1. DESCRIPCIÓN DE LA AUDITORIA INTERNA

Sistema de gestión auditado	**Sistema de Gestión de Seguridad de la Información**	
Método de auditoría *(marcar con x)*	**Presencial ____X____**	**Virtual _____**
Informe *(marcar con x)*	**Preliminar _____**	**Final ____X____**
Fecha informe *(dd/mes/año)*	**31/10/2023**	
Proceso auditado / Tema	Gestión del Proceso Auditor	**PAAI ___2023_____** *vigencia*
N° acta y fecha de aprobación PAAI por el CICCI	Acta Nro. 8 del 29 de agosto de 2023	
Líder del proceso auditado	Mariana Gutierrez Dueñas – Directora Oficina de Planeación	
Líder del equipo auditor	Leonardo Sierra Rodríguez	
Objetivo de la auditoría interna	Evaluar la conformidad de los requisitos de la norma NTC-ISO/IEC 27001:2022 implementados en el Modelo de Seguridad y Privacidad de la Información (MPSI), que permita la mejora continua de acuerdo al ciclo (PHVA).	
Alcance de la auditoría interna	Auditoría interna a los controles del Modelo de Seguriudad y Privacidad de la Información (MSPI) bajo la norma ISO/(IEC 27001:2022, con alcance a la protección de la confiendencialiad, integridad y disponibilidad de la información asociada al proceso de Gestión del Proceso Auditor	
Criterios de auditoría (CLIO)	NTC-ISO/IEC 27001:2022, ISO/IEC 27007:2020, ISO 19011:2018, SGSI - MSPI	

	Nombre	**Dependencia**	**Cargo**
Enlace – Guia (Funcionarios del proceso auditado)	Jose Antonio Mantilla Villareal	Grupo TIC	Asesor de Despacho
	Sandra Gil Rodriguez	Grupo TIC	Contratista
	Nombre	**Dependencia**	**Cargo**
Equipo auditor	Leonardo Sierra Rodríguez	Control Interno	Contratista
	Omar Hugo Rivas Jimenez	Control Interno	Profesional Especializado grado 04
	Yanet Sofia Rodriguez Leguizamón	Control Interno	Profesiónal Universitario Grado 02
	Eugenio Miguel Carrillo Espinosa	Control Interno	Profesional Universitario Grado 01
	Viviana Cáceres Castro	Control Interno	Tecnico 01

2. ASPECTOS EVALUADOS EN LA AUDITORIA INTERNA

Aspecto	SI	NO
2.1. Cumplimiento del plan de mejoramiento		x
2.2. Gestión frente al mapa de riesgos del proceso	x	
2.3. Medición de indicadores		x
2.4. Cumpllimiento del Plan Operativo Anual del proceso		x
2.5. Gestión frente a los informes externos de responsabilidad del proceso. (Según Agenda de Informes Externos de la AGR, elaborada por la OCI y actualizada por los responsables)		x

3. Fortalezas

Al evaluar los requisitos de la norma NTC-ISO/IEC 27001:2022 implementados en el Modelo de Seguridad y Privacidad de la Información (MPSI), se evidencio la adecuada implementación del ciclo (PHVA), al igual que la disponibilidad, disposición y cumplimiento de la oportunidad de la entrega de la información por parte de las dependencias de la AGR a las cuales se les solicito la información pertinente. De igual manera se resalta el compromiso por parte de líder de Gestión de Proceso Auditor como alcance de la implemtación de la norma ISO/IEC 27001:2022.

4. Resultados detallados de la auditoria interna - Hallazgos

4.1 Conformidades

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
1	4.1 Comprensión de la organización y su contexto	Se evidencio que se han determinado las partes interesadas, para el Sistema de Gestión de Seguridad de la Información (SGSI), estas se encuentran documentadas en el archivo, contexto grupo de interés y requisitos. Evidencia: Contexto grupo de interés y requisitos.
2	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Se evidencio que la entidad ha determinado las partes interesadas al SGSI, las necesidades, los requisitos alineados al Sistema de Gestión de Seguridad de la Información. Evidencia: Contexto grupo de interés y requisitos.
3	4.3 Determinación del alcance del sistema de gestión de seguridad de la información	Se evidenció el establecimiento del alcance del Sistema de Gestión de Seguridad de la Información dentro del documento: "TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0", numeral 2. ALCANCE DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI. Pág. 1. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
4	4.4 Sistema de gestión de seguridad de la información	Se evidenció y se observo, que el Sistema de Gestión de Seguridad de la Información, se encuentra operando bajo la estructura del ciclo de la mejora continua, donde se incluyen los procesos necesarios para dar cumplimiento a los requisitos de la norma, en pro de la mejora continua. Evidencia: Todas las evidencias aportadas y las observaciones en sitio, dan como resultado la evidencia como soporte de este control.
5	5.1 Liderazgo y compromiso	Se evidencio y se observo, que la alta dirección demuestra liderazgo y compromiso frente al Sistema de Gestión de Seguridad de la Información, apoyando al establecimiento de la política de seguridad, los objetivos, los requisitos, la comunicación asertiva, entre otros. Evidencia: Aprobación de la política de seguridad, contrataciones, mesas de trabajo, entre otros.
6	5.2 Política	Se evidencio que el Sistema de Gestión de Seguridad de la Información cuenta con una política de seguridad, donde se puede establecer que es adecuada frente a los propósitos de la entidad – AGR, donde se incluye los objetivos, los requisitos y la mejora continua, también se identifica que esta documentada y disponible. Dentro de las diferentes entrevistas se pudo evidenciar que los colaboradores reconocen, ubican y comprenden la importancia de la política.

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		Evidencia: Políticas de Seguridad de la Información y Protección de Datos Personales (publicada en la web). TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
7	A.5.15 Control de acceso	Se evidencio que se han establecido normas a nivel de políticas y buenas practicas para el control de acceso físico y lógico para el aseguramiento de los requisitos de la seguridad de la entidad (AGR) y de lainformación. Evidencia: Observación en sitio, políticas de seguridad de la información, procedimientos y entrevistas.
8	A.5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información	Se evidencio que no se han materializado riesgos asociados a la falta de incumplimiento de las políticas de seguridad de la información y no se han presentado incidentes de seguridad que comprometan los requisitos establecidos en el Sistema de Gestión de Seguridad de la Información. Evidencia: Políticas de seguridad de la información, procedimientos, entrevistas, entre otros.
9	A.5.4 Responsabilidades de la dirección	Se evidencio las responsabilidades de la alta dirección y el compromiso, establecidos en la política de seguridad de la información, en la participación activa con los procesos, en la comunicación asertiva en las diferentes sensibilizaciones y campañas de seguridad y con los requisitos contractuales de los colaboradores. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Socialización AGR MSPI.
10	5.3 Roles, responsabilidades y autoridades de la organización	Se evidencio que la alta dirección asigno las responsabilidades con la finalidad de implementar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI), para el cumplimiento de los requisitos y a su vez que estos comuniquen a la alta dirección sobre el desempeño del SGSI. Evidencia: Comité Institucional de Gestión y DesempeñoAGR-CIGD-10-23-OP-ACTA DE SESION 9 20-06-2023, TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, TI.120.P08.A04 Matriz RACI – Modelo de Seguridad y Privacidad de la Información – MSPI.
11	A.5.2 Roles y responsabilidades en la seguridad de la información	Se evidenció en la "TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0". los roles, responsabilidades para la seguridad de la información y la segregación de funciones. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0
12	A.5.9 Inventario de información y otros activos asociados	Se evidencio que el acta de comité institucional de gestión y desempeño No. 9 - 2023, con fecha del 20 de junio de 2023, se contemplo llevar a cabo la actividad asociada a la identificación y clasificación de los activos de información, se evidencio el inventario de activos de información cuenta con los criterios de Confidencialidad, Integridad y Disponibilidad de la información, así como la clasificación respectiva sobre información pública, información pública clasificada e información pública reservada, actualizado una vez al año. Evidencia: Procedimiento Activos de Información, Guía diligenciamiento Activos y formato Identificación Activos de Información y el TI.120.P09.A01 Consolidado Identificación de los Activos de Información.
13	A.5.10 Uso	Se evidenció que los activos de información de los servidores públicos se establece de

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
	aceptable de la información y otros activos asociados	acuerdo a sus funciones y responsabilidades y para los contratistas y/o proveedores para la ejecución de las funciones y obligaciones durante la relación laboral, dando cumplimiento a los requisitos establecidos en las políticas y demás directrices de seguridad de la información. Evidencia: TI.120.P09.I01 Instructivo Gestión de Activos de Información, TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
14	A.5.11 Devolución de activos	Se evidenció que todos los servidores públicos, contratistas y proveedores deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su contrato y/o cada vez que el mismo haga cambio de oficina o responsabilidades al interior de la Secretaría General. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
15	A.5.12 Clasificación de la información	Se evidenció que aplican lineamientos y procedimientos adecuados para identificar y clasificar los activos de información según los criterios de la confidencialidad, integridad y disponibilidad de la información, para poder determinar su nivel de criticidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Procedimiento Gestión de Activos de Información, Guía diligenciamiento de Activos de Información y TI.120.P09.A01 Consolidado Identificación de los Activos de Información.
16	A.5.13 Etiquetado de la información	Se evidenció que de acuerdo a la criticidad de la información se establecen lineamientos y controles que permiten identificar su nivel de criticidad. Y con el apoyo de gestión documental se articula la actividad con la finalidad de identificar y clasificar la información. Evidencia: TI.120.P09.A02 Requerimientos de Seguridad para Activos, TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
17	6.1.1 Acciones para abordar los riesgos y las oportunidades: Generalidades	Se evidenció que desde el contexto y la identificación de las partes interesadas, con respecto a las necesidades, cumplimiento y posibles desviaciones de los objetivos, se han implementado varios controles que permiten abordar los riesgos y de acuerdo a sus resultados evaluar la eficacia de los controles. Evidencia: Documento, contexto grupo de interés, requisitos, TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, EV.130.P13 Instructivo Valoración de Riesgos y Planes de Acción MSPI, EV.130.P13 Consolidado Valoración de Riesgos y Planes de Acción MSPI.
18	6.1.2 Acciones para abordar los riesgos y las oportunidades: Evaluación de riesgos de seguridad de la información	Se evidencio que para el SGSI se definió e implemento el proceso de evaluación de los riesgos asociados a la seguridad de la información y estos seencuentran documentados. Evidencia: EV.130.P13 Instructivo Valoración de Riesgos y Planes de Acción MSPI, EV.130.P13 Consolidado Valoración de Riesgos y Planes de Acción MSPI.
19	6.1.3 Acciones para abordar los riesgos y las oportunidades:	Se evidencio que para el tratamiento de los riesgos de seguridad de la información el comité institucional de gestión y desempeño No. 9 - 2023, con fecha del 20 de junio de 2023, se contemplo llevar a cabo la actividad. También se evidenció en el documento: EV.130.P13 Instructivo Valoración de Riesgos y Planes de Acción MSPI, las opciones

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
	Tratamiento de los riesgos de la seguridad de la información	de tratamiento de los riesgos de seguridad de la información, la la valoración y los tratamientos de riesgos "EV.130.P13 Consolidado Valoración de Riesgos y Planes de Acción MSPI". Evidencia: TI.120.P08.F04 Declaración de Aplicabilidad, documento del comité institucional de gestión y desempeño No. 9 – 2023, EV.130.P13 Instructivo Valoración de Riesgos y Planes de Acción MSPI, Matriz de excel "EV.130.P13 Valoración riesgos de Activos de Información Auditoría Vigilancia.
20	6.2 Objetivos de seguridad de la información y planificacion para alcanzarlos	Se evidencio que establecieron los objetivos de seguridad de la información y que son acordes con la política de seguridad de la información, estos se encuentran disponibles como información documentada. Los objetivos fueron comunicados al momento de sensibilizar las políticas de seguridad, puesto que están inmersos en ella. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0 - 5. Objetivos del Modelo de Seguridad y Privacidad de la Información.
21	6.3 Planificacion de los cambios	Se evidencio que cuentan con una matriz de control, para la implementación del Sistema de Gestión de Seguridad de la Información, donde se describen las actividades planeadas para el año vigente. Evidencia: TI.120.F08.F03 Hoja de Ruta Implementación Modelo de Seguridad y Privacidad de la Información con fecha del 15/06/2023, versión 1.0.
22	A.5.8 Seguridad de la Información en la gestión de proyectos	Se evidencio que por política se encuentra establecida la seguridad de la información en los proyectos, adicionalmente para los proyectos que se denominen estratégicos y/o sean prioritarios, y/o impacten los procesos de la Entidad y/o la actualización, y/o desarrollo y/o implementación de un nuevo sistema de información, se deben asegurar que los riesgos de Seguridad de la Información asociados a éstos, sean gestionados, usando una combinación de controles automáticos y manuales. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, TI.120.P05 Procedimiento Desarrollo de Software.
23	8.1 Planificación y control de la operación	Se evidenció que cuentan con un plan de seguridad digital, seguridad y privacidad de la información. Se identificó en la planificación y gestión el diagnostico, estructuración, actividades previas al plan, los planes, riesgos, cambios, auditoría, mediciones, entre otros. Evidencia: Plan de Seguridad Digital, Seguridad y Privacidad de la Información, Ver. 1.0 con fecha del 15/06/2023, TI.120.P08.F03 Hoja de Ruta Implementación Modelo de Seguridad y Privacidad de la Información, TI.120.P08.P Procedimiento de Seguridad y Privacidad de la Información.
24	8.2 Evaluación de los riesgos para la seguridad de la información	Se evidenció en la matriz de riesgos "EV.130.P13 Valoración riesgos de Activos de Información Auditoría Vigilancia", no cuenta con riesgos que requieran planes de tratamiento según la clasificación establecida "Catastrófico o Mayor". Y cuentan con una declaración de aplicabilidad, donde se evidencia que no se omite ningún control y que todos los controles se encuentran justificados. Evidencia: Instructivo Valoración de Riesgos y Planes de Acción MSPI, Matriz de excel "EV.130.P13 Valoración riesgos de Activos de Información Auditoría Vigilancia.
25	8.3 Tratamiento de riesgos de seguridad de la información	Se evidenció en la "TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0". se establece que se deben Gestionar los riesgos de Seguridad y Privacidad de la Información identificados en la Entidad. Respecto al proceso auditor el plan de tratamiento del riesgo en este momento no ha sido necesario su gestión dado

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		que no se ha presentado ningún riesgo de información asociado al proceso. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Instructivo Valoración de Riesgos y Planes de Acción MSPI, Matriz de excel "EV.130.P13 Valoración riesgos de Activos de Información Auditoría Vigilancia.
26	7.1 Recursos	Se observo que la AGR proporciona recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información. Se evidencian recursos como: personal, controles tecnológicos, controles físicos, contatos a nivel de servicios, tecnología en seguridad, entre otros. Evidencia: AGR-CIGD-10-23-OP-ACTA DE SESION 9 20-06-2023.
27	9.1 Seguimiento, medición, análisis y evaluación	Se evidencio que realizan seguimiento, medición, análisis y evaluación, se pudo observar que tienen establecidos diferentes indicadores de medición, donde se puede evidenciar que estas mediciones cuentan con el soporte o el insumo. También se evidenciaron las métricas establecidas para determinar el indicador. Evidencia: Indicadores MSPI 2023, Seguimiento Indicadores MSPI Agosto 2023. Herramienta de Autodiagnostico del Modelo de Seguridad y Privacidad de la Información.
28	9.2.1 Auditoría interna: Generalidades	Se observo dentro del Plan de Seguridad Digital, Seguridad y Privacidad de la Información, TI.120.P08.A01, Versión 1.0, con fecha del 15/06/2023, llevar a cabo la ejecución de las Auditorías Internas. Se puede evidenciar con base a los documentos desarrollados en esta actividad el cumplimiento del requisito al control. Evidencia: Plan de Seguridad Digital, Seguridad y Privacidad de la Información, TI.120.P08.A01, Versión 1.0, con fecha del 15/06/2023. Procedimiento evaluación, control y mejora EV. 130.P12.P, con fecha del 19/09/2023 Versión 4.8.
29	9.2.2 Auditoría interna: Programa de auditoría interna	Se realizo el programa de auditoria interna, se estableció el alcance, el cumplimiento de los requisitos de seguridad de la información, basados en la norma ISO/IEC 27001:2022 al Sistema de Gestión de Seguridad de la Información. Se puede evidenciar con base a los documentos desarrollados en esta actividad el cumplimiento del requisito al control. Evidencia: Procedimiento evaluación, control y mejora EV. 130.P12.P, con fecha del 19/09/2023 Versión 4.8. EV.130.P12.F02_Formato Plan de visitas, EV.130.P12.F03_Formato Cronograma de auditoria, EV.130.P12.F04_Formato Lista Verificación, EV.130.P12.F11 Declaración de Independencia y Cumplimiento de Compromisos Éticos, con fecha del 19/09/2023, Versión 1.0.
30	A.5.35 Revisión independiente de la seguridad de la información	Se evidenció se revisan los sistemas de información de manera regular en cada vigencia para el cumplimiento con los estándares de implementación de la seguridad. Con relación a los procedimientos relacionados con el análisis, desarrollo y mantenimiento de las aplicaciones, se realizan revisiones técnicas con lo cual se determina el incumplimiento de los controles establecidos para tomar acciones de mejora sobre éstos. Se realizó la auditoría interna bajo el acompañamiento de un auditor líder externo y bajo el acompañamiento de auditores internos de control interno. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Procedimiento evaluación, control y mejora EV. 130.P12.P, con fecha del 19/09/2023 Versión 4.8. EV.130.P12.F02_Formato Plan de visitas, EV.130.P12.F03_Formato Cronograma de auditoria, EV.130.P12.F04_Formato Lista Verificación, EV.130.P12.F11 Declaración de Independencia y Cumplimiento de Compromisos Éticos, con fecha del 19/09/2023, Versión 1.0.

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
31	A.5.31 Requisitos legales, legales, reglamentarios y contractuales	Se evidenciaron los requisitos legales, reglamentarios y contractuales que se tienen establecidos en el Sistema de Gestión de Seguridad de la Informacón. Evidencia: Normograma de los Procesos del Sistema de Gestión de la Calidad de la Auditoría General de la República, Ver. 2.4, con fecha 05/07/2022, TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
32	A.5.32 Derechos de propiedad intelectual	Se evidenció en la Política de Seguridad el cumplimiento adecuado a la legislación vigente y/o requisitos legales aplicables (derechos de propiedad intelectual, protección de registros, privacidad y protección de la información de datos personales, reglamentación de controles criptográficos) relacionados con seguridad de la información. Se evidencio de que se definen, documentan y actualizan todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la Entidad que son relevantes para cada sistema de información al menos una vez al año y/o cada vez que estos sean requeridos. Se asegura que el software que se instala y se utiliza en la Entidad cumple con los requisitos de derechos de autor, licenciamiento de uso y es original. La Oficina Jurídica y/o el Grupo de Tecnologías y Sistemas de Información establecen en los contratos cláusulas donde se obligue a no divulgar la información restringida o confidencial de la Entidad, a su vez a utilizar la información únicamente para el desarrollo el objeto del contrato Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, verificación física de algunas licencias de los sistemas operativos y de aplicaciones.
33	A.5.34 Privacidad Y protección de la información de identificación personal (PII, por sus siglas en ingles)	Se evidenció que la Entidad identifica, obedece y da cumplimiento de acuerdo a la Ley de Protección de Datos Personales en Colombia. Evidencia: Política rara El Tratamiento De Datos Personales Auditoría General De La República", Ver. 1.0, con fecha del 15/06/2023, TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, https://www.auditoria.gov.co/documents/.
34	A.5.5 Contacto con las autoridades	Se evidencio que para los temas pertinentes de la seguridad de la información identifican y establecen los lineamientos para mantener y acudir si es necesario a las autoridades pertinentes. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0
35	A.5.6 Contacto con grupo de interés especial	Se evidenció que la AGR tiene contacto con los grupos de interés, asociados a la seguridad de la información e identifica los diferentes canales de comunicación, como por ejemplo con, CCOC, CAI Virtual, MINTIC, entre otros. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
36	7.2 Competencia	Se evidenció que la entidad valida las competencias necesarias de las personas que realizan actividades para el aseguramiento de la información, basados en la educación, formación y experiencia. El Manual Específico de Funciones y Competencias Laborales adoptado mediante Resolución Reglamentaria No. 007 del 4 de noviembre de 2021 señala los requisitos de cada uno de los empleos y las competencias generales de los servidores públicos y por cada nivel jerárquico. De conformidad con la hoja de vida

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		presentada con todos los soportes por el aspirante, verifican el cumplimiento para el empleo frente a los requisitos del Manual Específico de Funciones y Competencias Laborales. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, . El Manual Específico de Funciones y Competencias Laborales adoptado mediante Resolución Reglamentaria No. 007 del 4 de noviembre de 2021. https://www. auditoria.gov.co/web/guest/auditoria/talento-humano/manual-de-funciones.
37	A.6.1 Selección	Se evidenció que para los servidores públicos, la obligación se encuentra de acuerdo con la posesión de cargo y de acuerdo con lo establecido por la Dirección de Talento Humano, teniendo en cuenta que las oficinas gestoras son las responsables de elaborar los estudios y documentos previos, adicionalmente de preparar el certificado de idoneidad en donde se evalúan los antecedentes. Posterior a ello toda la documentación es remitida a la Oficina Jurídica para su revisión y análisis legal y en el evento de encontrar inconsistencias se devuelven a la oficina de gestora para subsanar o se redacta el clausulado del contrato. Para los empleados de carrera administrativa ingresaron por concurso de méritos realizado por la CNSC. Para el caso de los empleados de libre nombramiento y remoción y provisionales se revisan las hojas de vida frente al Manual de Funciones. Antes del ingreso se revisan antecedentes disciplinarios, fiscales, judiciales y medidas correctivas en las respectivas plataformas de cada entidad. Evidencia: TH.232.P1 Provisión de cargos de libre nombramiento y remoción carrera administrativa y provisionalidad, TH.232.P21 Retiro, traslado, reubicación o permuta de funcionarios. GJ.110.P14.P Procedimiento de contratación.
38	A.6.2 Términos y condiciones de empleo	Se evidenció que todos los servidores públicos, contratistas y proveedores ya sean nuevos o antiguos deben recibir el apropiado conocimiento y capacitación en temas de Seguridad y Privacidad de la Información, Protección de Datos Personales, una vez al año y/o cuando se considere necesario y sea definido en conjunto entre la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y la Dirección de Talento Humano o por separado. En materia contractual, la minuta de contrato de prestación de servicios incorpora cláusulas atinentes a las responsabilidades en materia de la seguridad de la información. Así mismo, el Grupo TIC que hace parte de la Oficina de Planeación, a través de la intranet y en mesas de trabajo periódicas con los representantes de cada dependencia capacitan y empoderan a funcionarios y contratistas en la importancia de la seguridad de la información que se maneja en la AGR. Evidencia: TH.232.P3 Asignación de Funciones en el formato TH.232.P03.FI01_Formato Resolución asignación de funciones. TH.232 Memorando de comunicación de funciones. GJ.110.P14.P Contratación en el formato GJ.110.P14.F23 Formato de Acta de Inicio. Acuerdo de Confidencialidad y Reserva de Manejo de Información entre la Auditoría General de la República – AGR y Funcionarios Públicos. Ver. 1.0. Fecha 15/06/2023. TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
39	A.6.4 Proceso disciplinario	Se evidenció que se encuentra establecido un procedimiento donde se establece que los servidores públicos de la Entidad cuando incurran en alguna falla que incurra o atente contra la Confidencialidad, Integridad y Disponibilidad de los datos, información, activos de información que se encuentren asignados para el desarrollo de las funciones y responsabilidades asignadas, se les aplicará lo indicado en el documento GJ.110.P13.P Procedimiento para investigar la conducta de los sujetos disponibles

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		dentro de la AGR a través del documento GJ.110.P13.F01_Formato Control Procesos Disciplinarios.pdf. Evidencia: GJ.110.P13.P Procedimiento para investigar la conducta de los sujetos disponibles dentro de la AGR a través del documento GJ.110.P13.F01_Formato Control Procesos Disciplinarios.pdf. TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
40	A.6.5 Responsabilidades después de la terminación o cambio de empleo	Se evidenció que las personas que culminan la ejecución de un contrato, deben cumplir con la «obligación especial de confidencialidad» que señala: «Esta obligación se prolongará incluso después de finalizado el servicio por el término de dos (2) años, contados a partir de la terminación de cualquier relación contractual entre las partes. EL CONTRATISTA, antes o después de la vigencia del contrato, se considerará recibida con carácter de confidencialidad y será obligación EL CONTRATISTA utilizarla sólo para los propósitos de la prestación del servicio y dentro de los límites que le impone el desarrollo del objeto contractual.» En todo caso, corresponde al supervisor de cada contrato el establecer si pueden existir responsabilidades en materia de la seguridad de la información por parte de contratistas. Para el caso de funcionarios, corresponde a la Dirección de Talento Humano en conjunto con el Grupo TIC establecer las responsabilidades en esta materia. Evidencia: TH.232.P21 Retiro, traslado, reubicación o permuta de funcionarios, TH.232.P21.FI13_Formato Retiro o Traslado, TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
41	A.6.6 Acuerdos de confidencialidad o no divulgación	Se evidenciaron los acuerdos de confidencialidad para el manejo y no divulgación de los datos e información que se conocen a través del desarrollo de las funciones y actividades se establece con la firma y aceptación de conocimiento y la respectiva política de seguridad y privacidad de la información que se encuentran relacionadas en los acuerdos de confidencialidad para servidor público y contratista. Los funcionarios cuentan un acuerdo de confidencialidad y reserva de manejo de información con la AGR aspecto que puede ser verificado con la Dirección de Talento Humano. Respecto de contratistas, en los clausulados se incorporan obligaciones sobre confidencialidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Acuerdo de Confidencialidad y Reserva de Manejo de Información entre la Auditoría General de la República – AGR.
42	A.6.3 Conciencia de Seguridad de la información, educación y formación	Se evidenció que la AGR que sensibiliza y apropia la gestión de Seguridad y Privacidad de la Información en los servidores públicos, contratistas y proveedores de la Entidad. Y que se verifica el cumplimiento de las políticas, procesos, procedimientos, instructivos y anexos que integran el Sistema de Gestión de Seguridad de la Información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Acta de comité institucional de gestión y desempeño No. 9 - 2023, con fecha del 20 de junio de 2023.
43	7.3 Toma de conciencia	Se evidencio que el acta de comité institucional de gestión y desempeño No. 9 - 2023, con fecha del 20 de junio de 2023, se contemplo llevar a cabo la actividad de sensibilización: se evidenció que en la planeación y hoja de ruta del Plan de SPI. En las diferentes entrevistas se pudo evidenciar que se llevaron las sensibilizaciones y que los colaboradores entendieron el concepto de dicha sensibilización. Se evidenció que la política de seguridad, establece que se debe sensibilizar y apropiar la gestión de Seguridad y Privacidad de la Información en los servidores públicos,

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		contratistas y proveedores de la Entidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Acta de comité institucional de gestión y desempeño No. 9 - 2023, con fecha del 20 de junio de 2023. Socialización - AGR – MSPI julio 2023.
44	7.4 Comunicación	Se evidencia que la AGR identifica a nivel interno y externo a quien debe comunicar, cuando debe comunicar, con quien debe comunicarse dependiendo de la necesidad o de la afectación a la Seguridad de la Información, como por ejemplo: al momento que se presente un incidente de seguridad o se identifique un riesgo de seguridad Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Indagación en las entrevistas con los auditados.
45	7.5.1 Información documentada: Generalidades	Se evidencio que la entidad cuenta con la información documentada requerida y necesaria para el Sistema de Gestión de Seguridad de la Información, como la Política de Seguridad de la Información, Procedimientos, Guias, Matrices de Activos y Riesgos, Formatos, Indicadores, Acuerdos de Confidencialidad, Instructivos, entre otros. Evidencia: Política de Seguridad de la Información, Procedimientos, Guias, Matrices de Activos y Riesgos, Formatos, Indicadores, Acuerdos de Confidencialidad, Instructivos, entre otros.
46	7.5.3 Información documentada: Control de la información documentada	Se evidencio que la información o los documentos asociados al Sistema de Gestión de Seguridad de la Información, están disponibles para su uso, esta protegida a nivel de confidencialidad, integridad y disponibilidad y cuenta con control de cambios. Evidencia: Política de Seguridad de la Información, Procedimientos, Guias, Matrices de Activos y Riesgos, Formatos, Indicadores, Acuerdos de Confidencialidad, Instructivos, entre otros.
47	A.5.37 Procedimientos operativos documentados	Se evidencio que se tienen procedimientos operativos documentados y no documentados para la seguridad de la información. Evidencia: TI.120.P06.P Procedimiento Respaldo (backup) de información de los servidores y bases de Datos de la AGR, TI.120.P05.P Procedimiento desarrollo de software, TI.120.P04.P_Procedimiento Gestión de Cambios, TI.120.P03.P_Procedimiento Atención de usuarios de la plataforma tecnológica, TI.120.P01.P_Procedimiento Administración de la Infraestructura tecnológica.
48	A.7.1 Perímetros de seguridad física	Se evidenció en los centros de cableado, data center y cuartos técnicos por politica deben permanecer cerrados y con acceso restringido para personal no autorizado. El centro de datos ubicado en el piso 17 cuenta con control de acceso biométrico (lector de huella) y el del piso 18 cuenta con acceso por medio de llaves. Las personas deben contar con el permiso del Asesor de Despacho – Coordinador TIC, así mismo, las personas que llevan a cabo labores de aseo en las oficinas ingresan acompañados durante el tiempo que dure la labor de aseo en el Centro de Datos. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones del piso 17 y piso 18.
49	A.7.2 Entrada física	Se evidencio dentro de las instalaciones que los accesos físicos perimetrales son controlados, puesto que cuenta con diferentes niveles de seguridad, para el acceso a las instalaciones se debe reportar y toman los datos de las personas, así como la foto de la persona que va a ingresar. también confirman con el personal de la AGR para verificar que si le permiten el acceso, cuentan con guardas de seguridad y escaneo de cedulas. Una vez en el piso se identifica que las puertas cuentan con seguridad y no es

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		de libre acceso, por lo que el control es eficiente, al ingresar a la oficina siempre esta la persona acompañada por un colaborador, hasta el punto de salida del piso. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones del piso 17 y piso 18.
50	A.7.3 Asegurar oficinas, habitaciones e instalaciones	Se evidencio que la Entidad cuenta con el establecimiento y asignación de permisos de acceso a las oficinas, salas de capacitación y similares únicamente a los servidores públicos, contratistas y proveedores autorizados para su acceso. Estos accesos se realizan a través de la asignación de la respectiva tarjeta de proximidad entregada al ingreso a la Entidad. De igual forma, en caso de visitantes, solo tendrán acceso a las zonas comunes y permanecen en compañía de un servidor o contratista. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones.
51	A.7.4 Monitoreo de la seguridad física	Se observo, que los accesos físicos perimetrales son controlados, puesto que cuenta con diferentes niveles de seguridad, para el acceso a las instalaciones se debe reportar y toman los datos de las personas, así como la foto de la persona que va a ingresar. también confirman con el personal de la AGR para verificar que si le permiten el acceso, cuentan con guardas de seguridad y escaneo de cedulas. Una vez en el piso se identifica que las puertas cuentan con seguridad y no es de libre acceso, por lo que el control es eficiente, al ingresar a la oficina siempre esta la persona acompañada por un colaborador, hasta el punto de salida del piso. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, centros de datos (Datacenter), cuartos técnicos, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, son áreas de acceso restringido y en consecuencia cuentan con control biométrico (lector de huella). Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones.
52	A.7.5 Protección contra amenazas físicas y ambientales	Se evidencio que la Entidad cuentan con mecanismos adecuados contra las amenazas ambientales (temperatura, humedad, fuego, etc.), y se encuentran protegidos con UPS de respaldo para sostener la operación de la Entidad. También están establecidas en la política de seguridad: Se evidenció que en la política de seguridad, se determina que no se permite albergar, mantener y/o guardar elementos inflamables dentro de las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones.
53	A.5.5 Contacto con las autoridades	Se evidenció que en la política de seguridad, se establece la relación cercana con Entidades de Prevención y Atención de Emergencias tanto territoriales como nacionales, así como con grupos de interés o foros de especialistas en seguridad digital, seguridad y privacidad de la información, para que puedan ser contactados de manera oportuna en caso de que se presente un evento/incidente de seguridad digital, seguridad y privacidad de la información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
54	A.5.6 Contacto con grupo de interés especial	Se evidencio que la entidad tiene identificado y definido los grupos de interés, pertinentes para el aseguramiento de la información, como por ejemplo: ColCert: Grupo de Respuesta a Emergencia Cibernéticas de Colombia. www.colcert.gov.co – CCOC: Comando Conjunto Cibernético. CSIRT: Centro de Coordinación Seguridad Informática Colombia. www.csirt-ccit.org.co. Centro Cibernético Policial (CAI Virtual): Ciberseguridad en Colombia comandado por la Policía Nacional. www.policia.gov.co. MINTIC: Ministerio de las Tecnologías y las Comunicaciones www.mintic.gov.co. Comando Conjunto Cibernético – CCOC: Grupo que dirige las mesas de trabajo para garantizar la seguridad de las infraestructuras críticas del país ante cualquier eventualidad al correo atencionalciudadano@cgfm.mil.co. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
55	A.5.7 Inteligencia de amenazas	Se evidenció que la Auditoría General de la República – AGR se encuentra inscrita a los boletines de seguridad que permiten tener visibilidad de los eventos de seguridad reportados por dichas entidades y que seran redirigidos a la persona / equipo responsable del análisis, escalamiento y definición de acción según aplique. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
56	A.6.8 Informes de eventos de seguridad de la información	Se evidenció que es responsabilidad de todos los servidores públicos, contratistas y proveedores de la Auditoría General de la República – AGR reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los activos de información que se presente en la Entidad a través del Centro de Atención al Usuario (CAU). Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Entrevistas.
57	A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información	Se evidenció que en la política de seguridad, se establece que la atención y gestión de los incidentes reportados a través del CAU se realiza de acuerdo con lo establecido en el documento Guía Gestión de Incidentes con la que cuenta la Entidad. Cuentan con las categorías de los incidentes de seguridad y conforme a la criticidad, se establecen los mecanismos de atención adecuados para su solución. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Guía de gestión de incidentes de seguridad de la información Ver. 2.0, del mes de septiembre de 2023.
58	A.5.25 Evaluación y decisión sobre eventos de seguridad de la información	Se evidenció que el CAU se encuentra disponible para el reporte formal de eventos que son reportados por los servidores públicos, contratistas y proveedores que sean posiblemente sospechosos de incidentes de seguridad y privacidad de la información para ser registrado en la respectiva herramienta de gestión y escalado al Oficial de Seguridad de la Información (o quien haga sus veces) de la Entidad. Todos los servidores públicos, contratistas y proveedores de la Entidad conocen que deben realizar el reporte de eventos posiblemente sospechosos como incidentes de seguridad y privacidad de la información a través del CAU directamente por la herramienta de gestión o por medio de la cuenta de correo: centrodeservicio@auditoria.gov.co. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Guía de gestión de incidentes de seguridad de la información.
59	A.5.26 Respuesta a incidentes de seguridad de la	Se evidenció que cuando se realiza el escalamiento, atención y contención del incidente de información reportado a través del CAU, éste se realizará bajo los parámetros establecidos en el documento Guía Gestión de Incidentes con el cual cuenta la Entidad.

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
	información	Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Guía de gestión de incidentes de seguridad de la información.
60	A.5.27 Aprender de los incidentes de seguridad de la información	Se evidenció que a nivel de Política de Seguridad Digital Seguridad y Privacidad de la información se establece que se toman acciones correctivas oportunas ante los eventos e incidentes de seguridad reportados, con base en el aprendizaje obtenido en la gestión de incidentes de seguridad en la Entidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Guía de gestión de incidentes de seguridad de la información.
61	A.5.28 Recopilación de evidencias	Se evidenció a nivel de la Política de Seguridad Digital Seguridad y Privacidad de la información, se establece que mantienen las evidencias necesarias para establecer el reporte del incidente de seguridad para toda acción de seguimiento contra una persona y/o Entidad. Así mismo se cuenta con los soportes que sean exigidos por una acción legal (sea civil o criminal). Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Guía de gestión de incidentes de seguridad de la información.
62	A.5.29 Seguridad de la información durante una interrupción	Se evidencio la documentación pertinente a la seguridad de la información y la planeación frente algún evento que pueda afectar la interrupción o la disponibilidad. El Grupo de Tecnologías y Sistemas de Información cuenta con el respectivo registro en la herramienta de gestión del CAU en donde se encuentra el detalle de la detención, contención, erradicación y recuperación en la Entidad y de acuerdo con la Estrategia de Respuesta y Recuperación realiza las actividades de implementación de la misma para las aplicaciones y servicios TI que soportan la continuidad de los procesos misionales de la Entidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Plan Recuperación de Desastres, TI.120.P01.A05_Anexo 5 Plan de Recuperación.
63	A.5.30 Preparación de las TIC para la continuidad de negocio	Se evidenció en el Plan de Recuperación de Desastres, la adaptación de los controles de seguridad de la información durante la interrupción de las operaciones. El plan de Recuperación de Desastres, se evidencia que realiza la identificación de los procesos críticos de la Entidad, llevando a cabo un análisis de impacto para determinar los procesos y procedimientos más relevantes para la continuidad del negocio. Basado en el análisis de impacto, se define la estrategia de respuesta y recuperación para los procesos / servicios TI más relevantes para la continuidad del negocio y cumplimiento de la misionalidad de la Entidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Plan Recuperación de Desastres, TI.120.P01.A05_Anexo 5 Plan de Recuperación.
64	A.5.14 Transferencia de información	Se evidenció la política para la transferencia de información, donde se establece que se firmarán acuerdos de confidencialidad con los servidores públicos, contratistas, proveedores, entidades y ciudadanos que por diferentes razones requieran conocer o intercambiar información restringida y/o confidencial de la Entidad. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información. Los propietarios de la información que se requiera intercambiar son responsables de definir los niveles y perfiles de autorización para el acceso, modificación y eliminación.

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Plan Recuperación de Desastres, TI.120.P01.A05_Anexo 5 Plan de Recuperación.
65	A.5.16 Gestión de identidades	Se evidenció que todos los sistemas de disponibilidad crítica o media de la Entidad cuentan con reglas de acceso las cuales cuentan con segregación de funciones entre quien las administra, opera, realiza mantenimiento y audita. Las solicitudes de creación de usuarios para servidores públicos, contratistas y/o proveedores se realizará a través de una solicitud radicada ante el CAU con el documento remitido por la Dirección de Talento Humano o Supervisor de contrato previamente firmada por el jefe directo. Cuando el usuario solicita el cambio de la contraseña y se encuentre fuera del dominio o la red, lo realiza a través de solicitud al CAU para una nueva asignación de contraseña y esta se envía por medio de la herramienta establecida, la cual cuenta con la opción privado, y es sólo visualizada por el usuario solicitante. Se identifica que el grupo de Tecnologías de Información lleva el respectivo registro de cuentas de usuarios en donde se vincula o se identifica al usuario (a través del Directorio Activo). Para los casos de retiro de la Entidad se desactiva con la notificación de la Gerencia de Talento Humano o de la Oficina Jurídica. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
66	A.5.17 Información de autenticación	Se evidenció en la Política de Seguridad Digital Seguridad y Privacidad de la información el control para la autenticación y los accesos, también se evidenciaron las responsabilidades de la administración, los lineamientos establecidos para otorgar permisos según el nivel de clasificación de la información. Toda asignación de permisos de acceso cuenta con previa autorización del jefe, de área la oficina responsable y se soporta a través de la herramienta que gestiona y administra el CAU. Para servidores públicos mientras que para los contratistas o proveedores será solicitado por el supervisor designado para el contrato. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. GJ.110.P13.F01_Formato Control Procesos Disciplinarios.pdf. GJ.110.P13.F01_Formato Control Procesos Disciplinarios.pdf.
67	A.6.7 Trabajo remoto	Se evidenció que cuentan con una política para teletrabajo, se identifica que establecen parámetros de seguridad a nivel de seguridad física, lógica y los respectivos permisos. El teletrabajador debe realizar la conexión a través del canal VPN autorizado para acceder a los datos, información, aplicativos web y servicios de nube de la Entidad de una manera segura y conexión privada y a través del equipo asignado por ésta. Las medidas de control y seguridad de la información que se implementen para el trabajo remoto son responsabilidad de la Oficina de Planeación. En lo que tiene que ver con el control del trabajo y cumplimiento de las funciones por parte de los funcionarios la herramienta colaborativa Office 365 (Teams, Outlook, chat, llamadas, videollamadas, entre otros) será el principal canal de comunicación entre el jefe de la dependencia y los funcionarios así como el celular en horario laboral. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
68	A.5.18 Derechos de acceso	Se evidenció la política para el control de acceso, donde se establece que todos los sistemas de disponibilidad crítica o media de la Entidad, cuentan con reglas de acceso las cuales cuentan con segregación de funciones entre quien las administra, opera,

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		realiza mantenimiento y audita. Todos los servidores públicos, contratistas y proveedores son responsables de proteger la información a la cual acceden y procesan, para evitar su pérdida, alteración, destrucción o uso indebido. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Procedimiento TI.120.P1 Administración de la Infraestructura tecnológica.TH.232.P21.FI13_Formato Retiro o Traslado en el cual se oficializa la finalización del contrato del funcionario.
69	A.8.2 Derechos de acceso privilegiado	Se evidenció que los funcionarios que tienen acceso a: datos e información, infraestructura tecnológica, aplicaciones, bases de datos y sistemas de información, deben contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y privilegios establecidos sobre los activos de información que almacenan los datos e información, con el objeto de minimizar el uso o modificación no autorizada sobre los activos de información de la Entidad. Y que todos los sistemas de disponibilidad crítica o media de la Entidad cuentan con reglas de acceso las cuales cuentan con segregación de funciones entre quien las administra, opera, realiza mantenimiento y audita. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
70	A.8.3 Restricción de acceso a la información	Se evidenció que cuentan con una política para el control de acceso y que en ella están las responsabilidades de la administración, los lineamientos establecidos para otorgar permisos según el nivel de clasificación de la información. Y los servidores públicos que en ejercicio de sus labores tengan acceso a: datos e información, infraestructura tecnológica, aplicaciones, bases de datos y sistemas de información, deben contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y privilegios establecidos sobre los activos de información que almacenan los datos e información, con el objeto de minimizar el uso o modificación no autorizada sobre los activos de información de la Entidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
71	A.8.4 Acceso al código fuente	Se evidenció que los administradores de las plataformas de producción son los responsables de controlar el acceso y uso de los programas fuente de los sistemas y/o de las aplicaciones que operan en ellas, así como de coordinar y/o ejecutar las actualizaciones programadas. El acceso de los servidores públicos, contratistas y proveedores a los sistemas de producción sólo es permitido para realizar labores de soporte o mantenimiento, previa autorización. Cuentan con un control hacia el acceso al código fuente de los programas, sistemas de información y el software desarrollado por la Auditoría General de la República – AGR solo al personal autorizado y así mismo, se lleva el respectivo control de los cambios autorizados y realizados al código fuente de éstos. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. TI.120.P05.A 01 Guía para el desarrollo de software.
72	A.8.5 Autenticación segura	Se evidencio que cuentan con la política de responsabilidades de los usuarios, donde se identifica el buen uso que le deben dar a la información, los servidores públicos, contratistas y proveedores y los controles como por ejemplo, las características definidas en las contraseñas. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		información 2.0.
73	A.8.18 Uso de programas de utilidad privilegiados	Se evidenció que no se tiene permitido el uso de programas utilitarios como: editores, depurador de código y/o programa para recuperar datos perdidos o borrados accidentalmente en el disco duro entre otros sin justificación y autorización expresa por parte del Grupo de Tecnologías y Sistemas de Información. La instalación de cualquier tipo de hardware y/o software en los equipos de escritorio o equipos portátiles de la Entidad es responsabilidad de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y por tanto son los únicos autorizados para llevar a cabo esta labor. A nivel de muetreo se pudo observar, que los computadores y portátiles, tienen aplicaciones utilitarias con licencia libre. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
74	A.5.19 Seguridad de la información en las relaciones con proveedores	Se evidencio que establecen medidas de control de seguridad de la información, específicamente con el acceso de los proveedores a los datos e información de la Entidad. Así mismo, las partes interesadas de la Entidad deben tener conocimiento de sus responsabilidades relacionadas con la seguridad de la información y esta responsabilidad se debe ver reflejada en los contratos que ejecute la AGR. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
75	A.5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores	Se evidencio que las partes interesadas de la Entidad deben tener conocimiento de sus responsabilidades relacionadas con la seguridad de la información y esta responsabilidad se debe ver reflejada en los contratos que ejecute la AGR. Dentro de los acuerdos de servicios con terceras partes se incluye una cláusula la cual autoriza a la Auditoría General de la República – AGR a realizar auditoría para validar los controles utilizados por los terceros para el manejo de la información. La Oficina Jurídica realiza la respectiva identificación y documentación del proveedor con el cual la Entidad tiene o va a tener una relación contractual. Se firman los acuerdos de confidencialidad con relación a transferencias de la información entre la Entidad y terceras partes. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
76	A.5.21 Gestión de seguridad de la información en la cadena de suministro de la tecnología de información y las telecomunicaciones (TIC)	Se evidencio que cualquier acceso por parte de un tercero a los recursos tecnológicos o a la información de la Entidad, debe haber cumplido con las autorizaciones respectivas y además contar con los acuerdos o cláusulas de confidencialidad respectivos. Y que es obligatorio cumplir con lo indicado en la Política para el control de acceso de terceros que hagan parte de la cadena de suministro TIC. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Acuerdo de Confidencialidad y Reserva de Manejo de Información entre la Auditoría General de la República – AGR y Funcionarios Públicos. Ver. 1.0. Fecha 15/06/2023.
77	A.5.22 Seguimiento, revisión y gestión del cambio de los servicios de los	Se evidenció que los supervisores de contrato permiten que los proveedores tengan disponible la información relacionada con el MSPI de la entidad incluidos los procesos y procedimientos para dar cumplimiento de los requisitos de seguridad de la información establecidos. Y a cada proveedor de servicio se le diligencia el documento de Evaluación comportamiento proveedores, a través del cual se realiza el seguimiento y

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
	proveedores	posterior evaluación del servicio prestado por los diferentes proveedores de la Entidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, OI.120.P04.FI04_Evaluación comportamiento proveedores.
78	A.5.23 Seguridad de la información para el uso de servicios en la nube	Se evidenció que la entidad tiene establecido de que los procesos de adquisición, gestión y salida en producción de servicios en la nube, se debe acatar y seguir el Procedimiento Desarrollo de Software y la Guía de Desarrollo de Software en cumplimiento de los requisitos de seguridad de la información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Procedimiento Desarrollo de Software, Guia de Desarrollo de Software.
79	A.5.33 Protección de registros	Se evidenció que los registros de los sistemas y plataformas que soportan las aplicaciones y servicios TI se protegen y almacenan de acuerdo con las reglas de respaldo. Los registros son transferidos a la Plataforma de Monitoreo para la gestión correspondiente de acuerdo con lo definido. Cuentan con la asignación de privilegios correspondiente para el acceso a los sistemas o herramientas de monitoreo que permiten la visualización de registros. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
80	A.7.6 Trabajar en áreas seguras	Se evidenció que las áreas seguras se encuentran delimitadas a través de la designación de los espacios de Centros de Datos y cuartos técnicos o eléctricos en la Entidad, a los cuales sólo se puede acceder mediante la debida autorización por medio de biométrico (lector de huella) o acompañado a cada área designada como segura. Las personas que llegan de visita a las oficinas de la Entidad ubicadas en el Edificio Elemento PH son debidamente anunciadas a través de la oficina de Correspondencia y ésta autoriza el ingreso a las oficinas de acuerdo con la previa autorización del visitado. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones.
81	A.7.8 Emplazamiento y protección de equipos	Se evidenció a nivel de política que se establece que para la protección de los equipos que almacenan o procesan información fuera de las instalaciones de la organización: No dejar el equipo y los medios de almacenamiento sin supervisión en lugar públicos y no protegidos, mantener las condiciones ambientales para proteger el equipo en todo momento (agua, calor, humedad, polvo, campos electromagnéticos fuertes, entre otros), tomar las medidas de protección contra la visualización de información de acceso o información de la Entidad, por parte de personas no autorizadas. Almacenar la información en los repositorios asignados por la Entidad. Reportar de manera inmediata al CAU cualquier novedad / incidente que se presente con el equipo y la información que puede ser accedida a través de él. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
82	A.7.9 Seguridad de los activos fuera de las instalaciones	Se evidenció que los equipos pueden ser trasladados por el servidor público de la Entidad, ya que éstos cuentan al ingreso a la Entidad con una cláusula de responsabilidad con inventarios y los equipos se encuentran amparados con póliza y está asociado al procedimiento de inventarios. También a ivel de control cuentan con acuerdos de confidencialidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Acuerdo de Confidencialidad y Reserva de Manejo de Información

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		entre la Auditoría General de la República – AGR.
83	A.7.10 Medios de almacenamiento	Se evidenció que a través de la consola antivirus, el escaneo de medios removibles que son conectados para la búsqueda de virus o malware en éstos de manera automática. Los servidores públicos, contratistas y proveedores se comprometen a asegurar física y lógicamente el dispositivo a fin de no poner bajo ningún riesgo, la información de la Entidad y los demás activos de información bajo su custodia. Todos los servidores públicos, contratistas y proveedores deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su contrato y/o cada vez que el mismo haga cambio de oficina o responsabilidades al interior de la Secretaría General. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
84	A.7.11 Servicios públicos de apoyo	Se evidenció que los servicios de Centro de Datos cuentan con respaldo de suministro de energía en términos de UPS y Planta Eléctrica, por otra parte la entidad realiza los respectivos análisis de capacidad con los cuales cuentan las UPS cada vez que ingresan nuevos elementos que requieren alimentación de energía. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones (Centro de Datos).
85	A.7.12 Seguridad del cableado	Se evidenció que el cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información permanecen protegidos a través de canaleta para evitar el deterioro y disponibilidad del servicio. Los Centros de Datos, cableado y cuartos técnicos permanecen debidamente asegurados para reducir riesgos por manipulación. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones.
86	A.7.13 Mantenimiento de equipos	Se evidenció que llevan a cabo las actividades de mantenimiento preventivo, también mantienen registros a través del CAU donde se realiza la trazabilidad de las fallas, personas involucradas y actividades desarrolladas. Los respectivos mantenimientos que se realizan a los distintos elementos tecnológicos que soportan las aplicaciones y servicios TI, se realizan acorde con la programación que se maneja en el Grupo de Tecnologías y Sistemas de Información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, TI.120.P03.FI02_Formato Planilla de Registro.
87	A.7.14 Disposición reutilización segura de los equipos	Se evidenció que se establece en la política de seguridad, que todos los equipos que contengan información sensible y/o confidencial en sus medios de almacenamiento deben pasar por un procedimiento de respaldo de la información y posterior borrado seguro de los medios de almacenamiento, que es ejecutado por el Grupo de Gestión TIC antes de su reutilización o finalización de su vida útil. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
88	A.8.1 Dispositivos de punto final usuario	Se evidencio que cuentan con la política de responsabilidades de los usuarios, donde se identifica el buen uso que le deben dar a la información, los servidores públicos, contratistas y proveedores y los controles como por ejemplo, las características definidas en las contraseñas. Los dispositivos que se conecten a la red se acogerán a las políticas y controles establecidos de seguridad de la información definidas en el presente manual. Se restringe la conexión de dispositivos móviles tales como smartphones y/o tablets a las redes principales de la Entidad.

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
89	A.8.6 Gestión de la capacidad	Se evidenció que la entidad establece en la política de seguridad, que es responsabilidad del Grupo de Tecnologías y Sistemas de Información monitorear, revisar, proyectar y dar soporte oportuno para el uso y desempeño aceptable de capacidad sobre la infraestructura tecnológica, realizando una revisión periódica sobre la capacidad, tomar las acciones que se consideren necesarias para mantener la operación. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
90	A.8.7 Protección contra malware	Se evidenció a nivel de muestreo que los equipos tecologicos cuentan con el respectivo antivirus y a nivel de política de seguridad, deben contar con un sistema de antivirus y antispyware instalado y actualizado activamente para la protección contra códigos maliciosos. El administrador de la plataforma de antivirus o el CAU cuentan con los permisos necesarios para deshabilitar, remover, eliminar y/o desinstalar el software de antivirus, estas actividades se llevan a cabo bajo autorización previa del jefe de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información. Se realizan escaneos a intervalos regulares como control del estado de la infraestructura tecnológica a través de las herramientas de monitoreo Solarwind, Nagios, VMWare para determinar acciones de mejora que sean implementadas y garantizar la operación de la infraestructura tecnológica. A través de la consola antivirus se validan los puertos, servicios y prestaciones similares instaladas en los equipos de escritorio, portátiles o equipos de red que no se requieran específicamente para la funcionalidad de la Entidad y se deshabilitan o en otros casos, se retiran. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación a nivel de muestreo en algunos computadores.
91	A.8.8 Gestión de vulnerabilidades técnicas	Se evidenció que realizan el análisis de vulnerabilidades en intervalos programados sobre toda la infraestructura tecnológica, para evaluar los riesgos a los cuales se encuentra expuesta la mencionada infraestructura para generar los planes de tratamiento apropiados en pro de la mitigación de riesgos. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0, Matriz de Gestión de Análisis de Vulnerabilidades, Viernes 24 de Mazo de 2023 a Lunes 27 de Marzo de 2023 (Kiggu).
92	A.8.9 Gestión de la configuración	Se evidencio que frente a las políticas de seguridad establecidas y los diferentes procedimientos, garantizan el aseguramiento de los diferentes sistemas, también se identifica diferentes tipos de gestión que permiten controlar posibles riesgos de seguridad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
93	A.8.10 Eliminación de información	Se evidenció que se deben validar los acuerdos de confidencialidad para asegurar la respetiva eliminación de la información. Los propietarios de la información que se requiera intercambiar son responsables de definir los niveles y perfiles de autorización para el acceso, modificación y eliminación de ésta, garantizando siempre la privacidad de los datos e información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		información 2.0.
94	A.8.11 Enmascaramiento de datos	Se evidenció el documentado a nivel de Política para desarrollo seguro y la Guía para el desarrollo de software, también se identifico que manejan buenas practicas, por lo que tienen en cuenta los lineamientos dados por OWASP. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información. Guía para el desarrollo de software TI.120.P05. A 01.
95	A.8.12 Prevención de fugas de datos	Se evidenció que en la política para la transferencia de información, se establece que todo servidor público, contratista y tercero será responsable por proteger la confidencialidad e integridad de la información. Y deben terner cuidado con el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada. La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información realiza el debido respaldo de la información sobre los medios que serán dados de baja o reasignados entre los colaboradores, y estos son ubicados en el inventario de baja. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información.
96	A.8.13 Copia de seguridad de la información	Se evidencio que la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información genera las respectivas copias de respaldo y almacenamiento de la información almacenada en los sitios autorizados para ésta, de acuerdo con lo definido en el documento procedimiento respaldo (backup) de información de los servidores y bases de Datos de la AGR. Para la restauración de los backups, los administradores funcionales de las oficinas que tengan su backup dentro del software destinado por la Entidad para realizar las copias de respaldo, solicitan una restauración trimestral con el fin de que el administrador de copias de respaldo seleccione la cinta aleatoria del trimestre y la información sea entregada al administrador funcional, para que verifique la autenticidad la restauración de la información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P06 Respaldo (backup) de información de los servidores y bases de Datos de la AGR, Ver. 1.0. con fecha de 29/03/2022.
97	A.8.14 Redundancia de las instalaciones de procesamiento de información	Se evidenció que la AGR revisa la redundancia a intervalos planificados, definidos por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información. TI.120.P01.A05_Anexo 5 Plan Recuperación.
98	A.8.15 Registro	Se evidenció que activan la generación de registros en sistemas y plataformas que soportan las aplicaciones y servicios de TI; estos registros asociados a cambios de configuración, cambios en la asignación de privilegios, información de acceso, intento de uso de recursos, uso de privilegios, transacciones ejecutadas, entre otras y según aplique. Para los nuevos sistemas desarrollados in-house o por un proveedor, se producen registros de las actividades de auditoría, excepciones, eventos, fallas y se conservan bajo el periodo establecido por el área funcional y de acuerdo con el Grupo de Tecnologías y Sistemas de Información. Todos los accesos de usuarios a los sistemas, aplicaciones y redes de datos se registran y/o conservan con el fin de facilitar las labores de auditoría, en las aplicaciones que ameriten este control de auditoría. Se hacen copias de respaldo de información a los sistemas de información que tienen implementado eventos de auditoría, con el fin de

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		que estén disponibles en el caso que se presente un incidente de seguridad de la información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información.
99	A.8.16 Actividades de seguimiento	Se evidenció que realizan escaneos a intervalos regulares como control del estado de la infraestructura tecnológica a través de las herramientas de monitoreo Solarwind, Nagios, VMWare. Y realizan el monitoreo de los canales de comunicación, con el fin de establecer en los niveles de operación y desempeño de los mismos y generar los mecanismos de control a que haya lugar. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información.
100	A.8.17 Sincronización de reloj	Se evidenció que todos los relojes de los sistemas de procesamiento de información de la Auditoría General de la República – AGR están configurados según lo descrito para los distintos sistemas operativos. La configuración se encuentra descrita en el documento, Manual de Sistemas_Confidencial. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P01.A06_Anexo 6_Manual de sistemas_Confidencial.
101	A.8.19 Instalación de software en sistemas operativos	Se evidenció que el software instalado en la Entidad cuenta con su respectiva licencia de validez y legalidad en el mercado, verifican el normal funcionamiento de los aplicativos que se entregan a producción o están en producción, con el objetivo de no afectar la integridad, disponibilidad y desempeño de estos. La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información autoriza los accesos temporales y controlados a los terceros para realizar las actualizaciones sobre el software, así como monitorea las actualizaciones, en caso de ser necesario. También cuentan con una lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los equipos de la Entidad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P05.A 01 Guía para el desarrollo de software, TI.120.P05.P Procedimiento desarrollo de software.
102	A.8.20 Seguridad de redes	Se evidenció que a nivel de política de seguridad, se establece que ningún servidor público, contratista o proveedor está autorizado para conectar equipos de escritorio, equipos portátiles y demás recursos tecnológicos a la red que no sean propiedad o bajo el dominio de la Auditoría General de la República – AGR, de manera cableada o inalámbrica. Esta conexión se realiza únicamente a través de las solicitudes realizadas a través del CAU. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información.
103	A.8.21 Seguridad de los servicios de red	Se evidenció que los accesos a la red inalámbrica deben ser autorizados por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información, donde se establecen mecanismos de control necesarios para proteger la infraestructura y los datos e información de la Entidad. Los equipos de terceros que requieran acceder a la red de la Entidad deben cumplir con lo descrito en los documentos: Atención a usuarios de la plataforma tecnológica y Administración de la infraestructura tecnológica antes de conceder el acceso solicitado para conectar a la red de la Entidad.

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P03.P Atención a usuarios de la plataforma tecnológica, TI.120.P01.P Administración de la infraestructura tecnológica antes de conceder el acceso solicitado para conectar a la red de la Entidad.
104	A.8.22 Segregación de redes	Se evidencio que la entidad cuenta con segregación a nivel de accesos a la red, donde se deben tener los permisos correspondientes para su uso, esta red también cuenta con los respectivos controles de seguridad. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P01.P Administración de la infraestructura tecnológica antes de conceder el acceso solicitado para conectar a la red de la Entidad.
105	A.8.23 Filtrado web	Se evidenció que en la entidad, no esta permitido el uso de aplicaciones y servicios interactivos como: Team Viewer, TightVNC, RemoteVNC, Chrome Remote Desktop, Join.me, Ammy Admin, Putty, WinSCP, Screen Leap, Vyew, Croos Loop, Skype y similares. Los bloqueos los realizan a través del Firewall de la Entidad y también monitorean el uso del canal de navegación. También se evidencio que bloquean paginas relacionas con pornografía, drogas, terrorismo, segregación racial, hacking, chat, redes sociales, correos electrónicos personales, Web, YouTube, música, videos, TV, juegos. Realizan control mediante la herramienta End-Point para impedir el acceso a los diferentes sitios web. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información.
106	A.8.24 Uso de la criptografía	Se evidencio que se encuentra establecida la política para controles criptográficos y gestión de llaves, VPN site-to-site, certificados digitales, firmas electrónicas, firmas digitales, y los respectivos token's para firma digital. La administración de claves criptográficas y certificados digitales esta a cargo de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información.
107	A.8.25 Ciclo de vida de desarrollo seguro	Se evidenció que la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información, cuenta con direccionamiento IP a nivel de sistemas operativos Windows y Linux de manera separadas, para los ambientes de desarrollo, pruebas, taller y producción al interior de la Entidad. Los respectivos listados del direccionamiento IP se encuentran asignados a: ambiente de pruebas, ambiente de desarrollo y ambiente productivo para garantizar la seguridad de los datos. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información.
108	A.8.26 Requisitos de seguridad de las aplicaciones	Se evidenció que el suministro de la información para las pruebas de aplicaciones es validado por el área usuaria de la aplicación para asegurar que la data es correcta y apropiada. Validan los acuerdos de confidencialidad para asegurar la respetiva eliminación de dicha información. También a través del respectivo análisis de vulnerabilidades que se realiza a la infraestructura tecnológica durante el desarrollo (ambiente de pruebas) y el paso a producción (ambiente de producción) identifican posibles puertas abiertas para generar la respectiva remediación. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P05.A 01 Guía para el desarrollo de software.
109	A.8.27 Arquitectura	Se evidenció que se incorporan chequeos de validación en las aplicaciones para

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
	de sistemas seguros y principios de ingeniería	detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados. Hacen revisiones entre el usuario funcional y desarrollador, realizando pruebas de calidad antes de desplegar aplicaciones o correcciones en producción. Adicionalmente se gestionan las autorizaciones de despliegue por parte de los usuarios funcionales y se guardan las evidencias de dicho proceso. Se implementan los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y pruebas hacía ambiente de producción. La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información en conjunto con los propietarios de los aplicativos realizan pruebas necesarias: prueba de desarrollo y prueba funcional. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P05.P Procedimiento desarrollo de software.
110	A.8.28 Codificación segura	Se evidenció que no es permitido el uso y copia de información operacional como datos de pruebas, salvo autorización previa del rol del Oficial de Seguridad de la Información y el responsable del activo, o previa ejecución de procesos de anonimización de ésta. La información operacional la borran de los sistemas de aplicación de prueba inmediatamente después de haber completado la prueba; se registra el copiado y uso de la información operacional para proporcionar un rastro de auditoría. Se certifica que la información entregada a los desarrolladores para realizar las pruebas no revela información confidencial de los ambientes de producción. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P05.P Procedimiento desarrollo de software, TI.120.P05.A 01 Guía para el Desarrollo de Software.
111	A.8.29 Pruebas de seguridad en el desarrollo y aceptación	Se evidenció que los desarrolladores garantizan que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, se implementan mensajes de error genéricos. Los desarrolladores suministran opciones de desconexión o cierre de sesión de los aplicativos (logout) que permiten terminar completamente con la sesión o conexión asociada, las cuales se encuentran disponibles en todas las páginas protegidas por autenticación. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P05.P Procedimiento desarrollo de software, TI.120.P05.A 01 Guía para el Desarrollo de Software.
112	A.8.30 Desarrollo externalizado	Se evidenció que a nivel de politica de seguridad, se establecen los acuerdos sobre: las licencias, propiedad de los códigos y derechos de propiedad intelectual y convenios a que haya lugar en caso de falla de la tercera parte, derechos de acceso para auditar la calidad y exactitud del trabajo realizado, requisitos contractuales para la calidad y la funcionalidad de la seguridad del código, ejecución de pruebas antes de la instalación para detectar códigos troyanos o maliciosos. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P05.P Procedimiento desarrollo de software, TI.120.P05.A 01 Guía para el Desarrollo de Software.
113	A.8.31 Separación de entornos de desarrollo, evidencia y producción	Se evidencio que a nivel de política de seguridad de la información, las nuevas aplicaciones, desarrollos, y/o sistemas operativos o modificaciones a estos y que soporten los sistemas de información, solamente deben ser implementados en el ambiente de producción después de un protocolo de pruebas adecuado que involucre aspectos funcionales, de seguridad, de compatibilidad con otros sistemas de información y facilidad de uso.

No.	Requisito que se cumple	Condición (Descripción de la situación que corresponde al cumplimiento del requisito y la evidencia que fundamenta la Conformidad).
		Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P05.P Procedimiento desarrollo de software, TI.120.P05.A 01 Guía para el Desarrollo de Software.
114	A.8.32 Gestión del cambio	Se evidenció que a nivel de control, es responsabilidad del Grupo de Tecnologías y Sistemas de Información llevar a cabo revisiones periódicas, aprobaciones y evaluación de errores de los cambios programados a nivel de las aplicaciones antes, durante y después de su ejecución y debe existir una aprobación previa de las oficinas interesadas para la ejecución del cambio. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, TI.120.P04.P_ Procedimiento Gestión de Cambios, TI.120.P04.IP_ Instructivo General.
115	A.8.33 Información de las pruebas	Se evidenció que los desarrolladores garantizan que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, se implementan mensajes de error genéricos. El Grupo de Tecnologías y Sistemas de Información cuenta con la separación debida de ambientes: para desarrollo, para pruebas, taller y para producción, acorde con lo establecido e identificado a través del direccionamiento IP a nivel de sistema operativo Windows y sistema operativo Linux. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información, Procedimiento desarrollo de software, TI.120.P05.A 01 Guía para el Desarrollo de Software.
116	A.8.34 Protección de los sistemas de información durante las pruebas de auditoría	Se evidenció en la que las auditorías se ejecutan según lo establecido en el programa de auditorías definido por la Entidad y en caso de ser necesario se pueden programar revisiones parciales o totales sobre una o varias líneas de acción o trabajo, oficina, etc., con el fin de verificar la eficacia de las acciones correctivas. En caso de requerirse acceso a las aplicaciones o sistemas por parte de los auditores, estos son otorgados de consulta y en condiciones que impidan afectación de la disponibilidad o rendimiento requerido por las aplicaciones o sistemas. La información extraída o entregada como parte del proceso de auditoria será gestionada salvaguardando las condiciones de seguridad de información de la misma. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información.

4.2 No Conformidades mayores

No.	Requisito que se incumple	Condición (Descripción de la situación que corresponde al incumplimiento del requisito y la evidencia que fundamenta la no conformidad mayor)
	N/A	

4.3 No Conformidades menores

No.	Requisito que se incumple	Condición (Descripción de la situación que corresponde al incumplimiento del requisito y la evidencia que fundamenta la no conformidad menor)
1	A.5.1 Políticas de seguridad de la información	Se evidenció que la entidad cuenta con (2) políticas de seguridad de la información, una con fecha del 10-06-2023, bajo la versión 1.0, esta se encuentra aprobada, publicada (web) y socializada, esta política se alinea con los requisitos de la norma NTC-ISO/IEC 27001:2013. La segunda política, en la que se identifica el cumplimiento los requisitos de de la Norma NTC-ISO/IEC 27001:2022, no se encuentra aprobada, no ha sido comunicada, no es reconocida internamente, ni extrenamente y se ha revisado periódicamente como lo establece el control. Evidencia: TI.120.P08.A01 Política de Seguridad Digital Seguridad y Privacidad de la información 1.0 y entrevistas, TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0.
2	9.3.1 Revisión por la dirección: Generalidades	No se evidencio la revisión de alta dirección a intervalos planificados la conveniencia, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información.
3	9.3.2 Revisión por la dirección: Entradas de la revisión por la dirección	No se evidencio la revisión por la altadirección en los cambios del contexto, en las necesidades y expectativas de las partes interesadas, retroalimentación del desempeño del SGSI contemplando las no conformidades, acciones correctivas, resultados de seguimiento y medición, resultados de auditoria, cumplimiento de los objetivos de seguridad de la información, retroalimentación de las partes interesadas, oportunidades de la menjora continua.
4	9.3.3 Revisión por la dirección: Salidas de la revisión por la dirección	No se evidenciaron los resultados de la revisión por la altadirección, ni de las decisiones relacionadas con las oportunidades de mejora continua y cualquier otra necesidad de los cambios en el sistema de gestión de la seguridad de la información.
5	10.1 Mejora continua	No se evidencio, en que la organización realice mejoras continuamente en la conveniencia, adecuación y eficacia del sistema de gestión de seguridad de la información.
6	10.2 No conformidad y acción correctiva	No se evidencio la revisión de las no conformidades, de la eficacia de cualquier acción correctiva tomada, si es necesario hacer cambios en el sistema de gestión de seguridad de la información, de las acciones correctivas que son apropiadas para los efectos de las no conformidades encontradas. Se debe tener encuenta de que las no conformidades y cualquier acción subsecuente tomada y cualquier acción correctiva deben estar documentadas.
7	7.5.2 Información documentada: Creación y actualización	Se evidencio que varios documentos que conforman el Sistema de Gestión de Seguridad de la Información no cuentan con los estándares definidos por el Sistema de Gestión de Calidad, por lo que no cuentan con un adecuado control de cambios, titulo, número de referencia, versión, entre otros. Evidencia: Guia de gestión de incidentes, Guia de desarrollo de software, Política de Seguridad Digital Seguridad y Privacidad de la información.
8	A.7.7 Escritorio y pantalla limpios	Se evidencio que la entidad cuenta con la Política de Seguridad, donde establece que todos los colaboradores deben mantener la información clasificada con acceso restringido o confidencial bajo llave en sus escritorios y/o sitios de trabajo, sea cuando se retiren temporalmente de sus puestos de trabajo o en horas no laborales. Estos documentos incluyen: documentos impresos, dispositivos de almacenamiento, almacenamiento en la nube-cloud, medios removibles en general y similares. Así mismo, todos los equipos de escritorio y portátiles propios de la Auditoría General de la

No.	Requisito que se incumple	Condición (Descripción de la situación que corresponde al incumplimiento del requisito y la evidencia que fundamenta la no conformidad menor)
		República – AGR deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente una vez se bloquee la estación o después de cinco (5) minutos de inactividad, la cual se podrá desbloquear únicamente con la contraseña del usuario. Dado esto, se observo que varios de los computadores, no cuentan con el papel tapiz, protector de pantalla de la entidad y se idenctificarón en algunos computadores, accesos directos y archivos en el escritorio de las pantallas. Evidencia: TI.120.P08.A02 Política de Seguridad Digital Seguridad y Privacidad de la información 2.0. Verificación física en las instalaciones (Fotos).

4.4 Oportunidad de mejora

1. Acotar el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), teniendo en cuenta, que la implementación de los controles de seguridad de la información, son transvarsales para el aseguramiento de la información de la entidad.

2. Implementar en la Matriz de Riesgos de Seguridad de la Información, el listado de controles pertenecientes a la declaración de aplicabilidad del anexo A.

3. Actualizar los documentos pertenecientes al Sistema de Gestión de Seguridad de la Información, teniendo en cuenta, que en varios aún se identifican apartados de la norma anterior NTC-ISO/IEC 27001:2022. También revisar el control de cambios de los documentos y continuar con el proceso correspondiente a su validación, aprobación, publicación y sensibilización de los mismos.

4. Evaluar periodicamente la eficacia del Sistema de Gestión de Seguridad de la Información.

5. Fortalecer la gestión de la revisión por la dirección frente a las generalidades, entradas y salidas de la revisión por la dirección.

6. Fortalecer los controles de seguridad física, en especial de la seguridad de los data center (registros, cámaras de seguridad, accesos (llave-biometrico), revisión de extintores, elementos que puedan propagar un incendio, entre otros.

7. Auditar o monitorear el cumplimiento de las políticas por parte de los colaboradores, como por ejemplo: que no dejen los equipos desatendidos (sin bloquear), que no dejen información sensible en los escritorios, que tengan el fondo de pantalla y papel patiz correspondiente, que tengan el licenciamiento de Windows activado, que no tengan accesos directos, carpetas compartidas o archivos en el escritorio del PC.

5. Conclusiones

De acuerdo a los resultados de la auditoría, se puede evidenciar que el Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, el cual se encuentra alineado al Modelo de Seguridad y Privacidad de la Información (MSPI), bajo el cumplimiento de los requisitos de la Norma NTC-ISO/IEC 27001:2022, se encuentra

en la fase del verificar de acuerdo al ciclo de la mejora continua (PHVA). No obstante, se debe mantener y mejorar en atención a las no conformidades identificadas; esto, con el propósito de fortalecer los controles definidos y prevenir la materialización de riesgos, frente al desarrollo de cada una de las actividades y el fortalecimiento de su desempeño, con el objetivo de garantizar de manera efectiva la seguridad de la información.

5. NOMBRES		
Líder del equipo auditor	**Equipo de Auditores**	**Director de la Oficina de Control Interno**
Leonardo Sierra Rodríguez (líder equipo auditor)	**Omar Hugo Rivas Jimenez** **Yanet Sofia Rodriguez Leguizamón** **Eugenio Miguel Carrrillo Espinosa** **Viviana Cáceres Castro** **(Auditores en formación)**	**Claudia María Arroyave López** **Directora Oficina de Control Interno**