INFORME DE AUDITORÍA ESPECIAL No: 1- INCIDENTE DE SEGURIDAD

FECHA DE EMISIÓN DEL INFORME	**Día:**	25	**Mes:**	10	**Año:**	2022

1. PROCESO:	Incidente de Seguridad Informática.
2. LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):	• Directora de Tecnología de la Información y las Comunicaciones (E). • Oficial de Seguridad y, Coordinadores de los grupos de: • Innovación, Desarrollo y Arquitectura de Aplicaciones. • Sistemas y Arquitectura de Tecnología. • Arquitectura de Datos. • Proyectos de Tecnología. • Seguridad e Informática Forense y
3. OBJETIVO DE LA AUDITORÍA:	Evaluar el cumplimiento de guías, procedimientos y la conformidad de los requisitos del Anexo Técnico de la Norma NTC - ISO 27001:2013 Sistema de Gestión de la Seguridad de la Información, respecto de la gestión de incidentes informáticos.
4. ALCANCE DE LA AUDITORÍA:	Se realizó auditoría especial al incidente de seguridad informática, ocurrido el día 24 de junio de 2022, la cual fue solicitada por la Secretaría General mediante memorando No. 500-007147, radicado bajo el No. 2022-01-572536 del 25 de julio de 2022. El análisis y evaluación de la información se realizó por prueba selectiva o muestreo sobre las actividades desarrolladas por la Dirección de Tecnología de la Información y las Comunicaciones y los grupos que la integran, para el periodo comprendido entre el 01 de octubre de 2021 a la fecha de finalización de esta auditoría. Para su desarrollo se aplicaron las directrices para la auditoría de los Sistemas de Gestión, contenidas en la Guía Técnica Colombiana ISO 19011:2018 y la Guía No. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información de MinTic. No fue necesario incorporar hechos adicionales que estuvieran por fuera del alcance de la auditoría.

5. CRITERIOS DE LA AUDITORÍA:	Se verificaron los siguientes criterios: 1. La adecuada aplicación de las guías y procedimientos: • GINT-G-005 Guía DRP - Guía Plan de Recuperación ante Desastres. • GINT-G-006 Guía de Gestión de Incidentes. • GINT-G-007 Plan Recuperación Expediente Digital. • GINT-G-008 Plan Recuperación Postal. • GINT-G-010 Plan de recuperación BPM. • GINT-G-011 Plan de Continuidad Atención al Ciudadano. • GINT-G-012 Plan de contingencia para sistema SIIF. 2. Los controles del Anexo A de la norma NTC - ISO 27001: 2013: A.9.2.1, A.9.2.3, A.12.1.1, A.12.2.1, A.12.4.1, A.12.6.1, A.13.1.2, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7, A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1 y otros que les sea aplicable. Así como, los riesgos asociados a estos controles. 3. Seguimiento a las actividades Post-Incidente elaborado por la Dirección de Tecnología de la Información y las Comunicaciones.

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	05	**Mes**	10	**Año**	2022	**Desde:**	30/09/2022 D / M / A	**Hasta:**	28/10/2022 D / M / A	Día	28	Mes	10	Año	2022

6. HALLAZGOS DE LA AUDITORÍA

6.1 ASPECTOS FUERTES DEL PROCESO:

El compromiso de la Dirección de Tecnología de la Información y las Comunicaciones, junto con sus coordinadores, funcionarios y contratistas, que requirió una dedicación extra para superar el incidente de seguridad, gestionar y restablecer la infraestructura tecnológica de la Entidad, actividades que se continúan adelantando al cierre de esta auditoría.

6.2 OBSERVACIONES

En el desarrollo de la auditoría, el equipo auditor observó que:

1. En el Plan Anual de Adquisiciones desde la vigencia 2021, se contempló la suscripción al SOC "Security Operation Center", Centro de Operación de Seguridad que permite cuantificar amenazas de seguridad sobre la plataforma tecnológica. No obstante, ésta no se adelantó por recomendaciones del Comité de contratación, conforme a las observaciones registradas en el Memorando 159-008910 del 6 de septiembre de 2021, remitido por la Dirección de Tecnología de la Información y las Comunicaciones a la Dirección Administrativa. Durante la vigencia 2022, se formalizó mediante contrato 055 de 2022, cuyo objeto es prestar los servicios de un SOC para el monitoreo y alertamiento de la plataforma tecnológica de misión crítica de la Superintendencia de Sociedades, cuya ejecución inició el 22 de julio y finaliza el 30 de diciembre de 2022. Por ser esta una actividad prioritaria para la seguridad tecnológica, se sugiere mantener su continuidad, ampliar el cubrimiento y monitoreo de la plataforma tecnológica, definir el recurso humano necesario que realice seguimiento 24 horas todos los días (7*24) para actuar de manera oportuna e integrarlo en los documentos del proceso donde aplique.

2. Los ataques a las aplicaciones son una de las principales causas de infracción y la puerta de acceso a datos importantes. La Entidad cuenta con los equipos de Firewall y Firewall de Aplicaciones Web (WAF), con su correspondiente garantía y actualización, sin embargo, el profesional con conocimiento en la administración de estas herramientas, no cuenta con un espejo que se encargue del monitoreo en los tiempos de su ausencia temporal.

3. El Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI) que se articula con el Plan Estratégico Institucional, debe formularse para el periodo 2023 – 2026, contemplando los aspectos de fortalecimiento y desarrollo que requiere la Superintendencia de Sociedades para cumplir con la transformación digital y modernización institucional que demanda la Política de Gobierno Digital. Es la oportunidad para evaluar y actualizar la arquitectura empresarial (AE) para gestión de Tecnologías de la Información que posee la Entidad (segunda iteración de AE) y definir los proyectos estratégicos que permitan resolver las necesidades más apremiantes para la interacción con los diferentes grupos de interés y, a su vez, mejorar la capacidad y gestión de desempeño de TI y de la seguridad de la información.

4. Existen servidores en los cuales no se ha realizado modificación de contraseña de usuarios desde hace más de 5 años, por lo tanto, es necesario evaluar la implementación de mejores prácticas para la protección de la infraestructura Tecnológica, tales como:

a) Cambios de contraseñas.
b) Activación de la doble autenticación.
c) Bloqueo de contraseñas en caso de varios intentos errados.
d) Actualizaciones de protección contra virus y amenazas.
e) Monitoreo a las acciones que se llevan a cabo en las cuentas de usuario administrador.

5. La Entidad cuenta con el inventario completo de los recursos que conforman la plataforma tecnológica, sin embargo, es necesario analizar el estado actual de todos los componentes (hardware, software, sistemas de información, bases de datos, aplicativos, sistemas de almacenamiento y respaldo, entre otros) y delimitar cuáles son críticos para soportar los procesos y servicios de la Entidad, de manera que se puedan identificar las vulnerabilidades con mayor impacto y generar acciones para mitigarlos.

6.2 OBSERVACIONES

6. Existen diecisiete (17) estaciones de trabajo que no cumplen con los requisitos mínimos del sistema operativo y no soportan la actualización del Windows a la versión 10 21H2, generando una brecha de seguridad. Situación que debe ser solucionada con prioridad para minimizar los riesgos.

7. La Guía de Gestión de Incidentes GINT-G-006, versión 003, cuenta con actividades desactualizadas, por lo que es necesario revisar las siguientes:

En el numeral 6.1.1**.** Recurso de comunicación: En cuanto a la información de contacto no se relaciona la lista de las personas que conforman el grupo de gestión de incidente y es necesario hacer referencia al canal de comunicación con contratistas. Por último, para la política de comunicación de los incidentes de seguridad de la información, es importante definir el criterio para socialización y tratamiento según la magnitud y el impacto para la Entidad.

En el numeral 6.1.2. Recurso para el registro de incidentes: La lista de categorías de incidentes prevista en el Catálogo de servicios no se relaciona en la caracterización del proceso y se debe actualizar.

8. Es necesario reforzar la sensibilización y entrenamiento del personal, de forma que incluya entre otros contratistas, 4-72, personal de seguridad, mesa de ayuda, supernumerarios, judicantes y pasantes, de acuerdo con las políticas y buenas prácticas adoptadas por la Entidad en materia de seguridad de la información y ciberseguridad, actividad que se debe adelantar con el acompañamiento de Gestión del Talento Humano.

9. El contrato de prestación de servicios profesionales del Oficial de Seguridad de la Información se encuentra bajo la supervisión de la Dirección de Tecnología de la Información y las Comunicaciones y del Asesor del Despacho; situación que debe ser revisada y analizada para verificar que se cumpla con las recomendaciones y buenas prácticas emanadas del Ministerio de las Tecnologías y las Comunicaciones en el Manual de Gobierno Digital, en relación con la operación del elemento transversal de seguridad de la información, que señala: *"Para lograr un adecuado balance entre funcionalidad y seguridad, se recomienda que el elemento transversal de seguridad de la información opere de manera independiente a la Oficina de T.I. En este caso, la entidad puede ubicar esta iniciativa en un área como planeación, procesos, el área relacionada con gestión de riesgos, o bien, crear una nueva área dedicada a la seguridad de la información."*

10. La Entidad no cuenta con el personal experto para la administración de servidores, por cuanto, el contratista que cumplía con este rol, fue suspendido y por mutuo acuerdo, se dio por terminado el contrato el pasado 29 de septiembre de 2022. Situación que pone en riesgo el adecuado aseguramiento de la plataforma tecnológica de la Entidad.

11. Si bien es cierto aún existen actividades Post-Incidente pendientes de gestionar que no han permitido el cierre total del incidente, no se han documentado ni registrado de manera gradual las lecciones aprendidas de acuerdo al avance del restablecimiento de los servicios tecnológicos, información útil para la mejora de las medidas de seguridad y el proceso de gestión de incidentes. Esto es importante porque permite tener claridad

6.2 OBSERVACIONES

de lo que sucedió, si se tomaron las acciones adecuadas, qué se debe hacer cuando ocurra un incidente similar, identificar las acciones correctivas para prevenir incidentes similares en el futuro, entre otros.

12. El personal que está gestionando todas las actividades derivadas del post-incidente, es el mismo que se encarga del mantenimiento de la plataforma tecnológica y de la gestión de nuevos requerimientos. Es pertinente realizar un estudio de cargas de trabajo con el fin de determinar, de manera técnica, el volumen de tareas que se derivan de la gestión propia del proceso, frente a la cantidad de personal que sea necesario, para una gestión eficiente, efectiva y eficaz. Igualmente, es preciso mencionar que en los últimos años se han incorporado nuevas plataformas y herramientas tecnológicas, que requieren diseño, desarrollo, gestión, monitoreo y aseguramiento, sin embargo, no se ha aumentado el personal especializado requerido.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
1. Planes de Recuperación ante Desastres (DRP). La Entidad cuenta con planes de recuperación ante desastres (Disaster Recovery Plan o DRP), documentados en la caracterización del proceso de Gestión de Infraestructura y Tecnologías de la Información, no obstante, el equipo auditor identificó debilidades en los siguientes aspectos: **GINT-G-005 Guía: Plan de Recuperación ante Desastres** - El documento menciona la activación de un centro de cómputo en caso de afectación del centro de cómputo principal, del cual no se encuentra definida su ubicación, ni se han adelantado las actividades técnicas para su disponibilidad ante una emergencia. - Prevé pruebas periódicas de las estrategias y procedimientos para verificar el funcionamiento del DRP, en los diferentes escenarios de desastre, que no se han adelantado. - No se han realizado actividades de actualización y mantenimiento, capacitación y prueba del DRP con los funcionarios responsables, que están previstas. - No se define claramente la información que se debe documentar como evidencia de la ejecución del DRP. - El directorio de los responsables está desactualizado. **GINT-G-006: Guía DRP BPM** - No se han documentado las pruebas realizadas al DRP en el formato establecido. - No se ha realizado el Análisis de impacto en el formato establecido. - Falta actualización de los procesos que operan bajo BPM. - El directorio de los responsables del DRP está desactualizado	Control A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información de la norma ISO 27001:2013.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
GINT-G-007: Guía DRP Expediente Digital - El documento menciona la habilitación de un centro de cómputo alterno para un promedio de 100 usuarios concurrentes, que no existe. - Expone las direcciones IP de la infraestructura de servidores (Front End y Back End) y de base de datos, para funcionamiento del aplicativo. - Relaciona actividades de actualización, mantenimiento, capacitación y pruebas del DRP que no se han realizado. - El directorio de los responsables del DRP está desactualizado. **GINT-G-008: Guía DRP Postal** - No se documentan los diferentes escenarios de desastre ante una interrupción mayor. - Expone las direcciones IP de los servidores de base de datos y servicios Web. - No se realizaron pruebas a los escenarios definidos en el DRP. - El Directorio de los responsables del DRP está desactualizado. **GINT-G-011: Guía DRP ATC (Atención al Ciudadano)** - En los puntos 3.1 Escenarios de Contingencia, 3.4.3 Análisis de Impacto y 3.9 Recursos Mínimos se remite al anexo 1 para verificar los sistemas relacionados, pero no es coherente, porque el anexo 1 corresponde es al Directorio Telefónico. - No se realizaron actividades de entrenamiento, documentación, actualización y pruebas, que se relacionan en la guía. - Sólo se documentan las actividades del DRP para un escenario de contingencia “No es posible la atención personal al ciudadano en Bogotá”. Se deben contemplar los diferentes escenarios. - El directorio de los responsables está desactualizado **GINT-G-012: Guía DRP para Sistema SIIF** - El directorio de los responsables del DRP está desactualizado (Anexo 2). En relación con todos los DRP, no se ha realizado la identificación de la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la Entidad con el Análisis de Impacto al Negocio (Bussiness Impact Analisys - BIA).	

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
Lo anterior, incumple el Control A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información de la norma ISO 27001:2013.	
2. Uso y Registro de Computadores Personales. El equipo auditor evidenció que de ocho (8) contratos de prestación de servicios profesionales celebrados durante la vigencia 2022, para la Dirección de Tecnología de la Información y las Comunicaciones, sólo se asignó computador portátil a uno (1) de los contratistas y, por lo tanto, los demás se encuentran haciendo uso de sus equipos personales. Es importante garantizar el suministro de los equipos de trabajo por parte de la Entidad para usuarios con acceso privilegiado, con las condiciones de seguridad mínimas que requiere el ejercicio de sus tareas, toda vez que existen riesgos asociados a los dispositivos no autorizados. Lo anterior representa incumplimiento de las políticas de seguridad de la información: Política de trabajo remoto y dispositivos móviles y Política de uso adecuado de los recursos.	Documento de Políticas del SGI Código: GC-PO-001 Versión 013 del 9 de septiembre de 2022

7. CONCLUSIONES DE LA AUDITORÍA

De la evaluación realizada el equipo auditor concluye lo siguiente:

1. Es necesario fortalecer la política de control de acceso definiendo y documentando el plazo máximo para la deshabilitación de usuarios en el directorio activo, de acuerdo a su clasificación (usuario acceso general, usuario acceso privilegiado) y forma de vinculación (servidor público, contratista, pasante, entre otros).

2. Es importante concientizar y capacitar a todo el personal de la Entidad sobre las implicaciones y los riesgos de realizar ciertas actividades con el uso de la tecnología y los servicios informáticos, para lograr que se comprometan en el fortalecimiento de la seguridad de la información.

3. Se deben evaluar y documentar los DRP que cubran toda la plataforma tecnológica crítica de la Entidad, en caso de los diferentes escenarios de desastre que involucre todos los procesos, orientado a contar en un futuro cercano con una planeación de Continuidad del Negocio (Business Continuity Planning - BCP).

4. Para la atención del incidente ocurrido desde el 24 de junio de 2022, se adelantaron las actividades correspondientes definidas en las guías y procedimientos GINT-G-005 Guía DRP - Guía Plan de Recuperación ante Desastres y GINT-G-006 Guía de Gestión de Incidentes.

5. La Entidad debe garantizar los recursos económicos y de talento humano capacitado para el restablecimiento de la plataforma que aún continúa fuera de servicio, a causa del incidente tecnológico. Como lo son: System Center, Archivo histórico, Servicio de red inalámbrica y Calidad de datos. Cabe mencionar,

7. CONCLUSIONES DE LA AUDITORÍA

que el servidor de Ambiente de pruebas se recuperó después del incidente tecnológico, sin embargo, actualmente se encuentra fuera de servicio, debido a que sufrió un daño posterior a causa de un apagón.

6. Actualmente en la Dirección de Tecnología de la Información y las Comunicaciones existe personal que cumple funciones especiales para la administración y la gestión de TI, vinculados a la Entidad por contratos de prestación de servicios. La anterior situación, genera una alta rotación de profesionales, implementación deficiente de los sistemas de gestión, reprocesos, fuga de conocimiento, retrasos e inestabilidad para la Entidad. Este es el caso del Arquitecto de Software, el Administrador de Bases de Datos (DBA), el Oficial de Seguridad de la Información (Seguridad Digital), el Administrador de servidores, entre otros. Es pertinente que la administración evalúe la situación y de ser posible aplique la política de formalización de empleo impulsada por el Gobierno Nacional.

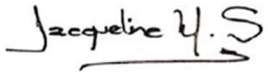
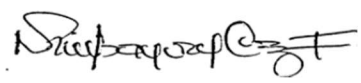
7. El plan de mejoramiento y de mitigación asociados con el incidente informático de seguridad, fue remitido por la Dirección de Tecnología de la Información y las Comunicaciones a la Oficina Asesora de Planeación el 24 de octubre de 2022. La efectividad y la ejecución de las acciones de los nuevos controles, deberá evaluarse en la próxima auditoría al proceso de Gestión de Infraestructura y Tecnología de información.

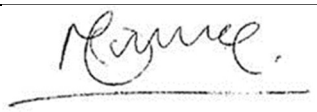
8. Se validó la conformidad de los controles del Anexo A de la Norma NTC-ISO 27001:2013 Sistema de Gestión de la Seguridad de la Información: A.9.2.1, A.9.2.3, A.12.1.1, A.12.2.1, A.12.4.1, A.12.6.1, A.13.1.2, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7, A.17.1.1, A.17.1.2, A.17.2.1, encontrándose conformes. No obstante, se identificó una (1) no conformidad que corresponde al control A.17.1.3 el cual requiere acciones de mejora.

En conclusión, se identificaron **doce (12) Observaciones y dos (2) No conformidades**, que requieren la estructuración de acciones preventivas y correctivas que permitan garantizar la mejora continua del proceso y en consecuencia 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 27 días del mes de octubre del año 2022

8. RESPONSABLES INFORME DE AUDITORÍA

Nombre Completo	Responsabilidad	Firma
Jacqueline Murillo Sánchez	Jefe Oficina de Control Interno	
Rocío Pedrozo Ulloa	Auditor Líder	
Nini Sayury Cruz Toloza	Auditor	
Miguel Darío Quintana Sánchez	Auditor	

8. RESPONSABLES INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad**	**Firma**
Lisbeth Heliana Hernández	Auditor	
Luis Felipe Mosquera	Auditor en Formación	

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