sobre modificaciones que puedan impactar la disponibilidad.

En cuanto a la disponibilidad técnica y trazabilidad operacional del sistema SimplifICA, se recibió un documento de la OTI que describió la existencia de “estadios” de respaldo (incluyendo respaldos diarios y respaldos en Azure con parámetros de retención/rotación) y relacionó artefactos de soporte tales como archivos de programación de tareas (cron.log) y reportes de trabajos exportados, además de señalar la existencia de archivos de auditoría (audit logs) y logs de sistema/aplicación para consulta.

Si bien en otros apartados del informe estos insumos se analizaron frente a completitud y cobertura temporal, su existencia aportó evidencia de que se generaban registros técnicos y que la OTI contaba con capacidad de extracción y suministro de trazas para propósitos de verificación. Finalmente, se evidenció articulación operativa para el entendimiento del sistema y del procedimiento auditado, en la medida en que se desarrolló una sesión de trabajo en la cual personal de la OTI explicó el flujo del registro de productos en el ambiente de pruebas de SimplifICA, precisando condiciones previas del registro y la estructura modular del formulario utilizado, y dejando constancia de que la sesión se grabó para mantener registro.

Esto contribuyó a consolidar entendimiento del soporte tecnológico del procedimiento y a orientar la revisión de controles asociados a la disponibilidad y trazabilidad.

## 5.4 RESULTADOS

Durante el desarrollo de la auditoría se analizó la evidencia documental y técnica remitida por la Oficina de Tecnologías de la Información (OTI) para sustentar la línea de disponibilidad (y la trazabilidad asociada) del MSPI sobre el sistema SimplifICA 1.0 – Alimentos para Animales, en el periodo 2024–2025. Con base en la comparación entre los criterios de auditoría (MSPI/SGSI institucional e ISO/IEC 27001:2022) y la evidencia recibida, se estructuraron las siguientes observaciones y sus recomendaciones asociadas.

**Observación 1. Deficiencia en el seguimiento de los instrumentos del MSPI en la línea de disponibilidad (SimplifICA 1.0)**

**Condición (situación evidenciada):** En la revisión se identificó que, si bien la OTI describió la existencia de controles operativos asociados a disponibilidad (respaldos, verificación básica y referencias a monitoreo), la evidencia aportada no permitió demostrar de manera suficiente,

periódica y trazable la operación y efectividad de dichos controles durante el periodo 2024–2025. En particular, se indicó que los "logs de ejecución" se encontraban "en crudo" y que debía corroborarse la ejecución revisando "scripts (.sh)", lo que, en el paquete documental revisado, no quedó respaldado con artefactos completos y consolidados de resultados por periodo.

**Criterio (referente evaluado):** El Manual de Políticas de Seguridad de la Información del ICA establece, entre otros, que el respaldo debe estar debidamente documentado, que el administrador de backup debe validar resultados y registrarlos, y que se deben realizar pruebas de restauración de manera trimestral; adicionalmente, exige mantener registros disponibles para controles o auditoría.



**Efecto (impacto/riesgo):** La condición descrita afectó el nivel de aseguramiento sobre la capacidad institucional de **prevenir, detectar y recuperar** oportunamente el servicio ante interrupciones, y limitó la trazabilidad necesaria para reconstruir eventos y soportar la auditoría de disponibilidad del sistema en el horizonte 2024–2025.

**Recomendación:** La Oficina de Tecnologías de la Información (OTI) debe asegurar la operación verificable, periódica y trazable de los controles de disponibilidad aplicables a SimplifICA 1.0 – Alimentos para Animales, mediante la consolidación y conservación de evidencia documentada que permita demostrar en auditoría: (i) la validación y registro de resultados de las copias de seguridad por parte del rol responsable (Administrador de backup) y el registro de novedades en bitácora; (ii) la realización y documentación de pruebas de restauración de manera trimestral conforme a los lineamientos institucionales; y (iii) el registro de cada copia de seguridad en logs del servidor o en un archivo externo que mantenga los soportes disponibles para controles o auditoría, garantizando su disponibilidad durante el periodo evaluado**.**

**Observación 2. Deficiencia en la trazabilidad: generación, conservación y disponibilidad de registros (logs) para reconstrucción de eventos**

**Condición (situación evidenciada):** Se evidenciaron debilidades en la trazabilidad debido a limitaciones en la conservación histórica y disponibilidad de logs. En el documento remisorio se indicó que, para base de datos, los logs fueron "personalizados" por incidentes de espacio, con retención de "hasta 7 archivos" y rotación al alcanzar "200M", situación que restringe la disponibilidad histórica para análisis y correlación de eventos en periodos amplios.

Adicionalmente, se aportaron extractos puntuales de logs del sistema operativo y de base de datos (p. ej., syslog y mysqlerror) que evidenciaron eventos/errores específicos, sin que ello constituyera una reposición integral y continua del histórico 2024–2025 solicitado.

**Criterio (referente evaluado):** La política institucional establece la obligación de generar y mantener registros de auditoría sobre actividades, excepciones y eventos de seguridad para soportar investigaciones y monitoreo; y dispone que las evidencias recolectadas deben contar con un lugar de almacenamiento de registros y monitoreo.

**Efecto (impacto/riesgo):** La limitación de retención/centralización y la ausencia de evidencia integral para el periodo solicitado afectaron la capacidad de la entidad para asegurar una **trazabilidad verificable** de eventos que impactan disponibilidad y para soportar ejercicios de auditoría, análisis operativo o forense sobre SimplifICA.

**Recomendación**: Se recomienda que la Oficina de Tecnologías de la Información (OTI) formalice, documente e implemente (para el alcance de SimplifICA 1.0 – Alimentos para Animales) un mecanismo de gestión de registros (logs) y trazabilidad que permita reconstruir eventos asociados a indisponibilidad, fallas, reinicios, errores, consultas de información sensible y cambios relevantes, y que asegure su conservación y disponibilidad para auditoría. Dicho mecanismo deberá evidenciar, como mínimo: (i) fuentes de registro consideradas (aplicación, base de datos, sistema operativo y/o componentes de infraestructura que soportan el servicio), (ii) responsables de generación, custodia y consulta, (iii) tiempos de retención definidos con base en la criticidad del servicio y las necesidades de investigación/auditoría, (iv) controles de integridad y acceso sobre los registros (protección contra alteración y accesos no autorizados),

(v) un repositorio o ubicación institucional (centralizada o equivalente) para el almacenamiento y monitoreo de los eventos, y (vi) evidencia periódica que permita demostrar la operación continua del control durante la vigencia evaluada (registros consolidados o extractos representativos con cobertura suficiente).

Lo anterior se fundamenta en que la política institucional establece la obligación de generar y mantener registros de auditoría sobre actividades, excepciones y eventos de seguridad, así como de **proteger** los registros **contra alteración y acceso no autorizado**, y de contar con un lugar de almacenamiento de registros y monitoreo para soportar auditorías e investigaciones; por lo cual la trazabilidad debe ser verificable y disponible cuando se requiera.



**Observación 3: Fortalecimiento de documentación y evidencia de copias de seguridad (backups)**
**Condición:** La OTI describió un esquema de respaldos con tres “estadios”, que incluyó respaldos programados y respaldos asociados a servicios en nube (Azure), con frecuencias diarias y horarias, y retenciones descritas (por ejemplo, 29 días para algunos respaldos y rotaciones referidas a 30 días). No obstante, en la misma evidencia se indicó que los “logs de ejecución” estaban “en crudo” y que debía corroborarse ejecución revisando scripts (.sh); en el paquete revisado no se aportaron scripts ni bitácoras consolidadas de resultados (éxito/fallo) por tarea y por periodo, que permitieran verificar integralmente el cumplimiento 2024–2025, más allá de la existencia de programaciones o reportes aislados.

**Criterio:** La política institucional exige que el procedimiento de backup esté documentado considerando criticidad y necesidades de disponibilidad; que se validen resultados y se registren novedades en bitácora; que se realicen pruebas de restauración trimestrales; y que cada copia quede registrada en logs o en un archivo externo disponible para auditoría.

**Causa (asociada a la evidencia):** La evidencia remitida privilegió descripciones y archivos técnicos sin consolidación operativa por periodo y sin soportes formales de verificación/restauración que acreditaran el control como evidencias auditables.

**Efecto:** Se limitó la verificación de la **efectividad** de los respaldos (no solo su existencia), y la capacidad de asegurar recuperación conforme a criticidad del servicio para el periodo auditado.

**Recomendación:** Se recomendó que la OTI y los responsables del sistema aseguraran que la ejecución de respaldos de SimplifICA y sus componentes asociados contara con evidencia consolidada, verificable y periódica (resultados por tarea/periodo y verificación documentada), manteniéndola disponible para seguimiento y auditoría conforme a la política institucional.

**Observación 4. Fortalecimiento de continuidad: planes y pruebas DRP con evidencias completas**
**Condición:** Para el requerimiento de recuperación ante desastres se recibió un documento denominado “Estrategia DRP – ICA Preliminar”, el cual se presentó como un informe de carácter estratégico (no ingeniería de detalle) y evidenció señales de documento en consolidación (p. ej., referencias/índices con errores). Adicionalmente, en la evidencia revisada no se identificaron soportes completos de pruebas de DRP 2024–2025 (planes, cronogramas, reportes de ejecución y resultados), pese a estar considerado como ítem solicitado dentro del bloque de continuidad.

**Criterio:** La política institucional establece que la OTI debe elaborar DRP para cada sistema/servicio de alto impacto, y debe asegurar pruebas periódicas con documentación completa (incluyendo cronogramas, resultados y evidencias).

**Causa (asociada a la evidencia):** La evidencia aportada correspondió a un insumo preliminar/estratégico, sin soportes de validación mediante pruebas ni documentación que permitiera verificar la capacidad probada de recuperación.

**Efecto:** No fue posible asegurar, con evidencia suficiente, la **capacidad probada de recuperación** ante escenarios de indisponibilidad mayor, limitando la evaluación de continuidad en el componente auditado.

**Recomendación:** Se recomendó que la OTI y los responsables del servicio aseguraran la existencia y disponibilidad de documentación completa y verificable sobre continuidad y recuperación aplicable a SimplifICA, incluyendo la evidencia de **pruebas ejecutadas** y sus resultados, de acuerdo con los lineamientos institucionales.



**Observación 5. Formalización y evidencia del monitoreo de disponibilidad y desempeño**
**Condición:** En el documento remisorio la OTI relacionó los componentes del bloque de monitoreo (manual/procedimiento, reportes de disponibilidad y bitácoras de alertas). Sin embargo, dentro del paquete documental revisado para el alcance 2024–2025 no se evidenciaron reportes formales y periódicos de disponibilidad (porcentajes, tiempos de caída, causas y acciones) ni bitácoras consolidadas de alertamiento para SimplifICA, lo que limitó la verificación del monitoreo como control preventivo/detectivo para asegurar disponibilidad.

**Criterio:** La política institucional exige mantener evidencias que soporten auditoría y monitoreo de eventos, y la gestión de incidentes contempla la necesidad de atender eventos/incidentología asociada, incluyendo afectación a disponibilidad, mediante el proceso definido y su trazabilidad.

**Efecto:** La ausencia de evidencia periódica de monitoreo impidió concluir sobre la operación sostenida del control de disponibilidad en 2024–2025, afectando la capacidad de demostrar supervisión continua del servicio.

**Recomendación:** Se recomendó que la OTI asegurara la generación y conservación de evidencia periódica del monitoreo de SimplifICA (indicadores y reportes verificables), de modo que el desempeño y la disponibilidad del servicio pudieran demostrarse y reconstruirse en auditoría.

**Observación 6. Robustecimiento de gestión de logs: retención, integridad y disponibilidad para auditoría**
**Condición:** Se indicó que, para la base de datos de producción, los logs fueron ajustados por incidentes de espacio, conservando “hasta 7 archivos” y rotando por tamaño (200M). Así mismo, se aportaron muestras de logs del sistema operativo y de base de datos que reflejaron eventos puntuales (por ejemplo, errores asociados a logrotate/compresión en syslog y registros de conexiones abortadas en mysqlerror), sin que existiera evidencia de conservación integral que cubriera de forma continua el periodo 2024–2025.

**Criterio:** La política institucional exige generar y mantener registros de auditoría sobre actividades, excepciones y eventos, y proteger dichos registros contra alteración o acceso no autorizado, asegurando almacenamiento para monitoreo y auditoría.

**Efecto:** Se afectó la capacidad de reconstrucción de eventos (trazabilidad) y la correlación de incidentes de disponibilidad con otras evidencias (respaldos, cambios, recuperaciones), especialmente en un horizonte de revisión 2024–2025.
Evidencias de monitoreo, dispon…

**Recomendación 4:** Se recomendó que la OTI asegurara que los registros (logs) relevantes para disponibilidad de SimplifICA contaran con condiciones verificables de **retención, conservación e integridad**, manteniéndolos disponibles para auditoría conforme a los lineamientos institucionales.

**Observación 7. Articulación operativa OTI – área misional (roles, incidentes y acuerdos de nivel de servicio)**

**Condición:** La evidencia remitida refirió que la gestión de incidentes se soportaba en mesa de ayuda y se adjuntaron registros/relaciones de incidentes; igualmente se señaló la existencia de

un SLA asociado a servicios (Azure) y se aportó un documento de SLA de servicios en línea de Microsoft (diciembre de 2025) que incluye conceptos de porcentaje de tiempo de actividad y créditos de servicio bajo ciertos umbrales. No obstante, en el conjunto revisado no se evidenciaron informes de cumplimiento del SLA específicos para SimplifICA en 2024–2025 ni mecanismos consolidados que permitieran correlacionar compromisos de disponibilidad, tiempos de respuesta/recuperación y su cumplimiento, con la incidentología del sistema durante la vigencia auditada.



**Criterio:** La gestión de incidentes definida institucionalmente estableció responsabilidades, clasificación y tratamiento de incidentes de seguridad, y contempló la necesidad de gestionar la disponibilidad como parte del aseguramiento de la información y continuidad de la operación.

**Efecto:** La falta de trazabilidad consolidada sobre compromisos de servicio y su cumplimiento limitó la rendición de cuentas y la capacidad de seguimiento sobre disponibilidad del sistema como soporte del procedimiento misional auditado.

**Recomendación:** Se recomendó que la OTI y el área misional aseguraran la existencia de evidencia consolidada que permitiera demostrar la articulación operativa para la disponibilidad de SimplifICA (roles, escalamiento, compromisos de servicio y trazabilidad de incidentes), manteniéndola disponible para seguimiento y auditoría.

**Observación 8. Trazabilidad de la gestión de cambios sobre SimplifICA (registro de cambios 2024–2025)**
**Condición:** La OTI aportó el procedimiento institucional de Gestión de Cambios, el cual incorpora elementos asociados a continuidad del servicio (incluida la determinación de realizar backup y la documentación/cierre de tickets en mesa de ayuda), y se relacionó en la evidencia la intención de remitir una “relación de cambios” para SimplifICA. No obstante, en el paquete documental revisado no se identificó un **registro consolidado de cambios ejecutados** sobre SimplifICA durante 2024–2025 (cambios de versión, ajustes de infraestructura o configuración), lo cual limitó la trazabilidad para correlacionar cambios con eventos de indisponibilidad o afectaciones del servicio.

**Criterio:** El procedimiento de Gestión de Cambios estableció directrices para la formalización, aprobación y ejecución de cambios, y contempló la documentación del cambio en la herramienta de mesa de ayuda, así como controles asociados a respaldo previo cuando aplique.

**Efecto:** La ausencia del registro consolidado afectó la capacidad de reconstruir de forma completa el historial de cambios 2024–2025 y su relación con disponibilidad y continuidad del servicio.

**Recomendación:** Se recomendó que la OTI asegurara la disponibilidad de un registro verificable y consolidado de cambios sobre SimplifICA (2024–2025), de acuerdo con el procedimiento institucional, para soportar trazabilidad, seguimiento y auditoría de disponibilidad del servicio.

## 6. RIESGOS DE LA UNIDAD AUDITABLE:

### 6.1 RIESGOS DEL MAPA DE RIESGOS INSTITUCIONAL ACTUAL.

Durante el desarrollo de la auditoría se revisó el insumo de riesgos suministrado por la Oficina de Tecnologías de la Información (OTI), correspondiente al Mapa/Consolidado de Riesgos y Oportunidades del SGSI (componente del Sistema de Gestión Integrado), en coherencia con el enfoque del MSPI y la gestión de riesgos orientada a garantizar disponibilidad y continuidad de los servicios institucionales. En ese marco, se observó que el SGSI reconoce la seguridad de la información como un activo institucional y establece como fin el aseguramiento de la integridad, disponibilidad y confidencialidad, mediante gestión y tratamiento de riesgos para prevenir incidentes y propender por la continuidad del servicio.

Como resultado de la revisión de dicho mapa/consolidado, no se evidenció un riesgo formulado de manera explícita que referenciara directamente el sistema “SimplifICA 1.0 – Alimentos para Animales” o el procedimiento PRA-SPA-P-017 V.2 dentro del enunciado del evento de riesgo. No obstante, sí se identificaron riesgos registrados en el mapa del SGSI que, por su naturaleza, guardaron relación con la disponibilidad/continuidad del servicio tecnológico y con la necesidad de trazabilidad asociada a la operación institucional.

En particular, los riesgos del mapa revisado que se asociaron con la unidad auditable (por involucrar el proceso misional auditado y/o el componente TIC que soporta la operación del servicio) fueron los siguientes:

**Riesgo N.° 34 (Proceso: Gobernabilidad de las TIC’s – Clasificación: Tecnológico):**

En el mapa del SGSI se registró un riesgo relacionado con la no disponibilidad de un Plan de Recuperación ante Desastres (DRP) para los servicios descritos en el catálogo liderado por la OTI, cuya consecuencia declarada correspondió a interrupción de la operación o del servicio. En su valoración, dicho riesgo se ubicó en nivel inherente EXTREMO (evaluación inherente 45, derivada de probabilidad 3 e impacto 15) y nivel residual EXTREMO (exposición residual 45), indicando como condición de control que no se contaba con DRP en el momento de su registro en el mapa. Este riesgo resultó directamente relacionado con el objeto auditado, al corresponder a la dimensión de continuidad/recuperación de servicios tecnológicos requerida para sostener la disponibilidad del servicio misional soportado en plataformas como SimplifICA.

**Riesgo N.° 11 (Proceso: Protección Animal – Subproceso: Gestión de Inocuidad e Insumos Pecuarios – Clasificación: Tecnológico):** El mapa del SGSI incluyó un riesgo asociado a la pérdida de información contenida en un equipo físico de oficina, con consecuencia registrada de pérdida y/o fuga de información. La valoración del riesgo se ubicó en nivel inherente ALTO (evaluación inherente 36; probabilidad 3, impacto 12) y nivel residual MODERADO (exposición residual 9). Como controles existentes se relacionaron acciones de sensibilización y aplicación de lineamientos/políticas institucionales. Si bien el enunciado del evento no refirió de forma específica a SimplifICA, el riesgo se ubicó dentro del proceso misional de Protección Animal y, por tanto, se consideró vinculado al contexto del procedimiento auditado en lo referente a disponibilidad de información soporte y su preservación.

**Riesgo N.° 9 (Proceso: Protección Animal – Subproceso: Gestión de Sanidad Animal – Clasificación: Tecnológico):** En el mapa se registró un riesgo relacionado con fallas de una aplicación utilizada en el proceso misional (asociada a generación de un producto/resultado operativo del proceso), cuya consecuencia declarada correspondió a interrupción de la operación o del servicio, derivada de fallas en la plataforma tecnológica. La valoración se ubicó en nivel inherente ALTO (evaluación inherente 36; probabilidad 3, impacto 12) y nivel residual MODERADO (exposición residual 18). Se listaron controles asociados a soporte y mantenimiento de plataforma e infraestructura. Este riesgo fue considerado pertinente como referencia del tipo de exposición que el propio mapa reconoce en el proceso misional frente a interrupciones de aplicativos; sin embargo, se reitera que el evento descrito en el mapa no citó expresamente a SimplifICA.

**Riesgo N.° 12 (Proceso: Protección Animal – Clasificación: Operativo):** El consolidado incluyó un riesgo relacionado con la modificación de información en base de datos atribuida a desconocimiento del proceso/actividad/procedimiento, con consecuencia declarada de interrupción de la operación o del servicio. Su valoración se ubicó en nivel inherente ALTO (evaluación inherente 24; probabilidad 2, impacto 12) y nivel residual BAJO (exposición residual 6), con controles orientados a revisión de información consolidada y comunicaciones de verificación. Este riesgo se consideró relacionado con el componente de trazabilidad en tanto implica exposición frente a alteraciones de datos y necesidad de reconstrucción/verificación de registros; no obstante, el enunciado del evento tampoco hizo referencia directa a SimplifICA.

En conclusión, el mapa/consolidado revisado sí evidenció riesgos relevantes sobre interrupción del servicio, ausencia de DRP y eventos que afectan información, pero no evidenció una

formulación específica de riesgo para SimplifICA 1.0 – Alimentos para Animales dentro del evento de riesgo registrado, aspecto que quedó documentado para su tratamiento en los apartados siguientes del informe (según corresponda al análisis de riesgos identificados y su alineación con el alcance).

### 6.2 MATERIALIZACIÓN DEL RIESGO.



Durante el desarrollo de la auditoría se revisaron las evidencias remitidas por la Oficina de Tecnologías de la Información (OTI) para establecer si, en el período 2024–2025, se presentaron eventos consistentes con la materialización de riesgos asociados a la disponibilidad (y su trazabilidad asociada) del sistema SimplifICA 1.0 – Alimentos para Animales, en el marco del procedimiento PRA-SPA-P-017 V.2.

Con base en la información allegada, se identificaron registros de incidentes y reportes de usuarios que evidenciaron ocurrencia de afectaciones a la operación (eventos que, por su naturaleza, son consistentes con la materialización del riesgo de indisponibilidad y/o degradación del servicio):

1. **Registro de incidentes (consolidado):** En el archivo **“REGISTRO INCIDENTES SIMPLIFICA.xlsx”** se registraron siete (7) incidentes distribuidos por vigencia así:
   - Vigencia 2024: tres (3) incidentes, con “duración total” registrada de 10:59, 02:05 y 02:20, y causas reportadas asociadas a DNS externo, proveedor de internet y espacio en el disco.
   - Vigencia 2025: cuatro (4) incidentes, con “duración total” registrada de 05:31, 00:56, 05:18 y “1 día 8:30”; en este grupo las causas reportadas se relacionaron principalmente con espacio/almacenamiento (p.ej., “espacio en el servidor”, “espacio”), y un (1) registro no consignó causa.

No obstante, en dicho registro se observaron inconsistencias entre el campo “Vigencia” y los campos “Fecha inicio/Fecha final” (se presentaron años que no correspondían con la vigencia reportada), situación que limitó la trazabilidad temporal para determinar con precisión el momento de ocurrencia de cada evento y su correspondencia con el período 2024–2025 requerido.

2. **Casos/tickets del sistema (mesa de servicio / soporte funcional y técnico):** En el archivo **“Reporte Casos Simplifica.xlsx”** (base remitida por la OTI) se identificaron registros clasificados como INCIDENTE durante el período 2024–2025, dentro de los cuales se encontraron casos cuyo asunto o descripción incluía expresiones asociadas a dificultades de acceso o uso (por ejemplo: “no carga”, “no deja ingresar/entrar”, “timeout/tiempo de espera”, entre otros).
   En términos de trazabilidad, esta base evidenció existencia de reportes de usuarios; sin embargo, no fue posible correlacionar de forma integral dichos reportes con métricas formales de disponibilidad, eventos de monitoreo o análisis de causa raíz, dado que tales evidencias periódicas y consolidadas no fueron aportadas dentro del bloque correspondiente (según lo ya descrito en las limitaciones del alcance).
3. **Muestras de logs (servidor de aplicación y base de datos):** Adicionalmente, se revisaron extractos de logs remitidos como soporte, en los cuales se evidenciaron eventos de error/advertencia en componentes de infraestructura durante 2025. En particular:
   - En el syslog del servidor de aplicación se observaron mensajes asociados a fallas en compresión/rotación de logs y eventos tipo “segfault”, así como errores de recursos (“thread constructor failed: Resource temporarily unavailable”), presentados como extracto/grep.
   - En el log de base de datos se observaron advertencias relacionadas con “Aborted connection … (Got an error reading communication packets)”, también presentadas como extracto.

En ambos casos, los soportes se allegaron en formato de **muestra** (con recortes/“…”), lo que **limitó** la reconstrucción completa de la secuencia de eventos y su correlación con incidentes, respaldos, restauraciones o afectaciones confirmadas de disponibilidad en todo el período 2024–2025.

**Conclusión sobre materialización**
En consecuencia, y **con base en la evidencia disponible**, se concluyó que **sí se evidenciaron** eventos consistentes con la materialización del riesgo asociado a indisponibilidad / afectación de la operación del servicio SimplifICA, particularmente asociados a aspectos de conectividad externa (DNS/proveedor de internet) y de capacidad/espacio (disco/servidor), con tiempos de afectación/atención registrados.

Sin embargo, por las limitaciones ya documentadas (completitud, periodicidad y trazabilidad), la auditoría no contó con evidencia suficiente y consolidada para determinar con precisión, para todo el período 2024–2025, la magnitud de la afectación del servicio ni su correlación integral con indicadores formales de disponibilidad, monitoreo continuo, y trazabilidad completa incidente–evento–recuperación.



## 6.3. RIESGO(S) IDENTIFICADO(S) POR LA OFICINA DE CONTROL INTERNO QUE NO SE ENCUENTRA(N) EN EL MAPA DE RIESGOS INSTITUCIONAL.

Durante el desarrollo de la auditoría, y con base en la evidencia documental recibida para la línea de disponibilidad del MSPI (y su trazabilidad asociada) sobre el sistema SimplifICA 1.0 – Alimentos para Animales, se identificaron exposiciones de riesgo que no fue posible asociar, con trazabilidad verificable, a un registro formal dentro del Mapa de Riesgos Institucional aplicable a la unidad auditable, dado que el insumo solicitado como “matriz o extracto de riesgos… asociados a indisponibilidad, fallas de respaldo o caídas del sistema SimplifICA, con sus respectivos controles definidos” fue referenciado en el consolidado remisorio, pero no se evidenció como parte integral y verificable de los soportes evaluados para el periodo 2024–2025.

En este contexto, la Oficina de Control Interno dejó documentados (para efectos de papeles de trabajo y del análisis del MSPI en la dimensión de disponibilidad) los siguientes riesgos identificados en la unidad auditable:
**Riesgo OCI-01. Indisponibilidad del servicio misional soportado en SimplifICA por debilidades en el monitoreo formal y evidenciable de la operación.**
Se identificó exposición al riesgo de interrupciones del servicio que no sean detectadas oportunamente o que no cuenten con trazabilidad suficiente para su gestión, en razón a que, si bien se relacionaron requerimientos de “manual/procedimiento de monitoreo”, “reportes de disponibilidad” y “bitácoras de alertas y monitoreo”, la evidencia evaluada se concentró en un documento descriptivo que listó los subnumerales, sin aportar reportes formales y periódicos (porcentajes de disponibilidad, tiempos de caída, causas y acciones) ni bitácoras consolidadas de alertamiento que permitieran evidenciar la operación del control durante el periodo solicitado 2024–2025.

**Riesgo OCI-02. Incapacidad de restauración o recuperación efectiva del servicio ante fallas, por insuficiente trazabilidad verificable de la ejecución y verificación de respaldos.**
Se identificó exposición al riesgo de que, ante una indisponibilidad o contingencia, la organización no cuente con evidencia suficiente para demostrar (y, por ende, asegurar) la efectividad de la recuperación a partir de respaldos, debido a que la evidencia recibida describió “estadios” de respaldo con frecuencias, retención y rotación; sin embargo, indicó expresamente que “los logs de ejecución van en crudo” y que debían corroborarse ejecuciones mediante scripts (.sh), sin que esto quedara sustentado con artefactos completos que permitieran verificar resultados de ejecución (éxito/fallo) de forma consolidada para 2024–2025.

Adicionalmente, frente a la verificación de respaldos, se documentó que se verificaban archivos “dump” por tamaño, contenido e integridad, pero no se evidenciaron actas o reportes formales de restauración (parcial o total) con resultados documentados para las vigencias 2024–2025, situación que incrementó la exposición al riesgo de fallas no detectadas en la recuperabilidad real.

**Riesgo OCI-03. Indisponibilidad prolongada ante escenarios de desastre o interrupción mayor, por ausencia de evidencia de pruebas de DRP y por encontrarse la estrategia en condición preliminar/estructural.**

Se identificó exposición al riesgo de afectaciones prolongadas del servicio ante eventos de interrupción mayor, al evidenciarse que, aunque se aportó un documento denominado “Estrategia DRP – ICA” (versión 1) como referencia de recuperación ante desastres, el soporte recibido correspondió a una estrategia elaborada como consultoría y, además, el propio documento señaló, en términos generales, que **“en la actualidad [el ICA] no cuenta con una adecuada estrategia de recuperación de los servicios de tecnología”**, lo cual incrementó la relevancia de contar con planes/pruebas formalmente ejecutadas y documentadas.



De forma consistente con lo anterior, en el documento remisorio de evidencias se listó el subnumeral de **“evidencias de pruebas de DRP (planes, cronogramas, reportes de ejecución y resultados) realizadas durante 2024 y 2025”** sin que se observaran soportes de ejecución para el periodo auditado, lo cual incrementó la exposición al riesgo de no contar con una capacidad probada de recuperación.

**Riesgo OCI-04. Trazabilidad insuficiente para reconstrucción de eventos que afecten disponibilidad (y para soportar auditoría), por retención/rotación limitada y ausencia de un esquema evidenciable de conservación histórica.**
Se identificó exposición al riesgo de limitación para reconstrucción de eventos y análisis técnico de incidentes de disponibilidad, debido a que se documentó que, para la base de datos de producción, los logs fueron “personalizados” por incidentes de espacio, con retención operativa de “hasta 7 archivos” y rotación cuando alcanzan “200 M”. Esta condición, sin evidencia complementaria de centralización, retención extendida o conservación histórica por el periodo 2024–2025, incrementó el riesgo de no disponer de registros suficientes para correlación de fallas, análisis forense/operativo, y soporte de rendición de cuentas sobre indisponibilidades.

**Riesgo OCI-05. Inconsistencias en la trazabilidad integral de la continuidad del servicio por dispersión de responsabilidades y evidencia no consolidada (OTI – área misional / mesa de ayuda).** Se identificó exposición al riesgo de que la gestión de incidentes de indisponibilidad no cuente con un histórico integral y trazable de punta a punta (detección–registro–escalamiento–resolución–cierre), en tanto el documento remisorio asoció los registros de incidentes a diferentes actores (área misional y mesa de ayuda), sin que, para el periodo solicitado, se evidenciara un repositorio consolidado que permitiera correlacionar los incidentes con los eventos técnicos y con los mecanismos de recuperación (respaldos/restauraciones/acciones correctivas).

Nota de auditoría (para consistencia del informe): los riesgos anteriores se formularon como **exposiciones de riesgo** identificadas en el ejercicio, derivadas de las mismas condiciones que soportaron las observaciones del numeral 5.4, y se registraron en este apartado debido a que, con la evidencia disponible, **no se obtuvo trazabilidad suficiente** para demostrar su incorporación formal (y su control asociado) dentro del Mapa de Riesgos Institucional aplicable a SimplifICA para el periodo 2024–2025.

## 7. SEGUIMIENTO A PLANES DE MEJORAMIENTO

En el marco de la auditoría interna al procedimiento PRA-SPA-P-017 V.2 “Registro de Alimentos para Animales”, con enfoque en la línea de disponibilidad (y la trazabilidad asociada) del Modelo de Seguridad y Privacidad de la Información (MSPI), se consideró pertinente verificar la existencia y estado de planes de mejoramiento derivados de ejercicios previos, en la medida en que el propio marco institucional del ICA vincula la Política de Gobierno Digital (MinTIC) con la implementación del SGSI y del MSPI, incluyendo componentes de continuidad y disponibilidad.

Lo anterior se sustentó en que el Plan de Seguridad y Privacidad de la Información del ICA indicó expresamente que se estableció para dar cumplimiento a lineamientos emitidos por el MinTIC, incluyendo la Política de Gobierno Digital, y para la implementación del SGSI institucional. Asimismo, dicho Plan definió como propósito “definir y aplicar lineamientos” para tratar

integralmente riesgos de seguridad y privacidad, seguridad digital y continuidad de la operación de los servicios, preservando la disponibilidad (junto con confidencialidad e integridad), y reiteró dentro de su política de alto nivel que el SGSI busca prevenir incidentes y propender por la continuidad de los servicios, en cumplimiento de requisitos normativos y legales.

De manera concordante, el Manual de Políticas de Seguridad de la Información (ICA) incorporó lineamientos explícitos sobre continuidad, señalando que la continuidad de seguridad de la información debía incluirse en los sistemas de gestión de continuidad de negocio, que la OTI debía elaborar el Plan de Recuperación ante Desastres (DRP) para servicios y sistemas con impacto alto, y que debían realizarse pruebas periódicas y verificaciones de controles de continuidad; adicionalmente, contempló lineamientos de redundancia y disponibilidad de instalaciones de procesamiento de información (GIT-PTI-POL-001).



Con base en ello, la relación entre Política de Gobierno Digital – MSPI/SGSI – continuidad/disponibilidad se consideró aplicable al análisis de este numeral. No obstante, para efectos del seguimiento a planes de mejoramiento, durante el desarrollo de la auditoría no se contó con evidencia documental que permitiera verificar un Plan de Mejoramiento vigente asociado a auditorías previas relacionadas con la Política de Seguridad y Privacidad de la Información, el SGSI y/o el MSPI, ni soportes formales de seguimiento (p. ej., plan oficializado, matriz de seguimiento, informes de avance o cierres). En consecuencia, no fue viable realizar seguimiento a planes de mejoramiento en los términos del informe, dado que el procedimiento institucional define el plan de mejoramiento como la herramienta para consolidar hallazgos/oportunidades y soportar el seguimiento a acciones de mejora.

En virtud de lo anterior, el numeral “Seguimiento a planes de mejoramiento” se registró como no evaluable, toda vez que durante el desarrollo de la auditoría no se evidenció la existencia ni se contó con el soporte del Plan de Mejoramiento (Forma 4-510) asociado al objeto auditado, ni con documentación que acreditara su formulación, oficialización y estado de avance. En consecuencia, no fue posible efectuar verificación de cumplimiento, trazabilidad de acciones y cierre, por ausencia de evidencia suficiente y adecuada para sustentar el seguimiento. *(Lo anterior se enmarca en el procedimiento CIG-OCI-P-002, según el cual el informe de auditoría constituye base para la definición del plan de mejoramiento y su suscripción por el área responsable en los términos establecidos.)*

## 8. RECOMENDACIONES GENERALES Y CONCLUSIONES

### 8.1 RECOMENDACIONES GENERALES

Con base en los resultados obtenidos durante el desarrollo de la auditoría al procedimiento PRA-SPA-P-017 V.2 “Registro de Alimentos para Animales” y el análisis de la evidencia recibida para la línea de disponibilidad (y su trazabilidad asociada) del MSPI sobre el sistema SimplifICA 1.0 – Alimentos para Animales, la Oficina de Control Interno recomendó que la Oficina de Tecnologías de la Información (OTI), en articulación con la unidad misional, consolidara la operación y el aseguramiento de evidencia verificable que permita demostrar de manera consistente la efectividad de los controles institucionales de disponibilidad (monitoreo, respaldos, recuperación/continuidad y trazabilidad), en coherencia con el marco institucional del SGSI que prevé seguimiento, medición e indicadores, así como auditoría interna y mejora continua como parte del ciclo de gestión del sistema.

De manera específica, la Oficina de Control Interno recomendó que la OTI asegurara que la gestión de respaldos de SimplifICA contara con registros consolidados, verificables y disponibles para auditoría, que evidenciaran la validación de resultados y el histórico de ejecución de las tareas, en línea con los lineamientos institucionales que establecen que el rol administrador de backups debe validar el resultado de las copias, registrar novedades en bitácora, realizar pruebas trimestrales de restauración y garantizar que cada copia quede registrada (logs o archivo externo) disponible para controles o auditoría.

En lo correspondiente a continuidad y recuperación, la Oficina de Control Interno recomendó que se robusteciera la disponibilidad de evidencia sobre la gestión integral de recuperación ante desastres, teniendo en cuenta que las políticas institucionales contemplan como lineamiento que

la OTI elabore el DRP para servicios y sistemas de alto impacto y que se asegure la realización de pruebas periódicas del DRP y/o continuidad, verificando y documentando dichas pruebas. Adicionalmente, se consideró pertinente que los avances se armonizaran con insumos institucionales existentes como la “Estrategia DRP” recibida (documento que plantea alternativas para responder ante interrupciones de servicios tecnológicos).

Respecto de la trazabilidad, la Oficina de Control Interno recomendó fortalecer la gestión de registros y logs del sistema, de forma que existiera evidencia suficiente para reconstruir eventos relevantes de disponibilidad. Esta recomendación se soportó en los lineamientos institucionales que establecen que se deben generar y mantener registros de auditoría sobre actividades de usuarios, excepciones y eventos, y que los registros deben protegerse contra intentos de alteración y acceso no autorizado, además de asegurar su disponibilidad para controles o auditoría.

Finalmente, la Oficina de Control Interno recomendó que los resultados del ejercicio de auditoría fueran gestionados dentro del esquema institucional de mejora, conforme a lo previsto por el SGSI respecto a la gestión de oportunidades de mejora y eliminación de causas de no conformidades, y en concordancia con el procedimiento institucional de auditoría interna que dispone que el informe de auditoría soporta la estructuración de planes de mejoramiento y la gestión posterior de ajustes en la Forma 4-510.

**8.2 CONCLUSIONES**

Como resultado de la auditoría, se concluyó que el Instituto contaba con un marco institucional que reconoce la disponibilidad y la continuidad como componentes del SGSI/MSPI, evidenciado en instrumentos como el Plan de Seguridad y Privacidad de la Información (aprobado en sesión del 02 de julio de 2024), cuyo objetivo incluyó tratar integralmente los riesgos de seguridad y privacidad y la continuidad de la operación de los servicios, preservando la confidencialidad, integridad y disponibilidad de la información.

La auditoría permitió evidenciar que la continuidad operativa del procedimiento PRA-SPA-P-017 y la confiabilidad de los registros asociados dependieron de manera significativa de controles tecnológicos administrados por la OTI. En consecuencia, las debilidades identificadas en evidencia de disponibilidad y trazabilidad se constituyeron en factores de riesgo para la Subgerencia de Protección Animal como unidad auditable, al impactar la capacidad de reconstrucción de eventos, análisis de incidentes y aseguramiento de la operación del servicio

No obstante, para el alcance auditado (SimplifICA 1.0 – Alimentos para Animales), se concluyó que la evidencia aportada por la OTI para el periodo 2024–2025 presentó limitaciones de completitud y trazabilidad que afectaron la posibilidad de verificar integralmente la operación, periodicidad y resultados de los controles de disponibilidad. En particular, en el documento remisorio recibido se indicó que los “logs de ejecución van en crudo” y que era necesario revisar ejecuciones a través de scripts para corroborar la operación; adicionalmente, se reportaron condiciones operativas de logs de base de datos asociadas a rotación/retención limitada, lo que reforzó la conclusión de que la trazabilidad histórica completa (para reconstrucción de eventos a lo largo del periodo requerido) no quedó plenamente soportada con evidencia integral y continua.

En materia de respaldos y recuperación, la auditoría permitió concluir que, aunque existían lineamientos institucionales que exigían validación del resultado de copias, registro en bitácora, disponibilidad de registros para auditoría y la realización de pruebas de restauración de manera trimestral, la evidencia entregada a la auditoría no permitió demostrar plenamente dichos componentes en forma consolidada y trazable para todo el periodo 2024–2025, por lo cual se mantuvo la exposición a debilidades en la demostración de efectividad de los controles de disponibilidad.

En continuidad, se concluyó que la Entidad contaba con lineamientos que establecían la necesidad de elaborar DRP para servicios/sistemas de alto impacto y de ejecutar y documentar pruebas periódicas; sin embargo, a partir de la evidencia documental revisada, la auditoría no logró soportar con suficiencia la ejecución y resultados de pruebas DRP en el periodo 2024–2025 (según la evidencia suministrada), lo cual limitó la capacidad de concluir sobre la capacidad

probada de recuperación frente a escenarios de indisponibilidad mayor, pese a la existencia de una estrategia preliminar recibida como insumo.
GIT-PTI-POL-001_POLITICAS_SEGUR…

En síntesis, se concluyó que las situaciones identificadas y descritas en las **Observaciones 1 a 8** evidenciaron oportunidades de fortalecimiento en la disponibilidad del servicio tecnológico que soportó el procedimiento PRA-SPA-P-017 V.2, particularmente en lo referente a: seguimiento evidenciable de instrumentos/controles del MSPI asociados a disponibilidad, trazabilidad de respaldos y restauraciones, formalización de monitoreo con reportes verificables, y gestión de registros/logs que permitieran reconstrucción de eventos para auditoría. Estas conclusiones guardaron coherencia con el enfoque institucional del SGSI de operar bajo seguimiento, medición e indicadores, y gestionar la mejora continua.



| FIRMA DE APROBACIÓN | NOMBRE Y FIRMA DEL(LOS) AUDITOR(ES) | FECHA DE APROBACIÓN |
|---|---|---|
| **Sandra Piedad Riaño Bustamante**<br>**Jefe Oficina Control Interno** | **Carlos Andrés Gómez Gómez** | **16/01/2026** |