AERONÁUTICA CIVIL
Unidad Administrativa Especial

OFICINA DE CONTROL INTERNO

RESULTADO DEL SEGUIMIENTO A LAS OBSERVACIONES REPORTADAS POR LA AUDITORÍA EXTERNA EN EL INFORME DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN 2021. – VIGENCIA 2022

Bogotá D.C. octubre 2022

Tabla de Contenido

1. INTRODUCCIÓN. 3
2. OBJETIVO DE LA AUDITORÍA. 3
3. ALCANCE DE LA AUDITORÍA. 4
4. CRITERIOS DE AUDITORÍA. 4
5. LIMITANTES DE AUDITORÍA. 5
6. REQUERIMIENTOS ESPECÍFICOS DE LAS NORMAS REGULADORAS DE LA SEGURIDAD DE LA INFORMACIÓN A TENER EN CUENTA EN EL PROCESO DE AUDITORÍA INTERNA. 6
7. DESARROLLO DE LA AUDITORÍA DE SEGUIMIENTO. 12
7.1. Dependencias y equipo auditor que intervinieron en el proceso de evaluación del sistema de control interno (auditoría interna). 12
7.1.1. Dependencias Auditadas. 12
7.1.2. Equipo auditor. 12
8. RELACIÓN DE EVIDENCIAS OBSERVADAS DURANTE LA PRESENTE EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO (AUDITORÍA INTERNA), HALLAZGOS, RECOMENDACIONES Y CONCLUSIONES. 12
8.1. Dependencia encargada de liderar el proceso de auditoría a la seguridad informática. 12
8.2. Competencias de los auditores asignados al proceso de auditoría a la seguridad de la información. 13
8.3. Solicitud y programación del curso de capacitación en la Norma ISO/CEI 27701. 13
8.4. Gestión adelantada por la Secretaría de Tecnología de la Información – TI sobre las observaciones reportadas en el informe de la Auditoría externa. 14
8.5. Gestión reportada por la Secretaría General sobre las observaciones reportadas en el informe de la Auditoría Externa. 24
8.5.1. Gestión adelantada por la Dirección Administrativa sobre las observaciones reportadas en el informe de la Auditoría Externa. 24
8.5.2. Gestión adelantada por la Dirección de Gestión Humana sobre las observaciones reportadas en el informe de la Auditoría Externa. 25
8.6. Gestión adelantada por la Oficina Asesora Jurídica sobre las observaciones reportadas en el informe de la Auditoría Externa. 26
8.7. Gestión adelantada por la Oficina Asesora de Planeación sobre las observaciones reportadas en el informe de Auditoría Externa. 27
9. RESUMEN DEL REGUIMIENTO A LAS OBSERVACIONES DEL INFORME 2021 28
10. HALLAZGOS 30
11. CONCLUSIONES. 31

1. INTRODUCCIÓN.

En el marco de los lineamientos establecidos mediante la Ley 87 de 1993, “por medio de la cual se establecen normas para el ejercicio del control interno en la entidades y organismos del Estado y se dictan otras disposiciones”, y teniendo en cuenta lo definido en el Modelo Integrado de Planeación y Gestión – MIPG en la dimensión de “Control Interno”, donde se define la auditoría como “una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la entidad; que ayuda a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno”:

La Oficina de Control Interno de la Unidad Administrativa Especial de Aeronáutica Civil, en cumplimiento del Programa Anual de Auditorías para la vigencia 2022, aprobado por el Comité Institucional de Coordinación de Control Interno, presenta el informe de auditoría del Sistema de Gestión de Seguridad de la Información enmarcado en el proceso GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN cuyo objetivo principal es el siguiente:

“Fortalecer la capacidad de TI de la Aerocivil para soportar las necesidades que se demandan en materia de tecnologías de la información, de manera articulada con los lineamientos del Gobierno y el cumplimiento de las políticas de desarrollo administrativo.”

Cabe señalar que, la presente auditoría al proceso de Gestión de Seguridad de la Información se desarrolla dentro del marco de implementación de Modelo Integrado de Planeación y Gestión - MIPG que ha sido ha adoptado por la Unidad Administrativa especial de Aeronáutica Civil y se encuentra vinculado intrínsecamente al desarrollo y fortalecimiento de las Políticas de Gobierno y Seguridad Digital, verificando aspectos transversales asociados a las políticas de Gestión Documental y Transparencia implementadas por la Entidad como parte fundamental del modelo MIPG. Adicionalmente el desarrollo de la presente auditoría busca fortalecer la sinergia entre las líneas de defensa de la entidad en pro de garantizar una efectiva gestión de los riesgos.

2. OBJETIVO DE LA AUDITORÍA.

Evaluar el adecuado diseño, implementación y ejecución de los controles establecidos dentro de la gestión realizada por la Secretaría de la Tecnología de la Información – TI, direcciones y grupo, dentro del marco de la Norma ISO/CEI 27701 Gestión de Seguridad de la Información y los demás procesos inmersos en la gestión de los controles aplicables al interior de la Unidad Administrativa Especial de Aeronáutica Civil para garantizar el adecuado tratamiento de los riesgos asociados con la seguridad de la información de conformidad con lo establecido en el Decreto 1008 de 2018, el Manual de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC; en concordancia con las leyes 1712 de 2014 y 1581 de 2012.

3. ALCANCE DE LA AUDITORÍA.

La auditoría a la gestión del proceso de Seguridad de la Información se encuentra dentro del marco del procedimiento Gestión de Seguridad de la Información, asociado a la gestión de riesgos de seguridad digital, así como el cumplimiento de políticas de seguridad y privacidad de la información, gestionados durante el período comprendido entre enero y diciembre de la vigencia 2021 y lo corrido del año 2022. No obstante, se aclara que el presente proceso se desarrolló sobre una muestra de las observaciones consignadas en el informe de auditoría externa que se adelantó en la Entidad durante la vigencia 2021.

En los casos que sea necesario ampliar información, se tomaran muestras de soportes o transacciones de años anteriores o posteriores.

4. CRITERIOS DE AUDITORÍA.

- Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 del 14 de junio de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1266 de 2008 Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 80 de 1993 Por la cual se expide el Estatuto General de Contratación de la Administración Pública.
- Circulares, Instructivos y Cronogramas expedidos por el administrador del sistema SECOP y aquellos pertinentes emitidos por la Superintendencia de Industria y Comercio.
- Manual de Gobierno en Línea
- Modelo de Seguridad y Privacidad de la Información.
- Procedimientos SIGI que sean pertinentes.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento de la Función Pública.
- Norma ISO 27001 - Gestión de la seguridad de la información, y su Anexo A.

5. LIMITANTES DE AUDITORÍA

Aunque se había solicitado con anticipación la capacitación relacionada con la norma ISO/CEI 27701, y que esta fue incluida por la Dirección de Gestión Humana en el Plan Institucional de Capacitación – PIC 2022, es importante manifestar, que esta actividad no se realizó, situación que imposibilitó disponer de Servidores Públicos capacitados, formados y con el perfil requerido para la realización de tan importante auditoría al interior de la Entidad. De acuerdo con lo expuesto anteriormente, a la Oficina de Control Interno, le fue imposible adelantar la auditoría al proceso Seguridad de la Información, limitando su actividad al seguimiento a las observaciones reportadas en el informe de la Auditoría Externa del periodo 2021.

6. REQUERIMIENTOS ESPECÍFICOS DE LAS NORMAS REGULADORAS DE LA SEGURIDAD DE LA INFORMACIÓN A TENER EN CUENTA EN EL PROCESO DE AUDITORÍA INTERNA.

Con la intensión que se observe el alcance de la auditoría que la Oficina de Control Interno debe realizar con base en la norma ISO/CEI 27701, sobre el proceso de Seguridad de la Información que se genera, almacena y trascribe a través de los diferentes sistemas informáticos instalados en las dependencias y/o áreas de la Entidad, se transcriben los requisitos que se deben auditar, incluido la verificación y el seguimiento al estado de implementación en el que se encuentra el proceso:

*"Las **normas** ISO de Gestión de la **Seguridad de la Información** se denominan familia de **normas** ISO 27000 y son las siguientes: ISO 27001: Es la **norma** principal de la serie y contiene los requisitos del sistema de gestión de **seguridad de la información**. Es la **norma** con arreglo a la **cual** se certifican por auditores externos.*

*Las auditorías se pueden realizar haciendo uso de la **Norma ISO 27002** que contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Esta normativa hace parte de la ISO 27000.*

***ISO 27000** es un conjunto de estándares internacionales sobre la Seguridad de la Información. La familia **ISO 27000** contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información.*

*¿**Quién debería utilizar la norma ISO/IEC 27701**?*

*La **norma ISO**/CEI **27701** es aplicable a todos los tipos y tamaños de organizaciones, incluidas las empresas públicas y privadas, las entidades gubernamentales y las organizaciones sin ánimo de lucro.*

De acuerdo con la Resolución número 00500 de marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" del Ministerio de Tecnologías de la Información y las Comunicaciones – MITIC, señala en los siguientes Artículos:

ARTÍCULO 1. Objeto. La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

ARTÍCULO 2. Ámbito de aplicación. Serán sujetos obligados de la presente resolución los señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

ARTÍCULO 5. La estrategia de seguridad digital. Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Adicionalmente, la estrategia de seguridad digital debe:

1. Ser aprobada a través de un acto administrativo de carácter general.
2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.
3. Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.
4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces.
5. La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.
6. Aplicar las demás consideraciones que a juicio de la entidad contribuyan a elevar sus estándares de seguridad digital.

ARTÍCULO 6. La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. Los sujetos obligados deben determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades:

1. Definir controles considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.
2. Realizar una gestión efectiva de la seguridad de la información y la seguridad digital en la entidad.

3. Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces.
4. Estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad, según las políticas que establezca la entidad de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad.
5. Establecer las capacitaciones que recibirán los funcionarios de la entidad en temas relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas.
6. Realizar el monitoreo del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información y sin perjuicio de aquellas tareas que realizan las autoridades de control.
7. Asesorar a la dirección de la entidad sobre seguridad de la información y seguridad digital para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.
8. Realizar un análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros.
9. Determinar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad. Dichos recursos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información.
10. Implementar y gestionar un Sistema de Gestión de Seguridad de la Información de acuerdo a lo establecido en el Modelo de Seguridad y Privacidad de la Información, que permita gestionar los riesgos de seguridad de la información de la entidad de una manera adecuada y oportuna.
11. Cumplir los lineamientos de gestión del riesgo establecidos en la guía para la administración del riesgo y el diseño de controles en entidades públicas expedida en el marco del modelo integrado de planeación y gestión.

ARTÍCULO 9. Gestión de incidentes de seguridad digital. Los sujetos obligados deben establecer un procedimiento de gestión de incidentes de seguridad digital, para realizar el tratamiento, investigación y gestión de los incidentes de seguridad digital que se presente en relación con los activos de información de cada proceso, para lo cual deben:

1. Gestionar los incidentes de seguridad digital, según el procedimiento establecido por MinTIC, para lo cual deben crear una bitácora que contenga la descripción de cada una de las actividades desarrolladas en la gestión de estos.
2. Designar dentro de la entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital.
3. Una vez identificado el incidente de seguridad digital se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave y Grave por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación del CSIRT Gobierno.
4. Los incidentes catalogados por el responsable de seguridad digital de la entidad, como Menos Grave y Menor, deben ser comunicados al CSIRT Gobierno en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.
5. Los sujetos obligados, según el análisis e investigación de los incidentes y teniendo en cuenta la causa raíz, deben realizar los respectivos planes de mejoramiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento.

ARTÍCULO 17. Etapas generales de la gestión de incidentes de seguridad digital. Los sujetos obligados deben incluir en su estrategia de seguridad digital las actividades a realizar en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje. Como mínimo deberán incorporar:

1. Prevención

La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de seguridad digital. En esta etapa, los sujetos obligados deben cuando menos:

1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales), protección de infraestructura y gestión de identidades, privacidad y protección de la información.
1.2. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.
1.3. Gestionar y documentar la seguridad de la plataforma tecnológica.
1.4. Contar con los recursos tecnológicos necesarios para realizar una adecuada gestión de seguridad de la información y la ciberseguridad.
1.5. Identificar, y gestionar los riesgos de seguridad de la información que puedan llegar a afectar a la entidad y establecer controles para su mitigación.
1.6. Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información.
1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques de seguridad de la información.
1.8. Determinar la necesidad de contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, entre otros, SIEM (Gestión de eventos de información de seguridad) o SOC (Centro de operaciones de seguridad).
1.9. De acuerdo con la estructura, infraestructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información institucionales oficiales tales como sistemas de información, infraestructuras críticas, correos electrónicos, sitios web, blogs, dispositivos y perfiles oficiales de redes sociales con el propósito de identificar posibles ataques cibernéticos contra la entidad.
1.10. Colaborar y articular con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad a nivel nacional.

2. Protección y detección La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Los sujetos obligados deben:

1.1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de seguridad que se presenten.
1.2. Gestionar las vulnerabilidades de aquellas infraestructuras criticas o plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.
1.3. Realizar un monitoreo continuo a su plataforma tecnológica e infraestructura critica con el propósito de identificar y predecir comportamientos inusuales que puedan evidenciar ataques contra la entidad.

1.4. Implementar tecnologías que permitan a la Entidad identificar el origen de los ataques, tipos de ataques, comportamientos y la detección predictiva de amenazas.
1.5. Realizar periódicamente auditorias de seguridad de la información tanto para los aspectos de gestión como para los aspectos técnicos, como podrían ser: auditorías internas y externas al modelo de Seguridad y Privacidad de la Información, análisis de vulnerabilidades, Hacking ético, pruebas de penetración a sistemas informático y pruebas de ingeniería social entre otras.

3. Respuesta y comunicación

Aún con las medidas de seguridad adoptadas, los sujetos obligados deben desarrollar e implementar planes de respuesta a incidentes de seguridad digital. Para hacerle frente a esta situación los sujetos obligados deben:

1.1. Establecer planes y procedimientos de respuesta a incidentes digitales y de seguridad de la información.
1.2. Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, a través del CSIRT sectorial, los incidentes de seguridad Digital que requieran de su gestión.
1.3. Comunicar a las autoridades competentes después de una fuga o afectación a la privacidad de la información de la Entidad o ciudadanos.
1.4. Dar un tratamiento adecuado a las evidencias forenses para que las áreas de seguridad digital y las autoridades puedan realizar su identificación, recolección, embalaje y disposición en las investigaciones correspondientes.

4. Recuperación y aprendizaje

Desarrollar e implementar actividades apropiadas para definir y mantener los planes de recuperación, resiliencia y restauración de las infraestructuras críticas, servicios, sistemas de información, procesos o en general de un activo de información que se haya deteriorado debido a un incidente de seguridad digital.

Los sujetos obligados deben:

1.1. Adoptar los mecanismos necesarios para recuperar los sistemas de información e infraestructuras al estado en que se encontraban antes del ataque de seguridad.
1.2. Ajustar sus sistemas de gestión de riesgo y de seguridad de la información como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.
1.3. Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector.

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27000 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

En este sentido, dentro del marco de la estrategia de gobierno en línea, se ha elaborado el modelo de seguridad y privacidad de la información, el cual a lo largo de los últimos años se ha ido actualizando en función de las modificaciones de la norma técnica que le sirve de sustento: ISO 27001, así como las mejores prácticas y cambios normativos de impacto sobre el modelo.

- *ACTIVO: Cualquier cosa que tenga valor para la organización. [NTC 5411- 1:2006]*
- *CONTROL: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.*
- *SEGURIDAD DE LA INFORMACIÓN. Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.*
- *POLÍTICA. Toda intención y directriz expresada formalmente por la Dirección.*
- *RIESGO. Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC Guía 73:2002]*
- *ANÁLISIS DE RIESGOS. Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [ISO/IEC Guía 73:2002]*
- *EVALUACIÓN DE RIESGOS. Todo proceso de análisis y valoración del riesgo. [ISO/IEC Guía 73:2002]*
- *VALORACIÓN DEL RIESGO. Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo. [ISO/IEC Guía 73:2002]*
- *GESTIÓN DEL RIESGO. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [ISO/IEC Guía 73:2002]*
- *TRATAMIENTO DEL RIESGO. Proceso de selección e implementación de medidas a para modificar el riesgo. [ISO/IEC Guía 73:2002]*

10.1. PERFIL DEL AUDITOR DE SISTEMAS

El Auditor es un asesor dentro de la entidad, su ubicación depende de la ubicación orgánica y funcional. Se requieren calidades humanas, de gestor y de organizador, algunas de ellas:

- *Eficiencia en su misión en la entidad.*
- *Ser diplomático.*
- *Manejo de pedagogía.*
- *Conocimiento de herramientas y métodos, para llegar al objetivo a alcanzar.*
- *Conocimiento en técnicas de auditoria.*

*La **norma ISO**/CEI **27701** es aplicable a todos los tipos y tamaños de organizaciones, incluidas las empresas públicas y privadas, las entidades gubernamentales y las organizaciones sin ánimo de lucro.*

Conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015

(DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", El parágrafo del artículo 16 del Decreto 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública" y la Resolución número 00500 DE MARZO 10 DE 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, la Entidad a través de la Oficina de Control Interno, le corresponde gestionar y realizar el proceso de Auditoría sobre la Seguridad de la Información que se genera, almacena y trascribe a través de los diferentes sistemas informáticos instalados en las dependencias y/o áreas de la Entidad de acuerdo con la ***norma ISO/CEI 27701,*** *la cual es aplicable a todos los tipos y tamaños de organizaciones, incluidas las empresas públicas y privadas, las entidades gubernamentales y las organizaciones sin ánimo de lucro."*

7. DESARROLLO DE LA AUDITORÍA DE SEGUIMIENTO.

7.1. Dependencias y equipo auditor que intervinieron en el proceso de evaluación del sistema de control interno (auditoría interna).

7.1.1. Dependencias Auditadas.

- Secretaria de Tecnología de la Información – TI.
- Secretaria General.
- Dirección Administrativa.
- Dirección de Gestión Humana.
- Oficina Asesora Jurídica.
- Oficina Asesora de Planeación.

7.1.2. Equipo auditor.

- Carlos Enrique Bacca Acosta.
- Víctor Manuel Valdivieso Ruiz

8. RELACIÓN DE EVIDENCIAS OBSERVADAS DURANTE LA PRESENTE EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO (AUDITORÍA INTERNA), HALLAZGOS, RECOMENDACIONES Y CONCLUSIONES.

8.1. Dependencia encargada de liderar el proceso de auditoría a la seguridad informática.

"Conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único

Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", El parágrafo del artículo 16 del Decreto 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública" y la Resolución número 00500 DE MARZO 10 DE 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, la Entidad a través de la Oficina de Control Interno, le corresponde gestionar y realizar el proceso de Auditoría sobre la Seguridad de la Información que se genera, almacena y trascribe a través de los diferentes sistemas informáticos instalados en las dependencias y/o áreas de la Entidad de acuerdo con la ***norma ISO/CEI 27701,*** *la cual es aplicable a todos los tipos y tamaños de organizaciones, incluidas las empresas públicas y privadas, las entidades gubernamentales y las organizaciones sin ánimo de lucro."*

8.2. Competencias de los auditores asignados al proceso de auditoría a la seguridad de la información.

Los Servidores Públicos asignados para adelantar el proceso de auditoría sobre la Seguridad de la información en la Entidad, deben contar con la capacitación respectiva y la correspondiente certificación como Auditores de Calidad en la Norma ***ISO/CEI 27701*** expedida por un ente externo debidamente reconocido por la autoridad competente.

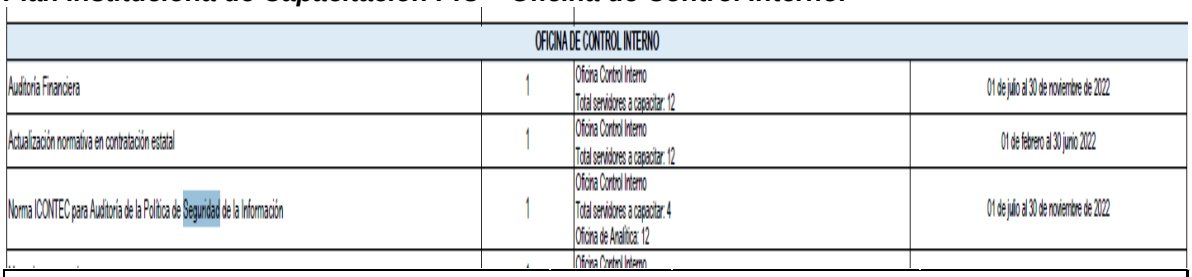
8.3. Solicitud y programación del curso de capacitación en la Norma ISO/CEI 27701.

La jefatura de la Oficina de Control Interno, consiente de la responsabilidad y la necesidad de realizar la Auditoría Seguridad de la Información en la Entidad, coordinó con la Dirección de Informática de la Secretaria de Tecnología de la Información - TI, la radicación con carácter de urgencia ante la Oficina Centro de Estudios Aeronáuticos – CEA y la Dirección de Gestión Humana la solicitud el curso de capacitación en la Norma Gestión de Calidad **ISO/CEI 27701** para veinte (20) Servidores Públicos de la Entidad**.**

La anterior solicitud se refleja en el Plan Institucional de Capacitación – PIC de la Entidad para la vigencia 2022, como se puede evidenciar en el resumen consignado a continuación:

Dirección Página Web: PIC 2022 Versión 2. Publicado en: http://www.centrodeestudiosaeronauticos.edu.co/cea/Programacion%20Acadmica/Plan%20Institucional%20de%20Capacitaci%C3%B3n%20Aerocivil%20-%20Ver.%202_AprobadoporelCIGD_15062022.pdf

Plan Instituciona de Capacitación PIC – Oficina de Control Interno.



OFICINA DE CONTROL INTERNO			
Auditoría Financiera	1	Oficina Control Interno Total servidores a capacitar: 12	01 de julio al 30 de noviembre de 2022
Actualización normativa en contratación estatal	1	Oficina Control Interno Total servidores a capacitar: 12	01 de febrero al 30 junio 2022
Norma ICONTEC para Auditoría de la Política de Seguridad de la Información	1	Oficina Control Interno Total servidores a capacitar 4 Oficina de Analítica: 12	01 de julio al 30 de noviembre de 2022

OFICINA DE CONTROL INTERNO			
Auditoría Financiera	1	Oficina de Control Interno Total Servidores a capacitar 12	01 de julio al 30 noviembre de 2022
Actualización normativa en contratación estatal	1	Oficina de Control Interno Total Servidores a capacitar 12	01 de febrero al 30 de junio de 2022
Norma INCONTEC para auditoria de la Política Seguridad de la Información	1	Oficina de Control Interno Total Servidores a capacitar 4	01 julio al 30 de noviembre de 2022

Plan Institucional de Capacitación - PIC – Secretaría de Tecnología de la Información - TI

SECRETARIA DE TECNOLOGÍAS DE LA INFORMACIÓN - TI			
Curso ISO 27001: Auditor Interno - Política Seguridad de la Información	1	Total servidores a capacitar 4	1 de julio al 30 de noviembre de 2022

SECRETARIA DE TECNOLOGÍAS DE LA INFORMACIÓN - TI			
Curso ISO 27001 - Auditor Interno - Política Seguridad de la Información	1	Total servidores a Capacitar 4	01 julio al 30 de noviembre de 2022

Es importante manifestar, que a pesar que la solicitud de capacitación se realizó con carácter de urgencia manifiesta y de estar incluida y programada en el Plan Institucional de Capacitación – PIC, al 30 de octubre de 2022, esta actividad no se ha gestionado, obligando a la Entidad, a reprogramar la fecha de la auditoría con el propósito de cumplir con lo reglamentado en Ley 1341 de 2009, el Decreto 1078 de 2015 y la Resolución número 00500 DE MARZO 10 DE 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, exponiendo a la Entidad, a sanciones del MINTIC y de los entes de control externos.

8.4. Gestión adelantada por la Secretaría de Tecnología de la Información – TI sobre las observaciones reportadas en el informe de la Auditoría externa.

En los cuadros relacionados a continuación, se describe la gestión adelantada por las dependencias sobre las observaciones que reporto el resultado de la auditoría externa ejecutada durante la vigencia 2021. Igualmente, se reportan las dependencias que no rindieron avances *(Ver columna – ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022)*:

- **Política Seguridad de la Información.**

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN					
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
5.1 Dirección de la Gestión de Seguridad de la Información	**Objetivo:** Proporcionar orientación y apoyo a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes relevantes				
5.1.1 Políticas para la Seguridad de la Información	Un conjunto de políticas de Seguridad de la Información deben estar definidos, aprobados por la dirección, publicados y comunicados a los empleados y partes externas relevantes.	4. Se realiza informalmente en forma total	En el manual del SGSI están publicadas y aprobadas la política general y las políticas del SGSI. No s evidencia su socialización ni su implementación, medición y mejora. No conforme	N/A	Las política general y las políticas del SGSI se encuentran aprobadas en Isolucion y publicadas en la intranet.
5.1.2 Revisión de las Políticas de Seguridad de la Información	Las políticas de Seguridad de la Información deben ser revisadas a intervalos planificados o si se producen cambios significativos, para asegurar su conveniencia, adecuación y eficacia.	2. No se realiza	N/A	N/A	No se han realizado cambios en las políticas

- Organización de Seguridad de la Información.

- Organización Interna.

6. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN					
6.1 ORGANIZACIÓN INTERNA	**Objetivo:** Para establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
6.1.1 Roles y Responsabilidades de Seguridad de la Información	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información	3. Se realiza parcial e informalmente	No se evidencia la asignación formal de roles y responsabilidades en SI. No conforme	Las responsabilidades en SI se deben asignar formalmente y cumplir el principio de separación de deberes y gestión integral del SGSI a todas las partes interesadas	Se asignaron todos los roles de seguridad de lnformación de la entidad en la guía de Roles y Responsabilidades del SGSI aprobada en Isolucion y publicada en la Intranet .
6.1.2 Segregación de funciones	Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	3. Se realiza parcial e informalmente	no se asignan los roles, y responsabilidades o accesos basados en este principio. No conforme	la creación de áreas y de usuarios debe hacerse cumpliendo este principio para evitar conflictos de interés o accesos no autorizados sobre información o entornos protegidos	No se han separado las áreas de responsabilidad y los usuarios.
6.1.3 Contacto con autoridades	Se deberían mantener contactos apropiados con las autoridades pertinentes	5. Se realiza formalmente y está documentado	El manual el SGSI establece los canales y el procedimiento, no hay evidencia de su implementación, medición y mejora	N/A	Se tiene comunicación con la Fiscalía y FAC.
6.1.4 Contacto con grupos de interés especial	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	3. Se realiza parcial e informalmente	no se evidencia un canal permanente de comunicación hay actualización con fuentes de vulnerabilidades, actualizaciones en temas de ciberseguridad, entra otros. No conforme	el área de SI, debe mantenerse permanente al día en grupos de interés con temas relacionados con la seguridad de la información y la ciberseguridad	Se establecieron los canales de comunicación con las entidades pertinentes
6.1.5 Seguridad de la información en la gestión de proyectos	La seguridad de la información se debería abordar en la gestión de proyectos, independientemente del tipo de proyecto	3. Se realiza parcial e informalmente	No se evidencia que los proyectos de la entidad incluyan requisitos de SI de manera programada y recurrente, las solicitudes de compras de tecnologías establecen algunos, dependiendo de lo que el solicitante establezca. No conforme	N/A	La guía de seguridad en proyectos y construcción de ANS se encuentra aprobada en Isolucion. Este documento se socializó con la Dirección Administrativa.

- Dispositivos Móviles y Teletrabajo.

6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
6.2.1 Política de Dispositivos Móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	3. Se realiza parcial e informalmente	Se evidencia la política y un estándar de gestión para dispositivos móviles. No hay evidencia de su implementación, medición y mejora. No conforme	Los dispositivos móviles y la estaciones de trabajo remoto, deben revisarse con regularidad para asegurar que cumplen con las políticas de SI establecidas	Las tablets proporcionadas por la entidad deben contar con sistema antimalware. Se realiza verificación y se exige al portador que instale el antimalware como medida de prevención y detección.
6.2.2 Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	3. Se realiza parcial e informalmente	Se evidencia la política de teletrabajo, pero no su revisión y mejora. No conforme	N/A	Los equipos PC o Portátiles utilizados para teletrabajo propiedad de la entidad tienen por políticas de SI instalados sistemas antimalware. Respecto a dispositivos móviles, su uso no es un estándar de la entidad. Los equipos que no son de la entidad son sometidos a checklist de verificación de seguridad asegurándose de que tiene medidas mínimas de seguridad instaladas y habilitadas.

- Gestión de Activos.

- Responsabilidad de los Activos.

8 GESTIÓN DE ACTIVOS					
8.1 RESPONSABILIDAD DE LOS ACTIVOS	**Objetivo:** Identificar los activos de la organización y definir las responsabilidades de protección adecuada				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
8.1.1 Inventario de los Activos	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos	5. Se realiza formalmente y está documentado	En el SOA dice que esta parcialmente implementado. Los responsables son los líderes de proceso para identificar los activos de información	Metodología para gestión de activos y matriz de gestión de tecnologías de información	Se tiene el inventario de los activos de información de los 34 procesos de la entidad.
8.1.2 Propiedad de los activos	Los activos mantenidos en el inventario deberían tener un propietario.	4. Se realiza informalmente en forma total	En el SOA dice que esta parcialmente implementado	Se establecen los propietarios de los activos, formalmente pero falta la inclusión de la responsabilidad frente a SI por la custodia de los activos. No conforme	Todos los activos de información tienen identificado su propietario y su custodio.
8.1.3 Uso aceptable de activos	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	5. Se realiza formalmente y está documentado	En el SOA dice que esta parcialmente implementado	Estándares aprobados para configuración y uso de los activos de SI, se tienen protocolos de configuración para los servidores que maneja la coordinación de soporte informático	Se tiene los estándares aprobados en Isolucion y publicado en la Intranet.
8.1.4 Devolución de activos	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	5. Se realiza formalmente y está documentado	Procedimiento de retiro de funcionarios, aplicativo gacel gestión de acceso de componentes en línea	Alineado con los procesos de retiro de gestión humana. Procedimiento de traslado y retiro de activos, instructivo y flujo de trabajo en GACEL, procedimiento de retiro de activos de información	El procedimiento de retiro de activos esta aprobado en Isolucion y publicado en la Intranet.

- Clasificación de la Información.

8.2 CLASIFICACIÓN DE LA INFORMACIÓN	**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
8.2.1 Clasificación de la Información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	3. Se realiza parcial e informalmente	En el SOA dice que falta ajustar documentación lo que incumpliría el control 7.5 de información documentada. No se evidencia que los criterios de clasificación de la información, se alineen con la política global y se apliquen en la valoración de los activos. No conforme	Procedimiento de etiquetado de activos de información, pero esta clasificación de la información debe alinearse con la política global de SI, verse aplicada en la valoración de activos	Se tiene el procedimiento de gestión de activos.
8.2.2 Etiquetado de la Información	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización	3. Se realiza parcial e informalmente	En el SOA dice que falta ajustar documentación lo que incumpliría el control 7.5 de información documentada. Además de no ser valido entonces que este totalmente implementado el control. No se evidencia que la información esté etiquetada. No conforme	Los repositorios físicos y lógicos o en eplicativos,deben establecer el nivel de acceso permitido, con base en los criterios definidos para clasificar la información	Se tiene el procedimiento de etiquetado de la Información aprobado en Isolucion y publicado en la Intranet.
8.2.3 Manejo de activos	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	3. Se realiza parcial e informalmente	Evidencia de un protocolo y procedimiento para gestión de activos, no se hacen revisiones sobre su aplicación y cumplimiento. No conforme	las revisiones sobre los activos de información deben poder establecer si se están usando de acuerdo con las policías de SI y con los niveles de clasificación de la información definidos	Se tiene el procedimiento de gestión de activos.

- Manejo de Medios.

8.3 MANEJO DE MEDIOS	**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios **Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios**Objetivo:** Evitar la divulgación no autorizada, modificación, supresión o destrucción de la información almacenada en los medios				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
8.3.1 Gestión de los medios removibles	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización	3. Se realiza parcial e informalmente	Procedimiento de gestión de medios removibles. No se evidencia su implementación. No conforme	N/A	N/A
8.3.2 Disposición de medios	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	3. Se realiza parcial e informalmente	Disposición segura de medios, se evidencia el estándar pero no su implementación y mejora	N/A	N/A
8.3.3 Transferencia de medios físicos	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	3. Se realiza parcial e informalmente	Se evidencia el instructivo de transferencia de medios pero no su implementación y mejora	N/A	N/A

- Control de Acceso.

- Requerimientos de Negocio de Control de Acceso.

9 CONTROL DE ACCESO					
9.1 REQUERIMIENTOS DE NEGOCIO DE CONTROL DE ACCESO	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
9.1.1 Politica de Control de Acceso	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información	5. Se realiza formalmente y está documentado	Aplicativo GACEL. Solicitudes para creación de accesos nuevos, validación de la meas de ayuda para validación. Estándar de seguridad para cuentas de usuario. Política de control de acceso.	la política de control de accesos, debe permitir gestionar los accesos de manera segura basados en roles y perfiles y siguiendo el principio de menor privilegio, no solo para los entornos lógicos sino para los entornos físicos	Aplicativo GACEL. Solicitudes para creación de accesos nuevos, validación de la meas de ayuda para validación. Estándar de seguridad para cuentas de usuario. Política de control de acceso. El workflow de aprobaciones considera la segregación de funciones del nivel jerárquico.
9.1.2 Acceso a la redes y servicios de red	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente	3. Se realiza parcial e informalmente	La implementación efectiva de entrega de usuarios y accesos se debe asegurar que cumple con las validaciones para mínimo privilegio y separación de deberes, no se evidencian auditorias sobre accesos. No conforme	los accesos una vez se entreguen de acuerdo con las políticas deben poderse revisar periódica y permanentemente para asegura su uso autorizado	El acceso a recursos de red, se controla mediante DA y reglas de control de accesos en firewall. Periódicamente el equipo de SI verifica que el personal retirado sea inactivado en el DA

- Gestión de Acceso de los Usuarios.

9.2 GESTIÓN DE ACCESO DE LOS USUARIOS	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
9.2.1 Registro y cancelación del registro de usuarios	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso	3. Se realiza parcial e informalmente	Aplicativo GACEL. Solicitudes para creación de accesos nuevos, validación de la meas de ayuda para validación.	Estándar de seguridad para cuentas de usuario. Política de control de acceso	Se tiene implementado el aplicativo Gacel al 100%
9.2.2 Aprovisionamiento del acceso de usuarios	Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios	3. Se realiza parcial e informalmente	Aplicativo GACEL. Solicitudes para creación de accesos nuevos, validación de la meas de ayuda para validación.	Estándar de seguridad para cuentas de usuario. Política de control de acceso	Se tiene implementado parcialmente el acceso de aprovisionamiento a los usuarios.
9.2.3 Gestión de derechos de acceso privilegiados	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado	3. Se realiza parcial e informalmente	Aplicativo GACEL. Solicitudes para creación de accesos nuevos, validación de la meas de ayuda para validación. No conforme	Estándar de seguridad para cuentas de usuario. Política de control de acceso. Tanto la gestión de usuarios estándar como la de altos privilegios, no cumplen con la revisión de los principios de separación de deberes y menor privilegio por parte del área de SI	El aplicativo gacel permite parcialmente gestionar las solicitudes de los usuarios privilegiados.
9.2.4 Gestión de la información secreta de autenticación de los usuarios	La asignación de información de autenticación secreta se debería controlar por medio de un proceso de gestión formal	3. Se realiza parcial e informalmente	las contraseñas se entregan de manera temporal con cambio al primer inicio de sesión, por correo para implementar en sitio por un funcionario de soporte. La politica esta mal definida por cuanto permite que un tercero use la contraseña a nombre del titular y se envían junto con el usuario para acceso. No conforme	la gestión de contraseñas es de carácter confidencial y privado para cada usuario, nadie aparte de el debe conocerla ni siquiera la temporal	la gestión de contraseñas es de carácter confidencial y privado para cada usuario, nadie aparte de el debe conocerla ni siquiera la temporal. El sistema GACEL y el DA aseguran que las contraseñas sean secretas.
9.2.5 Revisión de los derechos de acceso de los usuarios	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares	2. No se realiza	Se está haciendo una revisión en este momento de los usuarios de aplicativos por iniciativa del área de seguridad de la información, no forma parte de un procesos establecidos. No conforme	N/A	Este control es responsabilidad de los usuarios custodios y responsables de la información
9.2.6 Eliminación o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	2. No se realiza	Se está haciendo una revisión en este momento de los usuarios de aplicativos por iniciativa del parea de seguridad de la información, no forma parte de un procesos establecido	N/A	Este control es responsabilidad de los usuarios custodios y responsables de la información

- Responsabilidades de los Usuarios.

9.3 RESPONSABILIDADES DE LOS USUARIOS	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
9.3.1 Uso de la información secreta de autenticación	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta	3. Se realiza parcial e informalmente	Política de gestión de usuarios y contraseñas, no se evidencian auditorias sobre el uso de las contraseñas. No conforme	N/A	La responsabilidad recae sobre los usuarios, la STI no tiene forma de obligarlos a cumplir las reglas y normativas de SI. El control debería ser implementado en Talento Humano con apoyo de la Dirección General.

- Control de Acceso de Sistemas y Aplicaciones.

9.4 CONTROL DE ACCESO DE SISTEMAS Y APLICACIONES	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
9.4.1 Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	2. No se realiza	No se evidencia que haya separación de deberes en dispositivos críticos como el firewall y tampoco se hace auditoria sobre este tipo de usuarios. Hay un riesgo alto por mala definición, implementación y revisiones sobre las políticas de accesos. No conforme	la política de control de accesos, debe permitir gestionar los accesos de manera segura basados en roles y perfiles y siguiendo el principio de menor privilegio, no solo para los entornos lógicos sino para los entornos físicos	Todos los sistemas tienen sistema de control de accesos single sigan on via directorio activo.
9.4.2 Procedimientos de inicio de sesión seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	4. Se realiza informalmente en forma total	Se genera una contraseña temporal y se solicita cambio inmediato. Tiene un nivel de seguridad dada por la intervención del equipo de soporte en la primera configuración. Hay riesgos no identificados con este proceso como esta implementado en este momento. No conforme	los inicios de sesión deben asegurar que solo el usuario autorizado lo realiza, alineado con la política general de accesos y los principios de seguridad existentes en este sentido.	Los sistemas tienen control de accesos con cumplimiento de requisitos mínimos en cuanto a la creación de password y su vigencia. No se cuenta con control anti robot ni ataques de fuerza bruta.
9.4.3 Sistema de Gestión de contraseñas	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas	2. No se realiza	N/A	N/A	La calidad de las contraseñas depende de lo usuarios, los sistemas de información ofrecen la posibilidad de combinar caracteres que ofrecen alto nivel de complejidad.
9.4.4 Uso de programas utilitarios privilegiados	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	4. Se realiza informalmente en forma total	Se evidencian controles sobre descarga no autorizada de software		Existe restricción en el uso de programas y utilitarios no autorizados por las áreas responsables de la información. Desde la Dirección de Infraestructura y Soporte de TI se realiza escaneo periódico para controlar el uso de herramientas y software no autorizado
9.4.5 Control de acceso al código fuente de los programas	Se debería restringir el acceso a los códigos fuente de los programas.	2. No se realiza	No se evidencio en la auditoria. No conforme	N/A	El código fuente de los ambientes de desarrollo y de producción son protegidos y restringidos en acceso. Sólo los desarrolladores autorizados y el administrador de los servidores tiene acceso

- Criptografía.

- Controles Criptográficos.

10 CRIPTOGRAFIA					
10.1 CONTROLES CRIPTOGRÁFICOS	Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
10.1.1 Política sobre el uso de controles criptográficos	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información	4. Se realiza informalmente en forma total	política sobre uso de controles criptográficos y política de gestión de llaves de cifrado. No conforme	Se mencionan directrices de controles criptográficos que no están en cumplimiento	La entidad no cuenta con medios para cifrado de datos, medios, o canales.
10.1.2 Administración de llaves	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	4. Se realiza informalmente en forma total	Se evidencia incumplimiento de lo establecido en la política de controles criptográficos. No conforme	Se evidencia incumplimiento de lo establecido en la política de controles criptográficos	No se cuenta con llaves criptográficas.

- Seguridad Física y Ambiental.

- Áreas Seguras.

11 SEGURIDAD FÍSICA Y AMBIENTAL					
11.1 ÁREAS SEGURAS	Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
11.1.1 Perímetro de Seguridad Física	Los perímetros de seguridad deben ser definidos y utilizados para proteger las áreas que contienen tanto la información como las "information processing facilities" sensible o críticas.	2. No se realiza			La DSA, implemento Sistema de control de acceso a nivel central y algunas regionales. La STI tiene un nivel mas de seguridad de acceso a sus oficinas.
11.1.2 Controles de ingreso físico	Las áreas seguras deben ser protegidas con apropiados controles de ingreso para asegurar que sólo el personal autorizado tenga permitido el acceso.	2. No se realiza			La DSA, implemento Sistema de control de acceso a nivel central y algunas regionales. La STI tiene un nivel mas de seguridad de acceso a sus oficinas.
11.1.3 Asegurando oficinas, salas e instalaciones	La seguridad física para oficinas, salas e instalaciones debe ser diseñada y aplicada.	2. No se realiza			La DSA, implemento Sistema de control de acceso a nivel central y algunas regionales. La STI tiene un nivel mas de seguridad de acceso a sus oficinas.
11.1.4 Protección contra amenazas externas y ambientales	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	2. No se realiza			Se cuenta con seguridad física, CCTV, perímetro cerrado, y guardias de seguridad
11.1.5 Trabajando en áreas seguras	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	2. No se realiza			La entidad cuenta con grupos de SST y salud ocupacional
11.1.6 Zonas de despacho y carga	Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	2. No se realiza			Las zonas de despacho y carga de almacenes cuenta con CCTV y vigilancia

- Equipamiento.

11.2 EQUIPAMIENTO	Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
11.2.1 Ubicación y protección de equipos	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	2. No se realiza	No se evidenciaron protecciones específicas sobre los activos de acuerdo su valoración. No conforme	los accesos físicos permiten acceder a activos sin clasificar que potencialmente podrían representar un riesgo para la entidad	Los equipos tienen control de acceso temporizado via descansa pantallas. Las zonas de ubicación y su seguridad no le corresponde a la Dirección de Infraestructura y Soporte de T.I.
11.2.2 Servicios de Suministro	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	4. Se realiza informalmente en forma total	de acuerdo a la entrevista hay planta eléctrica, no hay estrategias que garanticen suministros de otros insumos principales como agua o esquemas de contingencia para internet		La administración, control, respaldo y monitoreo del fluido eléctrico no es responsabilidad de la Dirección de Infraestructura y Soporte de TI
11.2.3 Seguridad del Cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	4. Se realiza informalmente en forma total	el cableado es certificado		La administración, control, respaldo y monitoreo de áreas físicas y canaletas de cableado no es responsabilidad de la Dirección de Infraestructura y Soporte de TI Los racks y nodos de cableado son vigilados y monitoreados por el área administrativa seguridad física
11.2.4 Mantenimiento de equipos	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	2. No se realiza	hay un procedimiento de mantenimiento, en la auditoria no se evidencio mantenimiento preventivo sobre equipos críticos ni un programa en ejecución de mantenimientos programados sobre los activos de información y los dispositivos y elementos de red. No conforma		Se realiza mantenimiento de equipos una vez al año.
11.2.5 Retiro de activos	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	4. Se realiza informalmente en forma total	Hay un procedimiento establecido en funcionamiento, no se ha medido su efectividad respecto a SI. No conforme	N/A	Existe control físico de ingreso y retiro de equipos en las porterías de los edificios. El retiro de equipos portátiles requiere registro de los mismos.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	3. Se realiza parcial e informalmente	Se evidencia el estándar, no hay evidencia de su implementación. No conforme	los equipos que son trasladados por autorización especifica o razones de negocio deben tener acuerdos expresos sobre la responsabilidad, esquemas de respaldo y otras precauciones que la entidad determine para consenar los principios de seguridad del activo mientras esta fuera de las instalaciones	Los equipos conectados a la red de la entidad están sometidos a las mismas reglas de seguridad y respaldo que aplica para todos los equipos. La seguridad física es responsabilidad del portador.
11.2.7 Disposición segura o reusó de equipos	Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	2. No se realiza	Se evidencia el estándar, no hay evidencia de su implementación	N/A	La reasignación de equipos cuenta con un checklist que considera la actividad de "respaldo y borrado seguro".
11.2.8 Equipo del usuario desatendido	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	5. Se realiza formalmente y está documentado	Se evidencia la política implementada, falta hacer revisiones periódicas de cumplimiento	N/A	Existe control temporizado de inactividad de los equipos mediante bloqueo de pantalla.
11.2.9 Política de pantalla y escritorio limpio	Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información	5. Se realiza formalmente y está documentado	Se evidencia la política implementada, falta hacer revisiones periódicas de cumplimiento	N/A	Se realiza adecuadamente

- Seguridad de las Operaciones.

- Procedimientos y Responsabilidades Operacionales.

12 SEGURIDAD DE LAS OPERACIONES					
12.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
12.1.1 Procedimientos operacionales documentados	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten	5. Se realiza formalmente y está documentado			Existe documentación técnica, y de usuario para los sistemas de información y servicios de TI. En cuanto a operación de las plataformas servidores y consolas, existe documentación técnica disponible en redes y portales de los fabricantes.
12.1.2 Gestión del cambio	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	5. Se realiza formalmente y está documentado	Procedimiento de cambios en la infraestructura, las solicitudes de cada administrador de componentes, hacia comité de cambios	registro de comité de cambios. Criterios de valoración de la categoría del cambio alineados con ITIL3, riesgos	Se cuenta con un procedimiento de control de cambios documentado. Todo cambio debe pasar por un comité primario de cambios.
12.1.3 Gestión de la capacidad	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura	5. Se realiza formalmente y está documentado	Procedimiento de gestión de la capacidad y disponibilidad de los recursos de red	se hace un monitoreo mediante la herramienta de monitoreo, operación bridge microfocus hace monitoreo permanente y genera alertas para cada administrador de aplicativo, monitoreo por parte de los operadores de centro de cómputo envían alertas	se hace un monitoreo mediante la herramienta de monitoreo, operación bridge micrococos hace monitoreo permanente y genera alertas para cada administrador de aplicativo, monitoreo por parte de los operadores de centro de cómputo envían alertas
12.1.4 Separación de los ambiente de producción, desarrollo y pruebas	Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	3. Se realiza parcial e informalmente	No conforme	No tienen segmentación de red	Los ambientes de desarrollo, QA, pruebas y producción están separados. En cuanto a segmentación de red (¿?) se viene trabajando en el rediseño de la red y su segmentación.

- Protección Contra el Malware.

12.2 PROTECCIÓN CONTRA EL MALWARE	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
12.2.1 Controles contra el malware	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	4. Se realiza informalmente en forma total	Se usa IPS y el Gateway de la plataforma McAfee, se instala un apply instalado en el datacenter para 3300 usuarios, las políticas están en construcción, No se hacen auditorias o acciones de mejora con base en los reportes del antimalware	Se gestiona de manera centralizada por infraestructura. Contrato de soporte y monitoreo. Falta un proceso de gestión sobre las alertas y la información que genera el anti malware	Contra malware que no sea ramsonware se cuenta con antivirus McAfee y una consola ePO con alertamiento y un funcionario a cargo que monitorea los eventos parametrizados

- BACKUP.

12.3 BACKUP	Objetivo: Proteger contra la pérdida de datos.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
12.3.1 Respaldo de la Información	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	4. Se realiza informalmente en forma total	Back ups diarios, semanales, mensuales, anuales, base de datos diario, bog7, particiones graduales, conservación hasta por 10 años de acuerdo con las tables de retención documental. Políticas de back up, quedan en un servidor en el centro de datos, se hacen copias en cintas y se llevan a almacenamiento externo con MTI el resguardo, el proveedor ofrece mediante los ANS los esquemas de contingencia.No conforme en las pruebas de contingencia	Los respaldos deben probarse y los acuerdos con terceros que garanticen contingencias sobre los back ups deben formalizarse	Se realiza respaldo continuo de los datos con frecuencia diaria, semanal, mensual y anual. En algunos casos se realizan fullexport de bases de datos criticas.

- Registro y Monitoreo.

12.4 REGISTRO Y MONITOREO	Objetivo: Registrar eventos y generar evidencia				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
12.4.1 Registro de eventos	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	3. Se realiza parcial e informalmente	Cada administrador gestión los logs. No conforme	No se evidencia un proceso de gestión centralizada de eventos	Existe una consola EPO para alertamiento, monitoreo, y control de eventos a nivel de la red y los usuarios finales. En plataformas se monitorea y gestiona los eventos via software de monitoreo Bridge
12.4.2 Protección de la información de registros	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	3. Se realiza parcial e informalmente	Se gestionan dentro de los back ups. No conforme	los registros de logs, son información confidencia	Los logs de ambiente Windows, Linux, y de los equipos activos de red (switches y firewall) se llevan en un servidor con control de acceso.
12.4.3 Registros de operadores y administradores	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad	3. Se realiza parcial e informalmente	Los registros se les genera back up pero no se hace gestión sobre los eventos de los administradores. No conforme	Los administradores son superusuarios sobre los que se deben hacer procesos permanentes de auditorias	Se cuenta con losgs de los servidores, se hace revisión solo en caso de incidentes
12.4.4 Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo	4. Se realiza informalmente en forma total	Servidor NTP en el centro de computo que se sincroniza con el servicio de Microsoft. No se evidencio en la auditoria su aplicación	N/A	Los relojes de servidores y equipos están sincronizados y son monitoreados via consola de eventos.

- Control del Software Operativo.

12.5 CONTROL DEL SOFTWARE OPERATIVO	Objetivo: Asegurar la integridad de los sistemas operacionales				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
12.5.1 Instalación de software en sistemas operacionales	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	5. Se realiza formalmente y está documentado	Los equipos tienen sesión de usuario y no administrador, se instala a través de la mesa de ayuda	N/A	Todos los equipos tienen sistemas operativos, pero no es claro a que se refiere con la instalación de software en dichos equipos. La Dirección de Infraestructura y Soporte de TI controla el uso de herramientas y software no autorizado en la entidad.

- Gestión de las Vulnerabilidades Técnicas.

12.6 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
12.6.1 Gestión de las Vulnerabilidades Técnicas	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	3. Se realiza parcial e informalmente	La gestión de vulnerabilidades está documentada, no se evidencia un protocolo de actualización programada y preventiva del software, ni los reportes de vulnerabilidades que vengan de incidentes y/o de vulnerabilidad en el código. Las actualizaciones de Windows se notifican por las actualizaciones lanzadas por el fabricante. No conforme	Guía para le ejecución de pruebas de seguridad. Se han hecho escaneos en febrero 2021, las brechas del reporte no han sido tratadas.	Se realiza anualmente proyectos de ética hacking para detectar vulnerabilidades y remediarlas en la medida de lo posible. Se hacen pruebas de caja negra, fuerza bruta, caja gris, y campañas de phising.
12.6.2 Restricciones en la instalación del Software	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	5. Se realiza formalmente y está documentado	Los equipos tienen sesión de usuario y no administrador, se instala a través de la mesa de ayuda	N/A	La Dirección de Infraestructura y Soporte de TI controla y monitorea el uso de herramientas y software no licenciado o no autorizado en los equipos de la entidad.

- Consideraciones de la Auditoría de los Sistemas de Información.

12.7 CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
12.7.1 Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio	2. No se realiza	No se videncia gestión sobre los informes de auditoria. No conforme	las auditorias sobre los informes de eventos o registros de auditoria, son clave para asegurar una gestión proactiva de todo log en la red, si esto no se hace todos los elementos físicos y lógicos pueden estar siendo vulnerados y no ha sido detectado	No se han realizado auditorias a los sistemas de información.

- Seguridad de las Comunicaciones.

- Gestión de la Seguridad de las Redes.

13 SEGURIDAD DE LAS COMUNICACIONES					
13.1GESTIÓN DE LA SEGURIDAD DE LAS REDES	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
13.1.1 Controles de redes	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	2. No se realiza	No se evidencio en la auditoria. No conforme	la gestión de redes incluye reglas y políticas aplicadas y auditadas para segmentar grupos y equipos de trabajo, alineado esto con la política de gestión de accesos y de usuarios, aplicando y cumpliendo el principio de separación e deberes y menor privilegio. Este control se debe implementar tanto para las segmentaciones de red internas como para los servicios contratados o suministrados por terceros	Se realiza monitore y gestión de la red con ayuda de herramientas como Solarwinds NMNI. Algunos equipos de red no son gestionables por obsolescencia y requieren cambio. En lso equipos gestionables se controla y gestiona la seguridad en cuanto al acceso y parametrización, y la implementación de políticas de seguridad.
13.1.2 Seguridad de los servicios de red	Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	2. No se realiza	No se evidencio en la auditoria. No conforme		
13.1.3 Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes	2. No se realiza	No se evidencio en la auditoria. No conforme		

- Transferencia de Información.

13.2 TRANSFERENCIA DE INFORMACIÓN	Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
13.2.1 Políticas y procedimientos de transferencia de información	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	2. No se realiza	No se evidencio en la auditoria. No conforme	los acuerdos con terceros sobre transferencia de información, deberían generar los controles y procedimientos que garanticen su cumplimiento, p.ej. Carpetas con acceso seguro, conexiones con punto a punto, servicios web con protocolos seguros, carpetas o directorios SFTP, entre otros que la entidad determine y acuerde cuando genere acuerdos de transferencia	Las definiciones de politicasy procedimientos de protección de los datos y la información no es del alcance de la Dirección de Infraestructura y Soporte de TI. La clasificación y valoración de activos de información no es responsabilidad de la Dirección de Infraestructura y Soporte de TI En la STI se cuenta con la firma de "Acuerdos de confidencialidad" con terceros y contratistas para efectos de compartir información.
13.2.2 Acuerdos sobre transferencia de información	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas	2. No se realiza	No se evidencio en la auditoria. No conforme		
13.2.3 Mensajería electrónica	Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	3. Se realiza parcial e informalmente	hay politica, no hay evidencia de controles o procesos de revisión que aseguren su cumplimiento. No conforme	N/A	Aunque Outlook y Exchange ofrecen controles de etiquetado de información y manejo de privacidad y confidencialidad de información, estos controles aún no se utilizan en la entidad.
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	2. No se realiza	No se evidencio en la auditoria. No conforme	N/A	En la STI se cuenta con la firma de "Acuerdos de confidencialidad" con terceros y contratistas para efectos de compartir información. Su gestión, control y seguimiento no es responsabilidad de la Dirección de Infraestructura y Soporte de T

- Adquisición, Desarrollo y Mantenimiento de Sistemas.
- Requisitos de Seguridad de los Sistemas de Información.

14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
14.1.1 Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	1	Se hacen solicitudes al área grupo de proyectos de tecnología, ellos buscan soluciones creadas. No se generan interacciones con el grupo que hace desarrollo. Ellos proceden a buscar en el mercado soluciones existentes. No conforme, no se establecen por politica y procedimiento requisitos de SI en la adquisición o desarrollo de software o aplicaciones	Se hacen solicitudes al área grupo de proyectos de tecnología, ellos buscan soluciones creadas. No se generan interacciones con el grupo que hace desarrollo. Ellos proceden a buscar en el mercado soluciones existentes	Desde la Dirección de Infraestructura no se cuenta con un protocolo o procedimiento para desarrollo seguro o para solicitar cumplimientos de requerimientos de seguridad en sistemas de información que se adquieren. Las áreas usuarias que adquieren software de aplicación no aplican o definen requerimientos de controles respecto a nivel de seguridad que ofrecen los proveedores.
14.1.2 Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas	3. Se realiza parcial e informalmente	Metodología de desarrollo seguro en implementación. No conforme	Estándar de desarrollo seguro, procedimiento de aseguramiento y adquisición de software. No se evidencia que solicite el establecimiento y revisión de los requisitos de SI Todo está en implementación no se evidencia su cumplimiento	Ahora bien, con la transformación institucional, el Grupo de Proyectos de Tecnologías de la Información dejó de existir. No obstante, desde la Dirección de Información y Sistemas de TI para el proyecto de Solución tecnológica de la Secretaría de Autoridad para los procesos de
14.1.3 Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	2. No se realiza	No se evidencia su implementación. No conforme	Esta excluida en el SOA, el argumento es no transacciones financieras, pero este no es el concepto correcto para la exclusión. El control 14.1 hace referencia a establecer requisitos de seguridad, las transacciones no necesariamente son financieras, intercambio de información, una autorización, una consulta, son transacciones de información	El sistema transaccional SIAF (JDE) cuenta con controles de aseguramiento de finalización y completitud de transacciones.

- Seguridad en los Procesos de Desarrollo y de Soporte.

14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
14.2.1 Política de desarrollo seguro	Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización	2. No se realiza	Políticas de seguridad y privacidad de la información. No se evidencia su implementación> No conforme	N/A	No existen mecanismo ni protocolos de desarrollo seguro
14.2.2 Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios	2. No se realiza	No se evidencia su implementación, medición y mejora. No conforme	N/A	Existe un procedimiento y un comité de control de cambios
14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma operativa	Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	2. No se realiza	No se evidencia su implementación, medición y mejora. No conforme	N/A	La Dirección de Infraestructura y Soporte de TI no tiene recursos suficientes para este tipo de controles. No se aplican, no existen
14.2.4 Restricciones en los cambios a los paquetes de software	Las modificaciones a los paquetes de software deben desestimarse, limitarse a los cambios necesarios y todos los cambios deben controlarse estrictamente	2. No se realiza	No se evidencia su implementación, medición y mejora. No conforme	N/A	Existe un procedimiento y un comité de control de cambios
14.2.5 Principios de construcción de sistemas seguros	Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	2. No se realiza	Dos equipos de desarrollo, se reciben requerimientos funcionales y/o mantenimiento. Solo funcionales, SCRUM como metodología. Procedimiento de desarrollo seguro de software, listo para aprobación por el SGC. No se evidencia su implementación, medición y mejora. No conforme	N/A	No existen mecanismo ni protocolos de desarrollo seguro
14.2.6 Ambiente de desarrollo seguro	Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	2. No se realiza	No se tiene roles y perfiles para el acceso al código fuente, a pesar que si saben que usuarios tienen acceso al código fuente dentro del área. Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. No conforme	N/A	No existen mecanismo ni protocolos de desarrollo seguro
14.2.7 Desarrollo contratado externamente	La organización debería supervisar y hacer seguimiento de la actividades de desarrollo de sistemas contratados externamente	2. No se realiza	No se evidencia su implementación, medición y mejora. No conforme	N/A	No existen mecanismo ni protocolos de desarrollo seguro, y no se hace seguimiento al desarrollo de software que realizan contratistas.
14.2.8 Pruebas de seguridad de sistemas	Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad	2. No se realiza	No se evidencia su implementación, medición y mejora. No conforme	N/A	No existen mecanismos ni protocolos de desarrollo seguro
14.2.9 Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	2. No se realiza	No se evidencia su implementación, medición y mejora. No conforme	N/A	Existen ambientes de prueba y se realizan pruebas a cambios en lso sistemas

- TEST DATA.

14.3 TEST DATA	Objetivo: Asegurar la protección de los datos usados para pruebas				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
14.3.1 Protección de datos de prueba	Los datos de prueba se deberían seleccionar, proteger y controlar cuidadosamente	2. No se realiza	No se evidencia su implementación, medición y mejora. No conforme	N/A	N/A

- Gestión de Incidentes de Seguridad de la Información.

- Gestión de Incidentes de Seguridad de la Información y Mejoras.

16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
16.1. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
16.1.1 Responsabilidades y Procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	3. Se realiza parcial e informalmente	Hubo un incidente en agosto de 2021, lo gestionó a direccion informática, se cayo el servidor de archivos. El procedimiento existe en implementación. No conforme	Un equipo dedicado y formalmente asignado para gestionar de manera integral y proactiva los incidentes en SI es requerido para cumplir con este control. No solamente incidentes en los dispositivos de red, las violaciones a las políticas, la materialización de un riesgo, entro otros, forman parte de la gestión integral de incidentes	Existe un procedimiento de gestión de incidentes, pero aún no ha sido implementado
16.1.2 Reportar los eventos de Seguridad de la Información	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	3. Se realiza parcial e informalmente	Informe de direccion informática comité directivo 16 mayo 2021. se revisó el incidente, como caso puntual no como parte de un proceso integral de gestión de incidentes en SI. No conforme	N/A	La mesa de ayuda atiende a través de los medios autorizados, los reportes y/o solicitudes asociadas a eventos de seguridad de la información.
16.1.3 Reportar las debilidades de Seguridad de la Información	Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	3. Se realiza parcial e informalmente	No se evidencio un canal permanente para reportar incidentes de manera interna. No conforme	N/A	Se tiene el canal de linea3000, como punto único de contacto para reportar lo eventos de seguridad.
16.1.4 Evaluación de y decisión sobre los eventos de Seguridad de la Información	Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información	2. No se realiza	No se evidencia cumplimiento dado que los eventos de seguridad no se están gestionando. No conforme	N/A	Se atiende desde L3000 en primer nivel, se analiza y si el evento se escala al equipo de ciberseguridad y seguridad digital.
16.1.5 Respuesta a los Incidentes de Seguridad de la Información	Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados	3. Se realiza parcial e informalmente	Se han gestionado incidentes puntuales una vez se detecta su ocurrencia, no se evidencia un plan y equipo de respuesta a incidentes establecido permanente y formalmente. No conforme	N/A	Se gestionan los incidentes de acuerdo al procedimiento y la guía de incidentes de seguridad.
16.1.6 Aprendiendo de los Incidentes de Seguridad de la Información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	2. No se realiza	No se evidencia su implementación. No conforme		Teniendo en cuenta que la trazabilidad de los casos se gestiona a través de la mesa de ayuda, se cuenta con una base de conocimiento, que puede ser accedida desde Aranda.
16.1.7 Colección de la evidencia	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	2. No se realiza	No se evidencio la implementación, medición y mejora de un procedimiento para colección de evidencias. No conforme	N/A	Dentro del proyecto de ciberseguridad que se está estructurando, se incluye la implementación de un sistema de investigación forense, el cual incluye todas las etapas del análisis forense (recolectar, preservar, etc.)

- 17 Aspectos de la Seguridad de la Información de la Gestión de Continuidad del Negocio.
- Continuidad de la Seguridad de la Información.

17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO					
17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
17.1.1 Planeación de la Continuidad de Seguridad de la Información	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	3. Se realiza parcial e informalmente	Política y esquemas de continuidad y contingencia, no se evidencia implementación ni pruebas de continuidad sobre las estrategias que involucran la seguridad de la información	N/A	Se tiene un procedimiento de la gestión de continuidad de negocio, no se ha implementado.
17.1.2 Implementación de la Continuidad de Seguridad de la Información	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	2. No se realiza	Política y esquemas de continuidad y contingencia, no se evidencia implementación ni pruebas de continuidad sobre las estrategias que involucran la seguridad de la información	N/A	Se tiene un procedimiento de la gestión de continuidad de negocio, no se ha implementado.
17.1.3 Verificar, revisar y evaluar la Continuidad de la Seguridad de la Información	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas	2. No se realiza	Política y esquemas de continuidad y contingencia, no se evidencia implementación ni pruebas de continuidad sobre las estrategias que involucran la seguridad de la información	N/A	Se tiene un procedimiento de la gestión de continuidad de negocio, no se ha implementado.

- Redundancias.

17.2 REDUNDANCIAS	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información				
CONTROLES	DESCRIPCIÓN DEL CONTROL	ESTADO DE IMPLEMENTACIÓN 2021	OBSERVACION VIGENCIA - 2021	RECOMENDACIÓN - VIGENCIA 2021	ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022
17.2.1 Disponibilidad de las "información processing facilities"	Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad	2. No se realiza	Política y esquemas de continuidad y contingencia, no se evidencia implementación ni pruebas de continuidad sobre las estrategias que involucran la seguridad de la información	N/A	Se esta implementando el datacenter alterno en el Cgac

8.5. Gestión reportada por la Secretaría General sobre las observaciones reportadas en el informe de la Auditoría Externa.

- 5.1. Liderazgo.

5 Liderazgo					
CONTROLES	DESCRIPCIÓN DEL CONTROL	ESTADO DE IMPLEMENTACIÓN 2021	OBSERVACION VIGENCIA - 2021	RECOMENDACIÓN - VIGENCIA 2021	ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022
5.1 Liderazgo y compromiso					
1. ¿Los objetivos generales del SGSI son compatibles con la dirección estratégica?	Para ser más valioso, un SGSI debe apoyar el logro de los objetivos de negocio, y para asegurar mejor esto, los objetivos propuestos deben estar alineados con la dirección estratégica.	4. Se realiza informalmente en forma total	Se evidencia en el plan nacional de desarrollo, Plan de navegación aérea, plan institucional PEI y plan de acción anual desde la meta 110 hasta la 133 como objetivos que indican la necesidad de implementar un SGSI. En el Comité de gestión institucional se revisa el cumplimiento de los objetivos, los objetivos del SGSI son compatibles. Los indicadores no miden los objetivos del SGSI. No se evidencia establecimiento de objetivos de seguridad de la información, solo objetivos del SGSI, estos no están alineados con los objetivos institucionales.	Incluir una estrategia específica que muestre la gestión sobre la implementación y mejora del SGSI, dentro del plan de seguimiento, ajustar la redacción de los objetivos del SGSI para que corresponda con los indicadores del SGSI.	**El área no reporto información**
2. ¿La dirección garantiza los recursos necesarios para el SGSI cuando sea necesario?	Un SGSI sin recursos en el momento adecuado no puede lograr sus objetivos, la dirección tiene que asegurar que estos recursos están disponibles cuando sea necesario.	4. Se realiza informalmente en forma total	Se evidencia un Anteproyecto de presupuesto en abril de cada año, alineado con las metas institucionales a las que se les hace seguimiento trimestral. Se utiliza el presupuesto y el procedimiento de elaboración del presupuesto anual de la entidad regulado por la ley.	Se recomienda que las partidas presupuestales incluyan específicamente la implementación y la operación del SGSI y que cubran las inversiones por riesgos futuros.	**El área no reporto información**
3. ¿La dirección asegura que el SGSI logra sus resultados previstos?	Un SGSI que no puede ofrecer los resultados esperados es un fracaso, aunque opere según lo planeado y utilizando menos recursos de los esperado. Para evitar esto, la dirección debe asegurar que el 'SGSI ha conseguido los resultados propuestos.	2. No se realiza	En el manual SGSI, hay objetivos del SGSI, no se miden. No hablan de los planes para su cumplimiento. No conforme porque los indicadores no miden los objetivos y no están alineados en conjunto.	El objetivo institucional debe alinearse con los objetivos de Seguridad y con los objetivos del SGSI. Estos deben medirse y generarse el ciclo de mejora continua posterior a su medición.	**El área no reporto información**
5.2 Política					
1. ¿Existe una política de seguridad de la información con objetivos definidos o un marco para el establecimiento de objetivos?	La alta dirección debe definir la política de seguridad de la información dentro del alcance del SGSI. La política necesita ser apropiada a sus actividades, incluir un compromiso de mejora continua y proporcionar objetivos o un marco para su establecimiento.	4. Se realiza informalmente en forma total	La política se evidencia documentada en el manual SGSI, este manual fue aprobado en el repositorio. La política no establece un marco para su establecimiento dado que no hace referencia al tipo de información y los niveles de criticidad que son relevantes para la entidad.	Una declaración de política de seguridad de la información, debe permitir a todas las partes interesadas, entender y determinar el nivel o niveles de criticidad o de sensibilidad que tienen los diferentes tipos de información y datos que maneja la entidad, debe además servir como plataforma para la gestión de riesgos y la valoración de activos en función de la información que procesan, almacenan o transportan.	**El área no reporto información**
2. ¿La política de seguridad de información está documentada y es comunicada dentro de la empresa y a otras partes interesadas?	La política debe ser documentada, comunicada a los empleados y estar a disposición de otras partes interesadas.	3. Se realiza parcial e informalmente	La política está documentada y aprobada en el manual del SGSI. No se evidencia que sea conocida por las partes interesadas durante el desarrollo de las entrevistas de la auditoría.	La política debe ser conocida por todas las partes interesadas definidas en el alcance, las actividades del programa de capacitaciones deben asegurar que este entendimiento se da de manera efectiva.	**El área no reporto información**
5.3 Roles, responsabilidades y autoridades en la organización					
1. ¿Están asignadas y comunicadas los roles, responsabilidades y autoridades para la seguridad de la información?	La responsabilidad y autoridad debe ser asignada por la alta dirección para organizar las actividades de seguridad de la información, para asegurar que el SGSI es conforme a ISO 27001:2013 y que existe un reporte del rendimiento del SGSI a la alta dirección.	3. Se realiza parcial e informalmente	En el manual SGSI, No se evidencian las responsabilidades frente al SGSI, se evidencia que área es responsable de la política pero no cuales son esas responsabilidades, no se comunicaron y aceptaron formalmente estas responsabilidades. En la Guía de roles y responsabilidades para SGSI y en Caracterización de procesos establecen las responsabilidades en SÍ, están definidas las responsabilidades pero no se han aceptado formalmente. La entidad no tiene un líder formal del SGSI lo que incumple el requisito de la norma.	Las responsabilidades frente al SGSI no están asignadas formalmente	**El área no reporto información**

8.5.1. Gestión adelantada por la Dirección Administrativa sobre las observaciones reportadas en el informe de la Auditoría Externa.

- 15. Relación con proveedores.

15 RELACIÓN CON PROVEEDORES					
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
15.1. SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON LOS PROVEEDORES	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
15.1.1 Política de Seguridad de la Información para la relación con los proveedores	Requisitos de Seguridad de la Información para mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización deben ser acordados con el proveedor y debe ser documentados	3. Se realiza parcial e informalmente	Política para gestión de proveedores. Pr16 procedimiento seguridad proveedores. No conforme	En aprobación para implementación. Se emplean pliegos tipo, no se pueden modificar	**Sin información del área**
15.1.2 Abordando la seguridad dentro de los acuerdos con los proveedores	Todos los requisitos de seguridad de la información relevante deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de la infraestructura de TI para la información de la organización	3. Se realiza parcial e informalmente	Se encargan de elaborar los contratos, las áreas envían las solicitudes, se asigna a un abogado, procedimiento del manual de contratación. No conforme	supervisores del contrato, son los que monitorean los aspectos durante la vigencia del contrato	**Sin información del área**
15.1.3 Cadena de suministro de tecnología de información y comunicación	Los acuerdos con los proveedores debe incluir requerimientos para abordar los riesgos de seguridad de la información relacionados con los servicios de tecnologías de la información y las comunicaciones y la cadena de entrega de los productos.	2. No se realiza	Se preserva la privacidad enfocada en competencia y contratación transparente. No conforme	El área solicitante es la responsable de establecer y monitorear los ANS, en cabeza de los supervisores del contrato.	**Sin información del área**
15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE LOS PROVEEDORES	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.				
15.2.1 Monitoreo y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	5. Se realiza formalmente y está documentado	La entidad debe permitirse evaluar, informe de revisión y ejecución por el supervisor del contrato mensualmente, permite medir los cumplimientos. Al hacer la liquidación de los contratos, se hace la reevaluación y prestación satisfactoria del contrato	Conformidad por el control que se hace	**Sin información del área**
15.2.2 Gestión de cambios en los servicios de los proveedores	Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	2. No se realiza	supervisores del contrato, son los que monitorean los aspectos durante la vigencia del contrato. No se cubren los cambios en requisitos de SI en este momento. No conforme	N/A	**Sin información del área**

8.5.2. Gestión adelantada por la Dirección de Gestión Humana sobre las observaciones reportadas en el informe de la Auditoría Externa.

- 7 Seguridad del Recurso Humano.

7 SEGURIDAD DEL RECURSO HUMANO					
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
7.1 PREVIO A LA CONTRATACIÓN	**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados. **Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.**Objetivo:** Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuadas para los roles para los cuales ellos son considerados.				
7.1.1 Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos	3. Se realiza parcial e informalmente	Se evidencia que la perdida de información de los procesos de nómina , se tiene identificado como un riesgo, se identifican los diferentes repositorios críticos del área, se identifican los activos críticos y la información crítica, se gestionan accesos establecidos de acuerdo a la criticidad del acceso a los repositorios, historias clínicas y repositorios médicos, bases de datos de evidencias epidemiológicas y gestión psicológica se manejan como confidenciales. Se tiene conciencia de los riesgos asociados al tipo de información. Proyectos como la depuración de accesos deben tener un plan de tratamiento para mostrar PHVA. No conforme	4 coordinaciones de talento humano. Procedimiento de vinculación de personal, no se evidencia que la dirección de talento humano realice estudio de seguridad, se van implementar en respuesta a incidentes que se han presentado.	**El área no reporto información**
7.1.2 Términos y condiciones de empleo	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	2. No se realiza	No se evidencian clausulas respecto a confidencialidad , ley de protección de datos, propiedad intelectual. No conforme	N/A	**El área no reporto información**
7.2 DURANTE EL EMPLEO	**Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información. **Objetivo:** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.				
7.2.1 Responsabilidades de la Dirección	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización	5. Se realiza formalmente y está documentado	Plan estratégico de talento humano, nomina, administrativo SG SST, plan institucional de capacitación establece las responsabilidades	N/A	**Sin información del área**
7.2.2 Concienciación, educación y entrenamiento en Seguridad de la Información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo	3. Se realiza parcial e informalmente	Se han hecho sensibilizaciones mediante la construcción de la matriz de activos, PIC plan institucional de capacitación alineado con los objetivos del plan institucional, plan estratégico de la entidad, la capacitación se registra en el aplicativo Alejandría, planes nacionales de instrucción de carácter obligatorio. No se evidencia madurez en los procesos de capacitación en los temas del SGSI. No conforme	Desde 2018, se ha dentro del PIC 3 niveles de escenarios para capacitación, servidor publico 4.0, transformación digital, haberes esenciales incorporar el SGSI, específicos y especializados se solicitó diplomado en ciberseguridad, curso de auditoria en ISO 27001 programado para 2022	**Sin información del área**
7.2.3 Proceso disciplinario	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información	5. Se realiza formalmente y está documentado	Hoy depende de la secretaria general en la nueva estructura se crea como unidad independiente	N/A	**Sin información del área**
7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo. **Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.				**Sin información del área**
7.3.1 Terminación o cambio de las responsabilidades laborales	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir	5. Se realiza formalmente y está documentado	A través del aplicativo GACEL, los aplicativos integrados con las áreas correspondientes y con las áreas correspondientes. Procedimiento de traslado. Procedimiento de ingreso, desvinculación y actualización de cuentas del personal		**Sin información del área**

8.6. Gestión adelantada por la Oficina Asesora Jurídica sobre las observaciones reportadas en el informe de la Auditoría Externa.

- 18. Cumplimiento.

18 CUMPLIMIENTO					
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
18.1 CUMPLIMIENTO CON LOS REQUERIMIENTOS CONTRACTUALES Y LEGALES	Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad				
18.1.1 Identificación de los requerimientos contractuales y legales aplicables	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización	5. Se realiza formalmente y está documentado	Normograma publicado en el SGC, en actualización permanente por iniciativa de la Oficina Jurídica. expedición del decreto 1294	este normograma se debe integrar con los requisitos de las partes interesadas y darle seguimiento, medición y mejora continua	Se creo un espacio en la página web de la Entidad para publicar el Normograma y el mismo se esta actualizando trimestralmente y publicado en la web de la Entidad. Se anexa evidencias.
18.1.2 Derechos de Propiedad Intelectual	Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	3. Se realiza parcial e informalmente	Los procesos de contratación son apoyados para el área administrativa. Documentos.: Verificación de los requisitos legislativos y normativos relacionados con los derechos de propiedad intelectual. Acuerdos de transferencia y transmisión de datos personales.	los procesos de establecimiento de requisitos legales y de cumplimiento con personal interno, proveedores y demás partes interesadas se deben administrar de manera integrada con las demás áreas involucradas	Esta Observación no aplica para la Oficina Asesora Jurídica, la Dirección Administrativa de la Entidad es independiente y aplica sus procedimientos, y es quien verifica el uso de productos y la propiedad intelectual, por cuanto tiene sus abogados que la asesoran.
18.1.3 Protección de registros	Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio	2. No se realiza	Se están trabajando en la identificación de activos y riesgos de seguridad asociados no hay evidencia de su implementación. No conforme	N/A	
18.1.4 Privacidad y Protección de la información personal de identificación (PII)	Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y las reglamentaciones pertinentes.	2. No se realiza	En el SOA dice que falta ajustar documentación lo que incumpliría el control 7.5 de información documentada. Política de datos personales. No se evidencia el rol ni la implementación de los procesos de gestión sobre los datos personales. No conforme	N/A	
18.1.5 Regulación de los controles criptográficos	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	2. No se realiza	Política de controles criptográficos no implementada. No conforme	N/A	
18.2 Revisiones de Seguridad de la Información	Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures				
18.2.1 Revisión independientes de la Seguridad de la Información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos	2. No se realiza	No se evidencia su implementación. No conforme	N/A	
18.2.2 Cumplimiento de las políticas y normas de seguridad	Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad	2. No se realiza	No se evidencia su implementación. No conforme	N/A	
18.2.3 Revisión de cumplimiento técnico	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	2. No se realiza	No se evidencia su implementación. No conforme	N/A	

8.7. Gestión adelantada por la Oficina Asesora de Planeación sobre las observaciones reportadas en el informe de Auditoría Externa.

- 4. Contexto de la Organización.

4 Contexto de la organización					
CONTROLES	**DESCRIPCIÓN DEL CONTROL**	**ESTADO DE IMPLEMENTACIÓN 2021**	**OBSERVACION VIGENCIA - 2021**	**RECOMENDACIÓN - VIGENCIA 2021**	**ACCIONES GESTIONADAS POR LAS DEPENDENCIAS - VIGENCIA 2022**
4.1 Conocimiento de la organización y su contexto					
1. ¿La organización determina los fines del SGSI?	Usted debe determinar el propósito del SGSI (por ejemplo: garantizar el cumplimiento de las obligaciones legales, mejorar la capacidad operativa, mejorar la seguridad del producto/servicio, etc..)	5. Se realiza formalmente y está documentado	Auditado: Alfonso Antonio de Jesús Barrios (Contratista Grupo Organización y Calidad) y Carlos Serna (Jefe Oficina Asesora de Planeación). Nace de la Dirección de Informática, no hay claridad frente al origen y propósito del SGSI. Ofrecer tranquilidad dentro de los procesos y evitar ataques cibernéticos. El Plan Estratégico Institucional 2021 – 2022, Plan Aeronáutico 2018 – 2022. Matriz DOFA, anexo PEI versión 2.0 PEI 2021 – 2022, muestran un objetivo institucional relacionado con la seguridad de la información. Desde 2017 con base en el MSPI del MINTIC se hizo un autodiagnóstico frente a la implementación del modelo en la entidad, se contrató una consultoría para realizar el diagnóstico en 2 procesos. El autodiagnóstico se actualiza cada 2 meses. Mediante el PESI y el PETI se identificó un objetivo específico frente a los temas de SI, numeral 8 del plan de acción trimestral, se asignó formalmente los proyectos asociados con los procesos de autoevaluación del modelo MSPI. Plan estratégico de SI Resolución 4215 18 dic 2019 Director de la aeronáutica. Hay Actas en Isolucion enero 21 2021, plan de acción donde se presenta la activación del SGSI, marzo 17 2021 donde se presenta la política.	En la matriz DOFA debe aparecer una estrategia específica frente a SI, dentro de los planes de acción que la entidad tiene implementados debe incluirse la implementación, medición y mejora de un SGSI , basado en ISO 27001, para dar cumplimiento a lo solicitado dentro del MSPI. La sensibilización y concienciación frente a los aspectos estratégicos internos y cómo estos involucran a toda la entidad frente al SGSI, son débiles al preguntar al equipo auditado.	**Sin información del área**
2. ¿La organización determina las cuestiones internas y externas que son pertinentes para la finalidad de SGSI?	Es necesario definir cuáles son las cuestiones internas y externas que influyen en el propósito del negocio y son relevantes para la seguridad de la información (por ejemplo: cultura interna, recursos disponibles, cuota de mercado, perfil del cliente, la disponibilidad de proveedores, etc..)	4. Se realiza informalmente en forma total	A nivel interno se generaron reuniones en las que se definió la necesidad de implementar un SGSI	El seguimiento a los factores externos que afectan el SGSI, tienen un buen marco dado que las regulaciones vienen del gobierno, las cuestiones internas como la alineación de las diferentes áreas, la integración dentro de los procesos existentes y la concienciación evidencian una oportunidad de mejora en el establecimiento y seguimientos de los objetivos y planes de acción para implementar y mejorar un SGSI. La gestión de factores internos y externos debe ser integrada y mostrarse una gestión centralizada para toda la entidad.	**Sin información del área**
3. ¿Determina la organización cómo las cuestiones internas y externas podrían influenciar en la capacidad del SGSI para conseguir los resultados previstos?	Es necesario definir como las cuestiones internas y externas pueden afectar a la capacidad del SGSI para lograr los resultados previstos (por ejemplo: los requisitos legales cambian con frecuencia, los clientes tienen que cumplir con normas específicas, la cultura interna aprecia la información compartida, etc..)	2. No se realiza	Hay un contrato con una Unión Temporal que se encargan de actualizar el autodiagnóstico y tiene en cuenta las actualizaciones frente al modelo y frente a cambios en la regulación. Mintic solicita en las mesas de trabajo evaluar la implementación del Modelo SGSI. El seguimiento interno sobre el plan estratégico de SI no se lleva a cabo mediante indicadores o controles internos. Hay un seguimiento interno trimestral de metas del plan de acción y seguimiento al plan de adquisiciones por la Dirección Administrativa. El seguimiento interno se hace, se pueden evidenciar los informes de revisión trimestral y mensual. Dirección de Informática en mayo presenta en comité mediante acta la presentación de avances en ciberseguridad. Director de Informática en Comité Institucional de Gestión y Desempeño 2021 trimestral según resolución, por resolución 2405 2018, actualizado 2020 de la Aeronáutica, acta de enero 2021 Comité Institucional. El seguimiento interno se hace mediante seguimiento a los contratos con Unión Temporal para la ejecución de los proyectos	A nivel interno reforzar las estrategias de seguimiento sobre el SGSI derivadas de los informes de ciberataques, incluirlos dentro del plan de acción trimestral. El SGSI se establece como un medio para cumplir objetivos institucionales. Por un lado, deben fijarse objetivos para el proyecto de implementación, medirlos y generar, cuando aplique los planes de mejora; por otra parte, el SGSI propiamente debe medir si está cumpliendo el objetivo por el cual se implementó, alineado con el o los objetivos institucionales, los objetivos de seguridad de la información y los objetivos del SGSI y evidenciar su medición y mejora.	**Sin información del área**
4.2 Comprensión de las necesidades y expectativas de las partes interesadas					
1. ¿La organización determina las partes interesadas?	La organización debe definir qué partes interesadas son relevantes para el Sistema de Gestión de Seguridad de la Información (SGSI) (por ejemplo: clientes críticos y proveedores, empleados, agencias gubernamentales, etc..)	5. Se realiza formalmente y está documentado	Guía de atención al ciudadano elabora la matriz de partes interesadas. Caracterización de ciudadanos, usuarios y partes de interés.	Esta matriz de partes interesadas y los requisitos de cada una, debe integrarse con el normograma de la entidad y asegurar que se mantiene un proceso de actualización y revisión de cumplimiento y cambios sobre ella.	**Sin información del área**
2. ¿Existe la lista de todos los requisitos de las partes interesadas?	Tienes que definir el alcance del SGSI, considerando cuestiones internas y externas, los requisitos, las partes interesadas pertinentes e interfaces y las dependencias entre las actividades realizadas por la organización y las realizadas por otras organizaciones.	3. Se realiza parcial e informalmente	Se evidencia un documento en el que a través de encuestas se perfila a las partes interesadas. No se evidencia la lista de requisitos de las partes interesadas para el SGSI.	La lista de partes interesadas debe poder determinar, para cada una, las necesidades y/o requisitos para el SGSI.	**Sin información del área**
4.3 Determinar el alcance del SGSI					
1. ¿El alcance está documentado con los límites claramente definidos?	La organización debe definir qué partes interesadas son relevantes para el sistema de gestión de seguridad de información (SGSI) (por ejemplo: clientes críticos y proveedores, empleados, agencias gubernamentales, etc..)	3. Se realiza parcial e informalmente	Se evidencia en el manual del SGSI v.1.2. que Todas las locaciones del numeral 7.1.3 están en el alcance. El numeral 7.2.1 declara que los 34 procesos de la entidad y todo el personal y terceros están incluidos, se hace referencia a las partes interesadas del numeral 7.1.6, el cual no se encuentra desarrollado en el documento. El alcance se aprueba mediante aprobación del manual del SGSI que contiene la declaración de alcance, el proceso de aprobación y publicación se hace mediante el repositorio Isolucion de la entidad.	Sobre los aspectos del alcance que describe el Manual del SGSI, no hay una evidencia acerca de cómo se concientiza a la entidad sobre los efectos del alcance. La auditoría se desarrolló solamente en el Nivel Central y con solo los líderes de los procesos, el resto de personal no se audita.	**Sin información del área**
4.4 SISTEMAS DE GESTION DE INFORMACION DE SEGURIDAD					
1. ¿Han establecido, documentado, implementado, mantenido y mejorado continuamente un sistema de gestión de seguridad de información según los requisitos de la norma ISO 27001?	Debe establecer, documentar, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de información según los requisitos de la norma ISO 27001.	3. Se realiza parcial e informalmente	El SGSI se estableció formalmente dentro de los planes institucionales, se aprobaron el alcance, la política y los objetivos. El SGSI está en fase de implementación por lo que no se evidencia cumplimiento en cuanto al ciclo de medición y mejora continua. Aún no se ha implementado en todas las áreas de la entidad, alineado con la declaración de alcance.	El SGSI debe socializarse a toda la entidad y sus partes interesadas, se debe poder medir el ciclo de medición y mejora para el cumplimiento de objetivos de la implementación y del SGSI, así como de los objetivos de seguridad de la información y de los objetivos institucionales	**Sin información del área**

9. RESUMEN DEL SEGUIMIENTO A LAS OBSERVACIONES DEL INFORME 2021.

A continuación se relaciona de manera individual la gestión adelantada por las dependencias sobre las observaciones reportadas en el informe de la auditoría externa de la vigencia 2021, las cuales están relacionadas con el incumplimiento de

algunos ítems (Puntos) de la Norma ISO 27001 y que fueron catalogados al interior de la Entidad como ***No Conformes:***

CRITERIO	ESTADO 2021	ESTADO 2022
4.2 COMPRENSIÓN DE LAS EXPECTATIVAS Y NECESIDADES DE LAS PARTES INTERESADAS	NO CONFORME	SIN REPORTE DE AVANCE
4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	NO CONFORME	SIN REPORTE DE AVANCE
4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	NO CONFORME	SIN REPORTE DE AVANCE
5.1 LIDERAZGO Y COMPROMISO	NO CONFORME	SIN REPORTE DE AVANCE
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	NO CONFORME	SIN REPORTE DE AVANCE
6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	NO CONFORME	SIN REPORTE DE AVANCE
6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS	NO CONFORME	SIN REPORTE DE AVANCE
7.2 COMPETENCIA	NO CONFORME	SIN REPORTE DE AVANCE
9. EVALUACIÓN DEL DESEMPEÑO 9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	NO CONFORME	SIN REPORTE DE AVANCE

Con respecto a la información solicitada por el equipo auditor a las diferentes áreas auditadas y la entregada por los auditados, se logró obtener el siguiente resultado sobre los puntos evaluados, el cual se trascribe a continuación:

CRITERIO	REPORTE DE ACCIONES POR LAS ÁREAS
4 CONTEXTO DE LA ORGANIZACIÓN	SIN INFORMACIÓN
5 LIDERAZGO	SIN INFORMACIÓN
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	AREA REPORTO ESTADO
6. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	AREA REPORTO ESTADO
7 SEGURIDAD DEL RECURSO HUMANO	SIN INFORMACIÓN
8 GESTIÓN DE ACTIVOS	AREA REPORTO ESTADO
9 CONTROL DE ACCESO	AREA REPORTO ESTADO
10 CRIPTOGRAFIA	AREA REPORTO ESTADO
11 SEGURIDAD FÍSICA Y AMBIENTAL	AREA REPORTO ESTADO
12 SEGURIDAD DE LAS OPERACIONES	AREA REPORTO ESTADO
13 SEGURIDAD DE LAS COMUNICACIONES	AREA REPORTO ESTADO
14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	AREA REPORTO ESTADO
15 RELACIÓN CON PROVEEDORES	SIN INFORMACIÓN
16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	AREA REPORTO ESTADO
17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	AREA REPORTO ESTADO
18 CUMPLIMIENTO	AREA REPORTO ESTADO

Es decir, de los criterios sobre los cuales se consultó el estado de los mismos al interior de la Aerocivil, se recibió información del setenta y cinco por ciento **(75%)** de los auditados y el veinticinco por ciento **(25%)** no reporto ninguna actividad de seguimiento.

10. HALLAZGOS

Hallazgo número 1 – Servidores Públicos sin los requisitos exigidos, el perfil y la capacitación adecuada para la realización de la auditoría al proceso de Seguridad de la Información.

Como consecuencia del desconocimiento y la falta de capacitación en la Norma ISO/CEI 27701 Gestión de Seguridad de la Información, la Entidad en la actualidad, no dispone de Servidores Públicos capacitados para programar, estructurar y realizar la auditoría al proceso Seguridad de la Información. Es importante resaltar, que tanto la Oficina de Control Interno como la Secretaría de Tecnología de la Información – TI, solicitaron la capacitación respectiva, la cual fue programada e incluida en el Plan Institucional de Contratación – PIC, para ejecutarse en el periodo del 1 de julio al 30 de noviembre de 2022, actividad que no se cumplió, desconociendo las razones que lo originaron.

Actividad de Control Recomendada.

Reprogramar para los Servidores Públicos de la Entidad, la actividad de capacitación en la Norma ISO/CEI 27701 Gestión de Seguridad de la Información, con la intensión de adelantar durante la vigencia 2023, la auditoría al Proceso de Seguridad de la Información. Igualmente, teniendo en cuenta lo complejo y el alto volumen de actividades a evaluar, se debe estudiar la ampliar el número de cupos de la de capacitación.

Responsable.

Dirección de Gestión Humana.

Hallazgo número 2 – Sin seguimiento a las observaciones consignadas en el informe de la auditoría externa de la vigencia 2021.

Como se puede evidenciar durante el desarrollo del presente informe, algunas de las dependencias auditadas no efectuaron de manera oportuna, el debido seguimiento a las observaciones consignadas en el informe final reportadas por la auditoría externa en su momento.

Actividad de Control Recomendada.

Coordinar con la Secretaría de Tecnología de la Información – TI, el alcance y las acciones de mejora que permitan subsanar las observaciones consignadas en el informe de auditoría seguridad de la información.

Responsable.

Secretaria General,
Oficina Asesora de Planeación.

11. CONCLUSIONES.

- A pesar que la Secretaria de Tecnología de la Información – TI, ha venido capacitando y socializando con la mayoría de las dependencias la implementación del proceso de seguridad de la información en la Entidad, se evidencia un desconocimiento generalizado de un gran número de los servidores públicos encargados de gestionar esta actividad, situación por la que nuevamente, se requiere recapacitar a las dependencias sobre la responsabilidad y el rol que cada una de ellas tienen asignados en el proceso, los cuales deben gestionar oportunamente con la intención de lograr los objetivos planteados en las normas que lo regulan.

- Es importante generar desde la Alta Dirección, mediante la capacitación y la divulgación (Publicidad), conciencia en los servidores públicos sobre la necesidad y la obligación de conocer y participar en el proceso de Seguridad de la Información. Además, crear conocimiento que esta no es una actividad única de la Secretaría de Tecnología de la Información – TI, sino de todas las dependencias y de los servidores públicos que utilizan y manipulan los sistemas de información instalados en la Entidad.

- Convertir en una obligación institucional, la creación y actualización permanente de la política de seguridad de la información, la realización de las auditorías y el establecimiento de adecuados mecanismos de control, seguimiento y conservación de todos los equipos que dispone la Entidad en las áreas; misional, de apoyo, estratégico y de evaluación, con la intención de evitar la vulneración de la información y de los sistemas de información.

- Se resalta el alto compromiso de la Secretaría de TI, en especial por parte del Grupo de Seguridad de la Información, en el avance de la implementación de la norma ISO 27001 en la Aerocivil, pero mientras no se entienda que esta implementación depende de todos y cada uno de los funcionarios de la Entidad y especialmente de su Alta Gerencia, la implementación del proceso va a tomar mucho tiempo y pueden no obtenerse los resultados esperados.

Atentamente,

ALFREDO AVELLANEDA HIDALGO
Jefe Oficina de Control Interno (E)

Elaboró: **Víctor Manuel Valdivieso Ruiz/ Carlos Enrique Bacca Acosta /Oficina de Control Interno**
Reviso: **Sonia Maritza Machado Cruz/ Jefe Oficina de Control Interno.**