INFORME DE AUDITORÍA INTERNA No.: 5

FECHA DE EMISIÓN DEL INFORME	**Día:**	04	**Mes:**	08	**Año:**	2023

1. PROCESO:	Gestión de Infraestructura y Tecnologías de Información.
2. LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):	Líder Estratégico: Directora de Tecnología de la Información y las Comunicaciones. Responsables de la actualización: 1. Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones, 2. Coordinador Grupo de Sistemas y Arquitectura de Tecnología 3. Coordinador Grupo Arquitectura de Datos 4. Coordinador Grupo de Proyectos de Tecnología 5. Coordinador del Grupo de Seguridad e Informática Forense.
3. OBJETIVO DE LA AUDITORÍA:	Verificar y evaluar la efectividad de las acciones definidas en los planes de mejoramiento del proceso de Gestión de Infraestructura y Tecnologías de Información y la auditoría especial al "Incidente de Seguridad Informática", así como, el cumplimiento normativo y lo establecido en los procedimientos internos aplicables en el marco del Sistema de Gestión Integrado, con el fin de obtener información que permita identificar oportunidades de mejora para el proceso, el Sistema de Gestión Integrado, el Sistema de Control Interno y la Gestión Institucional.
4. ALCANCE DE LA AUDITORÍA:	Se realizó auditoría a la gestión del proceso, mediante prueba selectiva o muestreo de las actividades desarrolladas durante el periodo comprendido entre el 11 de junio de 2022 y el 04 de julio de 2023, fecha de inicio de esta auditoría. Para su desarrollo se aplicó el Modelo Integrado de Planeación y Gestión - MIPG, la Guía de Auditoria para Entidades Públicas, y las directrices para la auditoría de los Sistemas de Gestión, contenidas en la Guía Técnica Colombiana ISO 19011:2018.

	No fue necesario incorporar hechos adicionales por fuera del periodo definido.
5. CRITERIOS DE LA AUDITORÍA:	Se evaluaron y verificaron los siguientes criterios: • Norma Técnica Colombiana ISO 27001:2013: requisitos 10.1 No conformidades y acciones correctivas y 10.2 Mejora continua. • Controles Anexo A de la Norma Técnica Colombiana ISO 27001:2013 A.6.1.5; A.8.2.1; A.9.1.1; A.9.2.6; A.10.1.2; A.11.2.4; A.11.2.7; A12.1.2; A.14.1.1; A14.3.1; A.17.1.3. • Procedimientos Internos que le sean aplicables, en el marco del Sistema de Gestión Integrado.

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	10	**Mes**	07	**Año**	2023	**Desde:**	04/07/2023 D / M / A	**Hasta:**	04/08/2023 D / M / A	Día	04	Mes	08	Año	2023

6. HALLAZGOS DE LA AUDITORÍA

6.1 ASPECTOS FUERTES DEL PROCESO:

Destacamos la colaboración de la Dirección de Tecnología de la Información y las Comunicaciones, y sus equipos de trabajo, para el desarrollo de la presente auditoria.

6.2 OBSERVACIONES

No se identificaron observaciones en el proceso.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
1. Reincidencia plan de mejoramiento No. 880 - Seguridad de la Información en la Gestión de Proyectos. Las acciones propuestas en el plan de mejoramiento No. 880 para eliminar la causa raíz de la observación No. 1, identificada en la auditoría realizada al proceso en el año 2022, referentes al Control A.6.1.5 Seguridad de la Información en la Gestión de Proyectos, no fueron efectivas, debido a que se evidenció que el formato modificado "GC-F-015 Planeación de Proyectos", no se oficializó en el Sistema de Gestión Integrado y por lo tanto, no se identifican ni tratan riesgos de Seguridad de la Información en la gestión de proyectos en cada una de sus fases, cuando aplique, indistintamente del tipo de proyecto. Es importante precisar que no todos los proyectos se desarrollan a través de la ejecución de un contrato, por lo que no solo debe centrarse el área en los riesgos de seguridad de la información generados al ser parte de un proceso contractual. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.
2. Reincidencia plan de mejoramiento No. 879 – Clasificación de la información. Las acciones propuestas en el plan de mejoramiento No. 879 para eliminar la causa raíz de la observación No. 2, identificada en la auditoría realizada al proceso en el año 2022, referentes al Control A.8.2.1 Clasificación de la Información, no fueron efectivas, debido a que el documento GC-I-001 Instructivo para la Identificación, Clasificación, Valoración y Etiquetado de Activos de Información, no ha sido publicado en el Sistema de Gestión Integrado, sin embargo al revisar el documento, este cuenta con la criticidad y el tratamiento que se debe dar a los activos de la información, de acuerdo con los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
3. Reincidencia plan de mejoramiento No. 883 - Gestión de Llaves. Las acciones propuestas en el plan de mejoramiento No. 883 para eliminar la causa raíz de la no conformidad No. 3, identificada en la auditoría realizada al proceso en el año 2022, referentes al control A.10.1.2 Gestión de llaves, no fueron efectivas, debido a que se evidenció que las acciones tomadas se realizaron por fuera del plazo acordado. Adicionalmente, los documentos GC-MO-001 Documento de Modelos, GINT-PR-010 Gestión de Usuarios Plataforma Tecnológica y el formato FTO GINT-F-023 Seguridad para Respaldo de Contraseñas no se encuentran actualizados, de acuerdo a la directriz impartida por la Dirección de Tecnología de la Información y las Comunicaciones de cómo custodiar las contraseñas de acceso a servidores que forman parte de la plataforma tecnológica de la Entidad. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.
4. Reincidencia plan de mejoramiento 884 – Gestión de Cambios. Las acciones propuestas en el plan de mejoramiento No.884 para eliminar la causa raíz de la no conformidad No. 6, identificada en la auditoría realizada al proceso en el año 2022, referentes al Control A.12.1.2 Gestión de Cambios, no fueron efectivas, debido a que se evidenció que en las actas de las reuniones de Comité de Cambios no se registra el porcentaje real de la votación obtenida en cada sesión, conforme a los soportes de los votos de cada uno de los participantes. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013. La anterior situación es reiterativa, puesto que se identificó en la auditoría realizada en la vigencia 2020.	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
5. Reincidencia plan de mejoramiento 888 – Protección de Datos de Prueba. Las acciones propuestas en el plan de mejoramiento No.888 para eliminar la causa raíz de la no conformidad No. 8, identificada en la auditoría realizada al proceso en el año 2022, referentes al Control A.14.3.1 Protección de Datos de Prueba, no fueron efectivas, debido a que para esta vigencia se volvieron a evidenciar radicados de pruebas, sin anular y con estado “oficial” en el gestor documental. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.
6. Reincidencia plan de mejoramiento No. 893 – Indicadores de Gestión. Las acciones propuestas en el plan de mejoramiento No. 893 para eliminar la causa raíz de la no conformidad No.10, identificada en la auditoría realizada al proceso en el año 2022, referente al cumplimiento de la Guía de indicadores de Gestión GC-G-001, no fueron efectivas, lo cual se evidenció en lo siguiente: • Los Indicadores de Gestión de la vigencia 2023, no se encuentran publicados en la Página Web de la Entidad. • No se encuentran identificadas las bases de datos o archivos que soportan los registros de las variables de los indicadores. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013. La anterior situación es reiterativa, puesto que se identificó en la auditoría realizada en la vigencia 2020.	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.
7. Reincidencia plan de mejoramiento No. 889 – Riesgos de Gestión del Proceso. Las acciones propuestas en el plan de mejoramiento No.889 para eliminar la causa raíz de la no conformidad No. 11, identificada en la auditoría realizada al proceso en el año 2022, no fueron efectivas, debido	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
a que no hay evidencias del monitoreo de los riesgos para el año 2023, en el aplicativo de Riesgos y Auditoria. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.	
8. Reincidencia plan de mejoramiento No.881 – Actualización de la Información Documentada. Las acciones propuestas en el plan de mejoramiento No.881 para eliminar la causa raíz de la no conformidad No. 13, identificada en la auditoría realizada al proceso en el año 2022, referentes a la Creación y Actualización de la Información Documentada, no fueron efectivas, debido a que se hallaron documentos desactualizados en la caracterización del proceso o no se encuentran documentados como: • Los Planes de recuperación ante desastres (Disaster Recovery Plan o DRP), en los que no se ha realizado la identificación de la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la Entidad. • El Normograma no se ha actualizado. • La Entidad no cuenta con un Plan de Continuidad del Negocio que contenga el Análisis de Impacto al Negocio (Bussiness Impact Analisys - BIA) y las estrategias asociadas, desarrollado por la Oficina Asesora de Planeación, que le permita a la Dirección de Tecnología de la Información y las Comunicaciones determinar la disponibilidad de la plataforma tecnológica requerida para soportar los procesos de la Entidad, desde el punto de vista técnico. No es de exclusiva responsabilidad de los líderes de este proceso la construcción del Plan de Continuidad del Negocio, puesto que, derivado de éste, la Dirección de Tecnología de la Información y las Comunicaciones construye e implementa el Plan de Recuperación ante Desastre y el levantamiento de la información pertinente, para construir estos planes, por lo que es necesario que se aborde con los responsables. Por lo anterior, se incumple el requisito del numeral 10.1 No conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
9. Reincidencia plan de mejoramiento No. 919 – Guía Gestión de Incidentes GINT-G-006. Las acciones propuestas en el plan de mejoramiento No. 919 para eliminar la causa raíz de la observación No. 7, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, referentes a la actualización de la Guía de Gestión de Incidentes GINT-G-006, no fueron efectivas, debido a que se evidenció que ésta si bien se actualizó, no se oficializó en la caracterización del proceso, de acuerdo con el control de cambios, el cual registra que el último fue realizado el 23 de diciembre de 2021. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.
10. Reincidencia plan de mejoramiento No. 921 – Oficial de Seguridad de la Información. Las acciones propuestas en el plan de mejoramiento No. 921 para eliminar la causa raíz de la observación No.9, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, referente al contrato de prestación de servicios del Oficial de Seguridad de la información en cuanto a la supervisión, que se encontraba bajo la Dirección de Tecnología de la Información y las Comunicaciones y del Asesor del Despacho, no fueron efectivas ya que para el año 2022 y 2023 las designaciones del supervisor se encuentran así: • Contrato No. 076 de 2022 *"(…) - CLÁUSULA DÉCIMA PRIMERA. - DESIGNACIÓN DEL SUPERVISOR: La Superintendencia de Sociedades, con el fin de verificar el cumplimiento del contrato y la calidad del servicio, ejercerá los debidos controles a través de la supervisión, que será ejercida por el Director de Tecnología de la Información y las Comunicaciones. En caso de ausencia temporal o definitiva del Supervisor principal, el Asesor del Despacho Grado 11 asumirá lo reemplazará (…)"* • Contrato No. 102 de 2023 *"(…)- CLÁUSULA DÉCIMA PRIMERA. - DESIGNACIÓN DEL SUPERVISOR: La Superintendencia de Sociedades, con el fin de verificar el cumplimiento del contrato y la calidad del servicio, ejercerá los debidos controles a través de la supervisión, que será ejercida por la Directora de Tecnología de la Información. En caso de vacancia temporal o definitiva del*	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
cargo de quién ejerce la supervisión de manera principal, la misma será ejercida por el Coordinador del Grupo de Proyectos de Tecnología (…)" Lo anterior, evidencia que no se consideró la observación que se realizó en la auditoria del año 2022, la cual fue soportada de acuerdo a lo dispuesto por el Ministerio de las Tecnologías y las Comunicaciones en el Manual de Gobierno Digital. Ahora bien, en concordancia con lo anterior, en la Resolución 500 del 2021 del Ministerio de las Tecnologías y las Comunicaciones, por la cual se establecen los lineamientos y estándares para la estrategia de Seguridad Digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital, en su Anexo No. 1. Documento Maestro del Modelo de Seguridad y Privacidad de la Información, en su numeral 7.2.3 Roles y Responsabilidades se indica lo siguiente, frente al Oficial de Seguridad de la Información: *"(…) Se debe delegar a un responsable de la seguridad y privacidad de la información y el equipo humano necesario para coordinar la implementación del MSPI; si el cargo no existe en la Entidad deberá ser delegado por acto administrativo y deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador), de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto y en el comité de control interno con voz(…)"* Por lo anterior, se incumple el requisito del numeral 10.1 No conformidades y acciones Correctivas de la Norma NTC ISO 27001:2013.	
11. Reincidencia plan de mejoramiento 925 – Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información. Las acciones propuestas en el plan de mejoramiento No. 925 para eliminar la causa raíz de la no conformidad No. 1, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, referentes al Control A.17.1.3 Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información, no fueron efectivas, por cuanto no se han cumplido las actividades propuestas en el plan de mejora relacionadas con el Plan anual con proyecto de continuidad, el	Numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
Cronograma de actualización de documentos y el Plan de Ejecución de Pruebas. Por lo anterior, se incumple el requisito del numeral 10.1 No Conformidades y Acciones Correctivas de la Norma NTC ISO 27001:2013.	

7. CONCLUSIONES DE LA AUDITORÍA

El equipo auditor concluye lo siguiente:

1. El plan de mejoramiento No. 878, propuesto para eliminar la causa raíz de la observación No. 3, identificada en la auditoría realizada al proceso en el año 2022, es efectivo, puesto que se tramitó por parte de la Dirección de Tecnología de la Información y las Comunicaciones la solicitud de un cargo técnico o profesional, para el funcionario encargado de la extracción de evidencia digital, asignado al Grupo de Seguridad e Informática Forense. Se adjuntó como evidencia, la Resolución de nombramiento provisional de encargo, radicado 2022-01-949061 del 27/12/2022.

2. El plan de mejoramiento No. 886, propuesto para eliminar la causa raíz de la no conformidad No. 1, identificada en la auditoría realizada al proceso en el año 2022, referente al Control A.9.1.1 Política de Control de Acceso, de la norma NTC ISO 27001:2013, es efectivo. Se verificaron las novedades de retiro y se emitió el memorando radicado 2022-01-954516 del 30/12/2022, se informa sobre la actualización de los cargos de los funcionarios de la Entidad.

3. El plan de mejoramiento No. 885, propuesto para eliminar la causa raíz de la no conformidad No. 2, identificada en la auditoría realizada al proceso en el año 2022, referente al Control A.9.2.6. Retiro o Ajuste de los Derechos de Acceso, de la norma NTC ISO 27001:2013, es efectivo. No obstante, es importante identificar los usuarios asociados a las diferentes aplicaciones, bases de datos y estandarizar las nomenclaturas de usuarios con su ubicación.

4. El plan de mejoramiento No. 882, propuesto para eliminar la causa raíz de la no conformidad No. 4, identificada en la auditoría realizada al proceso en el año 2022, referente al Control A.11.2.4 Mantenimiento de Equipos, de la norma NTC ISO 27001:2013, es efectivo. Se adjuntó el Programa de Mantenimientos Preventivos.

5. El Plan de mejoramiento No. 887, propuesto para eliminar la causa raíz de la no conformidad No. 5, identificada en la auditoría realizada al proceso en el año 2022, referente al Control 11.2.7. Disposición Segura de Equipos, fue efectivo, sin embargo, es importante revisar el seguimiento a las actividades y puntos de control indicados en el procedimiento GINT-PR-016 Respaldo y Borrado de Información para Equipos de funcionarios y Contratistas.

7. CONCLUSIONES DE LA AUDITORÍA

6. El Plan de mejoramiento No. 890, propuesto para eliminar la causa raíz de la no conformidad No. 12, identificada en la auditoría realizada al proceso en el año 2022, no fue efectivo, ya que los planes No 555: Indicadores de Gestión, 556: Cargue en el aplicativo extemporáneo y 560: Gestión de Cambios presentaron reincidencia en el presente informe.

7. El plan de mejoramiento No. 892, propuesto para eliminar la causa raíz de la no conformidad No. 7, identificada en la auditoría realizada al proceso en el año 2022, referente al Control A.14.1.1 Análisis y Especificación de Requisitos de Seguridad de la Información, de la norma NTC ISO 27001:2013, no es posible evaluar su efectividad, teniendo en cuenta que desde el cierre del plan de mejoramiento 30/06/2023 a la fecha de terminación de esta auditoria no se han desarrollado mantenimientos evolutivos de los sistemas existentes, que tengan que ver particularmente con temas de seguridad. La efectividad se evaluará en la próxima auditoria al proceso.

8. El plan de mejoramiento No. 891, propuesto para eliminar la causa raíz de la no conformidad No. 9, identificada en la auditoría realizada al proceso en el año 2022, referente al numeral 2.1.4.1 del Documento de Modelos, GC-MO-001, es efectivo. Sin embargo, es pertinente contar de forma permanente con el profesional especializado para el Rol de Oficial de Seguridad de la Información para asegurar el mantenimiento y la mejora del Sistema de Gestión de la Seguridad de la Información en la Entidad.

9. El Plan de mejoramiento No. 913, propuesto para eliminar la causa raíz de la observación No. 1, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo, por lo que se debe continuar con el aseguramiento y la priorización de la contratación del SOC/ NOC, Centro de Operación de Seguridad y demás acciones tendientes a la seguridad de la plataforma tecnológica.

10. El Plan de mejoramiento No. 914, propuesto para eliminar la causa raíz de la observación No. 2, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo. Sin embargo, es necesario mantener la continuidad de la prestación de los servicios de los especialistas, en la administración del Firewall y- Firewall de Aplicaciones Web (WAF), teniendo en cuenta el impacto y la criticidad de los servicios, que protegen los activos de información de la Entidad.

11. El Plan de mejoramiento No. 915, propuesto para eliminar la causa raíz de la observación No. 3, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo. Sin embargo, este debe contar con un horizonte de las necesidades de Tecnología de la información - TI a corto, mediano y largo plazo, que permita mejorar los servicios al ciudadano.

12. El Plan de mejoramiento No. 916, propuesto para eliminar la causa raíz de la observación No. 4, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo. Sin embargo, es necesario mantener los cambios de contraseñas, la activación de la doble autenticación y el monitoreo en las cuentas de usuario administrador para garantizar que los usuarios que ingresan sean los autorizados.

13. El Plan de mejoramiento No. 917, propuesto para eliminar la causa raíz de la observación No. 5, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo. Es

7. CONCLUSIONES DE LA AUDITORÍA

importante analizar permanentemente el estado de todos los componentes de la plataforma tecnológica de la Entidad, para actuar de manera ágil y oportuna ante cualquier vulnerabilidad.

14. El Plan de mejoramiento No. 918, propuesto para eliminar la causa raíz de la observación No. 6, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo. Es necesario mantener actualizadas las licencias de las versiones Windows 10 y Windows 10 21H2, que permitan instalar las nuevas versiones del antivirus y proteger los activos de información de la Entidad.

15. El Plan de mejoramiento No. 920, propuesto para eliminar la causa raíz de la observación No. 8, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo, puesto que se identifican campañas de sensibilización, así como correos y tips orientados a fomentar la toma de conciencia en todos los funcionarios, contratistas, pasantes y practicantes de la Entidad frente a la seguridad de la información y la ciberseguridad.

16. El Plan de mejoramiento No. 922, propuesto para eliminar la causa raíz de la observación No. 8, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo, puesto que se identifica que en la Entidad hay profesionales que ejercieron las funciones en la administración de servidores y posteriormente, en la orden de compra No. 111108 del 9 de junio de 2023 en el ítem 17, se encuentra identificada la contratación del mismo, así: *"(…)mst02--8 - IT-MS-02-541-e-Agente de Mesa de Servicios Nivel 2 Mensual Mayor o igual a 6 meses. En sitio (Instalaciones de la Entidad) - zona 1_Especializado en Administrador en Servidores y Aplicaciones - zona 1 Jornada Ordinaria-Bronce(…)".*

17. El Plan de mejoramiento No. 923, propuesto para eliminar la causa raíz de la observación No. 11, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo. Desde la Dirección de Tecnología de la Información y las Comunicaciones se documentaron y socializaron las lecciones aprendidas. Es importante cerrar el evento del incidente tan pronto se culmine con las actividades pendientes.

18. El Plan de mejoramiento No. 924, propuesto para eliminar la causa raíz de la observación No. 12, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo. En el informe final del incidente, en la sección de FASE POST-INCIDENTE, se realizaron los requerimientos de personal y se aprobó la contratación de los profesionales expertos. Es importante mantener la continuidad del personal especializado requerido.

19. El Plan de mejoramiento No. 926, propuesto para eliminar la causa raíz de la no conformidad No. 2, identificada en la auditoría realizada al Incidente de Seguridad Informática en el año 2022, es efectivo. Se le están asignando computadores de la Entidad a contratistas con acceso privilegiado con las condiciones de seguridad requerida.

20. Se evaluó la conformidad del requisito del numeral 10.2 Mejora Continua de la Norma NTC ISO 27001:2013 y se declara conforme. Se ha trabajo en la consecución de los expertos necesarios para la gestión de los diferentes componentes de TI, se está trabajando en la documentación del proceso y se

7. CONCLUSIONES DE LA AUDITORÍA

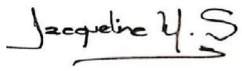
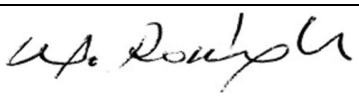
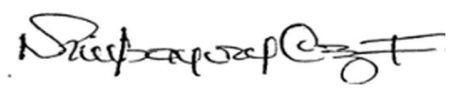
están generando alertas de situaciones peligrosas que pueden afectar la seguridad de la información institucional.

Se realizó la socialización de la importancia del autocontrol para detectar desviaciones y efectuar correctivos, asegurando el logro de los resultados y contribuyendo a la mejora continua.

En conclusión, se identifican once (11) no conformidades, que requieren la estructuración de acciones correctivas que permitan garantizar el aseguramiento y mejora continua del proceso y por ende la madurez del Sistema de Gestión Integrado, el Sistema de Control Interno y la Gestión Institucional.

Para constancia se firma en Bogotá D.C., a los 04 días del mes de agosto del año 2023.

8. RESPONSABLES INFORME DE AUDITORÍA

Nombre Completo	Responsabilidad	Firma
Jacqueline Murillo Sánchez	Jefe Oficina de Control Interno	
Rocío Pedrozo Ulloa	Auditor Líder	
Miguel Darío Quintana Sánchez	Auditor	
Nini Sayury Cruz Toloza	Auditor	
Claudia Yaneth Pardo Cornelio	Auditor en formación	Funcionaria que al cierre de esta auditoría, se encuentra en vacaciones.

9. ANEXOS

Las listas de verificación, papeles de trabajo y evidencias se adjuntan en el aplicativo de Riesgos y Auditoría.