AUDITORÍA
GENERAL DE LA REPÚBLICA - COLOMBIA

POLÍTICAS DE SEGURIDAD DIGITAL, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE PLANEACIÓN

Bogotá, D.C. noviembre 2023

CONTENIDO

Ilustraciones

Tablas

INTRODUCCIÓN

La **Auditoría General de la República – AGR** entiende, reconoce, acepta y declara que sus datos e información como un activo el cual tiene valor y la cual es indispensable para la consecución de los objetivos definidos por la estrategia de gobernabilidad de la Entidad, y por lo tanto, es necesario establecer un marco legal, normativo y de mejores prácticas en el cual se asegure que la información que: genera, procesa, administra, modifica y custodia es debidamente protegida y tratada de manera adecuada sin importar la forma en la que se procesa, se transporta y/o se almacena ya sea en medio físico, digital y/o electrónico.

El presente documento describe tanto las políticas como los respectivos controles de la Seguridad Digital, Seguridad y Privacidad de la Información definidos por la **Auditoría General de la República – AGR**, los cuales se desarrollaron basados tanto en la Norma ISO/IEC 27001[1] como en las recomendaciones definidas en el estándar ISO/IEC 27002[2]. Así mismo, estas políticas y controles son parte fundamental del Modelo de Seguridad y Privacidad de la Información – MSPI de la Entidad y por lo cual, se convierten en la base para llevar a cabo la implementación de los procedimientos, guías e instructivos que contribuyen no solamente a la implementación sino también a la mejora continua de la seguridad, privacidad y protección tanto de los datos como de la información que: genera, procesa, administra, modifica y custodia de y para la Entidad y se encuentra en cualquier medio físico o electrónico que alberga el dato y/o la información.

Con base en lo anterior, la Entidad entiende que la Seguridad de la Información es una prioridad y por lo tanto es responsabilidad de todos sus funcionarios, contratistas, proveedores y demás que tengan relación comercial/laboral con la Entidad de velar por el cumplimiento de cada una de las políticas y controles establecidos en el presente documento.

[1] Las normas establecidas en este manual son las necesarias de acuerdo con la Norma ISO27002 última versión generada por ISO y que se encuentran descritas en el numeral 10.2 de este documento. El manual será actualizado de acuerdo con las últimas versiones que genera ISO sobre Seguridad de la Información.

[2] Ídem anterior.

1. OBJETIVO DE LA POLÍTICA DE SEGURIDAD DIGITAL, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Definir, establecer y socializar las respectivas medidas estratégicas, misionales, técnicas y legales que son necesarias para proteger la Confidencialidad, Integridad y Disponibilidad de los datos e información y los activos de información que almacenan esta frente a posibles riesgos de seguridad digital, seguridad y privacidad de la información a los que se encuentran expuestos, a través de la aprobación y disposición de los recursos humanos, técnicos que se consideren necesarios que garanticen el progreso del Modelo de Seguridad y Privacidad de la Información de la Información en la Entidad.

2. ALCANCE DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

Inicia por el conocimiento de los objetivos estratégicos de la entidad, la comprensión del contexto externo e interno de la entidad, los riesgos y oportunidades que deben abordarse como parte del MSPI, al igual que los requisitos pertinentes de las partes interesadas, con los cuales se definen los objetivos de la seguridad de la información, la política general y las políticas secundarias sobre el **Proceso de Gestión del Proceso auditor** de la Entidad. El Comité Institucional de Gestión y Desempeño, desarrolla la respectiva gestión y aplicación de las políticas y controles definidos en el presente documento y que se aplican los procesos de la Entidad y termina con la respectiva gestión, seguimiento y mejora continua de éstos al interior de la Entidad, sin dejar de lado la respectiva actualización de manera periódica de la identificación/actualización de los activos de información identificados, definidos, administrados y custodiados y que son la base para el desarrollo de la misión institucional y el cumplimiento de los objetivos estratégicos de ésta.

3. NORMATIVIDAD

- **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 454 del 21 de marzo de 2020.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, con la incorporación de la política de gestión de la información estadística a las políticas de gestión y desempeño institucional.
- **Decreto 1287 del 24 de septiembre de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **Decreto 338 de 2022:** "Por medio del cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital".
- **Directiva Presidencial 03 de 15 de marzo de 2021:** Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.

- **Documento CONPES 3701 de 2011** - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.
- **Documento CONPES 3854 de 2016** - Política Nacional de Seguridad Digital.
- **Documento CONPES 3995 de 2020** - Política Nacional De Confianza y Seguridad Digital.
- **Ley Estatutaria 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **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 1955 de 2019.** por la cual se expide el Plan Nacional de Desarrollo 2018-2022, establece en su artículo 147 como uno de los principios de los proyectos estratégicos de transformación digital en la permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las que la Política de Gobierno Digital como política de gestión y desempeño institucional, debe contemplar como acción prioritaria el aprovechamiento de tecnologías emergentes en el sector público, incremento de la confianza y seguridad digital y el fomento a la participación y la democracia por medios digitales.
- **NTC/ISO 27001:2022**. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- **Resolución 500 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"

4. ALCANCE DE LA POLÍTICA DE SEGURIDAD DIGITAL, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Inicia con la gestión y administración de la política general, políticas secundarias, procedimientos, guías e instructivos, pasando por el respectivo seguimiento y monitoreo de su aplicabilidad en la Entidad y terminando con el desarrollo y/o ajuste de políticas, procedimientos, guías e instructivos, garantizando el cumplimiento y la mejora continua de lo descrito en el presente documento, sin dejar de la definición de la estrategia de capacitación y sensibilización sobre el Modelo de Seguridad y Privacidad de la Información para toda la Entidad sobre el Proceso de Gestión del Proceso Auditor de la Entidad.

5. OBJETIVOS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

- Establecer y mantener el compromiso del Comité Institucional de Gestión y Desempeño para apalancar el cumplimiento de la **Política de Seguridad Digital, Seguridad y Privacidad de la Información** al interior de la Entidad.
- Definir, establecer y socializar desde el Comité Institucional de Gestión y Desempeño los controles para la gestión, administración, seguimiento y mejora continua de la seguridad digital, seguridad y privacidad de los datos e información, de manera clara y estructurada, basados en las buenas prácticas, la Norma ISO/IEC 27001 y demás normas, estándares y disposiciones legales y normativos relacionadas[3] con el Modelo de Seguridad y Privacidad de la Información.
- Contribuir al cumplimiento legal vigente sobre la seguridad y protección de los datos e información: públicos, públicos clasificados, públicos reservados, de propiedad intelectual, transparencia, protección de los datos personales, protección y salvaguarda de los activos de información sean estos físicos y digitales, entre otras, para brindar tranquilidad a los funcionarios, contratistas, proveedores y demás que tengan relación laboral con la Entidad y se encuentra bajo la custodia esta.
- Generar la alineación con el Sistema de Gestión de Calidad de la Entidad, garantizando el cumplimiento de los planes y acciones (preventivas o correctivas) generadas en el seguimiento interno, la revisión por la dirección y/o las auditorías internas o externas.
- Gestionar los riesgos de Seguridad y Privacidad de la Información que se identifiquen en la Entidad.
- Generar la respectiva sensibilización apropiada para la adecuada gestión de Seguridad Digital, Seguridad y Privacidad de la Información en los Entidad funcionarios, contratistas y proveedores y demás partes interesadas de y en la Entidad.

6. FACTORES DE ÉXITO – MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

- Generar conciencia en todos los funcionarios, contratistas, proveedores y demás partes interesadas o que tengan relación laboral con la Entidad sobre la importancia de conocer, aplicar y seguir las políticas y controles establecidos en el presente documento, los cuales ayuden a garantizar que la Información que la Entidad genera, procesa, administra, modifica y custodia conserve los atributos de Confidencialidad, Integridad y Disponibilidad sobre los datos e información.
- Contar con instancias de gestión, revisión, monitoreo y decisión a distintos niveles de la Entidad (táctico, operativo, estratégico y de seguimiento) en los cuales se realice la presentación de los resultados de los procesos y actividades asociadas al Modelo de Seguridad y Privacidad de la Información – MSPI.
- Implementar un esquema de gestión de eventos/incidentes de seguridad de la información que recoja notificaciones continúas realizadas por parte de los funcionarios, contratistas y proveedores, y en donde se analice cada uno de los eventos, se generen mejoras en los controles definidos y reporte a las instancias de revisión y decisión los resultados de la gestión llevada a cabo.

[3] Norma ISO/IEC 27001:2013 Sistemas de Gestión de Seguridad de la Información; ISO/IEC 27002:2013 Códigos de práctica para los controles de Seguridad de la Información; ISO/IEC 27005:2009 Gestión del Riesgo en la Seguridad de la Información.

- Incluir en todos los procesos de la Entidad, así como en los proyectos prioritarios y no prioritarios los criterios de gestión del Modelo de Seguridad y Privacidad de la Información.

7. DEFINICIONES

- **Activo de Información:** Es todo aquello que en la Entidad es considerado importante o de alta validez para la misma, ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **AGR:** Auditoría General de la República – AGR
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Carpetas Compartidas:** es básicamente igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.
- **CAU:** es el único Centro de Atención al Usuario en donde el grupo TIC presta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servicios TIC en la AGR
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, Entidades o procesos no autorizados.
- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** Acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, Entidades o procesos autorizados cuando lo requieran.
- **Drive:** Sitio para almacenamiento virtual en la nube de la información pública de las áreas de la institución.
- **File Server:** Es un servidor de archivos que almacena y distribuye diferentes tipos de archivos informáticos confidenciales o críticos de la AGR
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Información confidencial o crítica:** Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en la AGR
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **MSPI:** Es el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información – MINTIC.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

8. POLÍTICA DE SEGURIDAD DIGITAL, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de la **AUDITORÍA GENERAL DE LA REPÚBLICA – AGR**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un **Modelo de Seguridad y Privacidad de la Información – MSPI** buscando establecer un marco de confianza en el ejercicio de sus deberes para con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para la Entidad la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, la confidencialidad y la disponibilidad de los datos e información, acorde con las necesidades de los diferentes grupos de interés identificados en la mencionada Entidad.

Con base en lo anterior, esta política aplica a la Entidad según como se define en el alcance, sus servidores públicos, contratistas, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Modelo de Seguridad y Privacidad de la Información – MSPI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones críticas e importantes de la Entidad.
- Cumplir con los principios de seguridad digital, seguridad y privacidad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los grupos de interés.
- Apoyar la innovación tecnológica.
- Proteger los activos de información de la Entidad.
- Establecer las políticas, procedimientos, guías e instructivos en materia de seguridad digital, seguridad y de la información.
- Fortalecer la cultura de seguridad digital, seguridad y privacidad de la información en los funcionarios, contratistas y proveedores.
- Garantizar la continuidad del negocio frente a eventos/incidentes de seguridad digital, seguridad y privacidad de la información.

La Entidad ha decidido definir, implementar, gestionar y mejorar de manera continua el Modelo de Seguridad y Privacidad de la Información – MSPI soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos mandatarios, legales y regulatorios.

9. CONSIDERACIONES GENERALES.

9.1. Consideraciones Generales

9.1.1. Responsabilidad

Es responsabilidad de las Direcciones, Oficinas y Jefes de Oficina de la **Auditoría General de la República – AGR** aplicar las políticas, controles, procesos, procedimientos, guías e instructivos de seguridad digital, seguridad y privacidad de la información como parte de sus herramientas de gobierno y gestión las cuales garanticen la respectiva gestión, monitoreo, cumplimiento mejora continua del Modelo de Seguridad y Privacidad de la Información – MSPI.

9.1.2. Cumplimiento

El cumplimiento de las políticas, controles, procesos, procedimientos, guías e instructivos de Seguridad de la Información, aplica y aplicará para todos los funcionarios, contratistas y proveedores que interactúen con los activos de información de propiedad de la Entidad, si los parámetros aquí descritos se infringen, la **Auditoría General de la República – AGR** se reservará el derecho de tomar las medidas correspondientes de acuerdo con lo establecido en el documento **GJ.110.P13.P Procedimiento para investigar la conducta de los sujetos disponibles dentro de la AGR** para servidores públicos y para contratistas se aplica lo establecido en la **Ley 1952 de 2019 "Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario."** y se traslada a la Procuraduría General de la Nación..

9.1.3. Excepciones

Las excepciones a cualquier incumplimiento de lo descrito en el presente documento deberán ser preaprobadas por la Oficina de Planeación - Grupo de Tecnologías y Sistemas de Información y aprobadas por el Comité Institucional de Gestión y Desempeño. Todas las excepciones a lo descrito en el presente documento deben ser formalmente documentadas, registradas y revisadas por el comité en mención.

9.1.4. Administración de políticas y controles

Toda política y/o control(es) de seguridad de la información nuevo, modificado y/o eliminado, serán propuestos por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y serán aprobadas por el Comité Institucional de Gestión y Desempeño de la **Auditoría General de la República – AGR.** Dichas políticas y/o controles serán revisados con la periodicidad que defina el mencionado Comité y/o cada vez que sea requerido.

9.2. Exclusiones.

- No se excluye ningún numeral de la norma ISO/IEC 27001 versión actual[4].

[4] Ídem pie de nota Número. 1

- En caso de existir exclusiones, éstas se encontrarán definidas y sustentadas en la respectiva Declaración de Aplicabilidad del Modelo de Seguridad y Privacidad de la Información – MSPI de la Entidad

9.3. Referencias informativas.

- **Ver documento:** Normograma de los Procesos del Sistema de Gestión de la Calidad de la Auditoría General de la República – **TI_Normograma.pdf** de la Entidad.

9.4. Vigencia y actualización de la Política

La actualización y mantenimiento del presente documento son responsabilidad de la Oficina de Planeación - Grupo de Tecnologías y Sistemas de Información conforme a lo aprobado en la **Política de Seguridad Digital, Seguridad y Privacidad de la Información** y sea socializada en el Comité Institucional de Gestión y Desempeño, el cual se realizará al menos una (1) vez al año.

En las revisiones periódicas se deben tener en cuenta factores como:

- Requerimientos normativos y legales.
- Requerimientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Requerimientos emitidos por la Coordinación Nacional de Seguridad Digital[5].
- Mapa de riesgos de la Entidad.
- Eventos/Incidentes de seguridad de la Información.
- Vulnerabilidades detectadas, sean actuales o no.
- Cambios en la infraestructura organizacional y/o tecnológica de la Entidad.
- Cambios en la estrategia de gobierno, objetivos y/o procesos de la Entidad.

La versión oficial del presente documento será la que se encuentre revisada y aprobada por el Comité Institucional de Gestión y Desempeño, publicada y divulgada en el Sistema Integrado de Gestión de la Entidad.

10. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ENTIDAD[6].

10.1. Roles y responsabilidades para la seguridad de la información.

La Entidad cuenta con un grupo interdisciplinario denominado Comité Institucional de Gestión y Desempeño , el cual vela por el gobierno y cumplimiento del Modelo de Seguridad y Privacidad de la Información en la Entidad. Mencionado comité se apoya en la Oficina de Planeación - Grupo de Tecnologías y Sistemas de Información, en donde se encuentra la responsabilidad de: *Definir, establecer y asegurar los respectivos soportes técnicos y administrativos para desarrollar, sustentar y gestionar iniciativas sobre Seguridad y Privacidad de la Información, protección de datos personales y ciberseguridad, a través de*

[5] Documento Modelo Integrado de Planeación y Gestión – MIPG, Pág. 46 Numeral "3.2.1.4 Política de Seguridad Digital".

[6] Hace referencia al numeral 5.3 de la Norma ISO/IEC 27001:2013: "5.3. Roles, Responsabilidades y Autoridades en la Organización."

compromisos apropiados y uso de recursos adecuados en la Entidad, sin dejar de lado el respectivo monitoreo y seguimiento para la mejora continua del mencionado Modelo.

Con este apoyo, se busca gestionar, fortalecer, revisar y mejorar de manera continua el proceder del Modelo de Seguridad y Privacidad de la Información – MSPI en la Entidad.

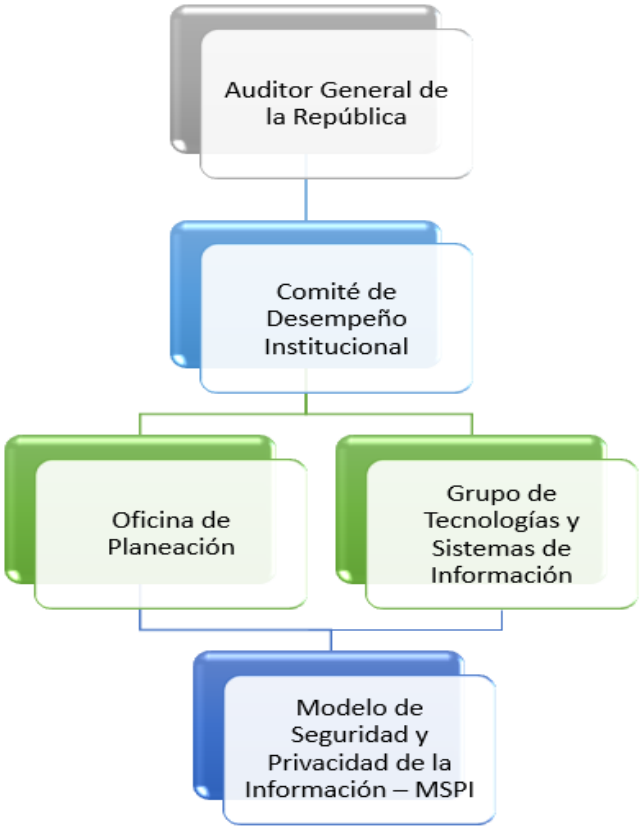
Las partes interesadas internas de la **Entidad**, los servidores públicos, contratistas, proveedores, usuarios y beneficiarios de los servicios de la Entidad deben tener conocimiento de sus responsabilidades y sus obligaciones relacionadas con la seguridad digital, seguridad y privacidad de los datos e información y esta responsabilidad se debe ver reflejada en los instrumentos jurídicos y legales que regulen las relaciones de estas partes para con la Entidad y debe ser verificada por el Comité Institucional de Gestión y Desempeño de manera continua.

Esta matriz puede ser consultada en el documento **Matriz RACI – Modelo de Seguridad y Privacidad de la Información – MSPI.**

10.2. Estructura Organizacional – Seguridad de la Información.

La estructura organizacional para el funcionamiento del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad es el siguiente:

Ilustración 1: Estructura Organizacional Modelo de Seguridad y Privacidad de la Información – MSPI –Auditoría General de la República – AGR



Fuente: Elaboración propia

La conformación del **Comité Institucional de Gestión y Desempeño** se encuentra detallada en la Resolución 10 de 2018 en la Entidad.

10.3. Segregación de Funciones.

Los funcionarios, contratistas y proveedores que en ejercicio de sus labores tengan acceso a la información, infraestructura tecnológica y a los sistemas de información, deben contar con el nivel de acceso y privilegios mínimos requeridos sobre los datos e información y los activos de información para la ejecución de sus labores, con el fin de mitigar y evitar el uso y/o modificación no autorizada sobre los activos de información de la **Auditoría General de la República – AGR**

La segregación de funciones cobija a:

- Los servicios, sistemas de información y sus respectivas bases de datos clasificados como críticos, deben incluir reglas de acceso lógico que aseguren una adecuada segregación de funciones entre quien autorice, administre, opere y mantenga, y audite y, en general, tenga la posibilidad de acceder a los sistemas de información y bases de datos respectivamente. Aplica para servicios on premise como para servicios en nube.
- Los cambios o pasos de los ambientes de pruebas a ambientes productivos solo se podrán realizar una vez sean aprobados por el área usuaria o solicitante del requerimiento a través de una gestión de cambios.
- Las funciones de soporte técnico, desarrollo y operación deben estar claramente segregadas, así como distribuidos los ambientes de desarrollo, de pruebas y de producción, según corresponda y se encuentren definidos en la Entidad.
- La administración y gestión de las redes y comunicaciones y de la infraestructura tecnológica en la Entidad deben incluir reglas de acceso lógico que aseguren una adecuada segregación de funciones entre quien autorice, administre, opere y mantenga, y audite y, en general, tenga la posibilidad de acceder a los sistemas de información y bases de datos respectivamente.

10.4. Contacto con las autoridades y grupos de interés especial.

La **Auditoría General de la República – AGR** deberá establecer y mantener una relación cercana con Entidades de Prevención y Atención de Emergencias tanto territoriales como nacionales, así como con grupos de interés o foros de especialistas en seguridad digital, seguridad y privacidad de la información, para que puedan ser contactados de manera oportuna en caso de que se presente un evento/incidente de seguridad digital, seguridad y privacidad de la información.

Los grupos de interés son los siguientes:

- **ColCert:** Grupo de Respuesta a Emergencia Cibernéticas de Colombia. www.colcert.gov.co – CCOC: Comando Conjunto Cibernético.
- **CSIRT:** Centro de Coordinación Seguridad Informática Colombia. www.csirt-ccit.org.co

- **Centro Cibernético Policial (CAI Virtual):** Ciberseguridad en Colombia comandado por la Policía Nacional. www.policia.gov.co
- **MINTIC:** Ministerio de las Tecnologías y las Comunicaciones www.mintic.gov.co
- **Comando Conjunto Cibernético – CCOC:** Grupo que dirige las mesas de trabajo para garantizar la seguridad de las infraestructuras críticas del país ante cualquier eventualidad al correo atencionalciudadano@cgfm.mil.co

En la eventualidad que se llegasen a presentar eventos/incidentes relacionados con la seguridad de la información al interior de la Entidad, deben ser reportados de la siguiente manera:

- Seguridad Digital, Seguridad y Privacidad de la Información: seguridaddelainformacion@auditoria.gov.co
- El oficial o encargado de la seguridad de la información debe reportar acorde a lo que se encuentra a continuación:

Tabla 1: Cuadro de reportes de eventos/incidentes de Seguridad Digital, Seguridad y Privacidad de la Información – MSPI

Descripción	Entidad	Contacto
Acceso abusivo a sistemas informáticos	Centro Cibernético Policial (CCP)	http://www.ccp.gov.co/
Violación de Datos personales		
Uso de Software malicioso		
Suplantación de Sitios Web		
Transferencia no consentida de activos		
Hurto por medios informáticos		
Phishing / Ingeniería Social		
Respuesta a Emergencias Cibernéticas de Colombia	COLCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	www.colcert.gov.co/
Atención a incidentes de seguridad informática colombiano	CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co
Emergencia por Incendio	Bomberos	119
Robo	Policía Nacional	112
Antisecuestro y Antiextorsión	Gaula	165
Siniestros ambientales	Defensa Civil	144
Incidentes Laborales	Cruz Roja	132
	Centro Toxicológico	136
Robo	DIJIN	157

Fuente: Elaboración propia

10.5. Seguridad de la Información en la Gestión de Proyectos

Los proyectos que se denominen al interior de la **Auditoría General de la República – AGR** sean estratégicos y/o sean prioritarios, impacten los procesos de la Entidad y/o la actualización o implementación de un nuevo sistema de información, deben incluir la Gestión de Riesgos de Seguridad de la Información. Se debe tener presente el balance entre seguridad, funcionalidad, los demás objetivos establecidos y el cumplimiento de los tres principios: Confidencialidad, Integridad y Disponibilidad de los datos e información de la Entidad.

10.6. Monitoreo al Modelo de Seguridad y Privacidad de la Información – MSPI

El monitoreo al Modelo de Seguridad y Privacidad de la Información – MSPI de y en la Entidad se realizará de manera interna y bajo la responsabilidad de la Dirección de Control Interno dentro del cronograma de auditorías anuales. Se revisará la aplicabilidad de las políticas y controles definidos en el presente documento, en donde se validará su implementación, resultados, y se realizarán los cambios, modificaciones, actualizaciones y/o eliminaciones de políticas y/o controles allí definidos. Así mismo, será el responsable de mantener actualizado el Sistema de Seguridad de la Información de Seguridad de la Información en su totalidad.

10.7. Competencia y concientización

- Validar la competencia necesaria de las personas que realizan actividades críticas para la seguridad de la información de la Entidad. Esta competencia puede estar basada en la educación, formación o experiencia.
- Realizar acciones que permitan fortalecer la competencia asociada a estas actividades críticas para la seguridad de la información de la Entidad.
- El rol de oficial de seguridad de contar con la competencia técnica sobre las plataformas y sistemas que soportan las aplicaciones y servicios TI, y de la norma ISO:27001
- Las personas que trabajan bajo el control de la organización deben ser conscientes de: la política de la seguridad de la información, su contribución a la eficacia del MSPI y las implicaciones de no cumplir con los requisitos del MSPI. Esta concientización debe realizarse anualmente y como parte del proceso de inducción de nuevos funcionarios y al inicio de nuevos contratos.

11. POLÍTICAS TÉCNICAS DE SEGURIDAD DE LA INFORMACIÓN:

11.1. Política de Seguridad de la Información.

La **Política de Seguridad Digital, Seguridad y Privacidad de la Información** aprobada por el Comité Institucional de Gestión y Desempeño de la Entidad que se detalla en el **numeral 8 Política de Seguridad Digital, Seguridad y Privacidad de la Información** se encuentra publicada como componente en el Sistema Integrado de Gestión de la **Auditoría General de la República – AGR** en la página web de la Entidad: https://www.auditoria.gov.co/

11.1.1. Responsabilidades de la Dirección.

El Comité Institucional de Gestión y Desempeño aprueba el **presente documento** como muestra de su compromiso y apoyo en el diseño e implementación de acciones eficientes que garanticen la seguridad de la información de la Entidad.

Adicionalmente, el Comité Institucional de Gestión y Desempeño de la **Auditoría General de la República – AGR** demostrará su compromiso a través de:

- La revisión de la **Política de Seguridad Digital, Seguridad y Privacidad de la**

Información y puesta a disposición para su revisión y su respectiva aprobación, publicación y divulgación ante la Entidad.

- La revisión, aprobación y verificación del cumplimiento de las Políticas Técnicas y controles asociados contenidos en este documento.
- La promoción activa de una cultura de Seguridad y Privacidad de la Información.
- La divulgación y verificación del presente documento a todos los servidores públicos, contratistas y proveedores de la Entidad.
- La solicitud para asegurar la asignación de los recursos adecuados para implementar y mantener las políticas y controles mencionadas en el presente documento.
- La promoción de los canales adecuados para que los servidores públicos, contratistas y proveedores reporten sucesos, eventos y/o incidentes que afecten, vulneren o representen un incumplimiento de las políticas y/o controles de seguridad de la información.

11.2. Seguridad de la información en la gestión de proyectos.

Los proyectos que se denominen estratégicos y/o sean prioritarios, y/o impacten los procesos de la Entidad y/o la actualización, y/o desarrollo y/o implementación de un nuevo sistema de información, deben asegurar que los riesgos de Seguridad de la Información asociados a éstos serán gestionados, usando una combinación de controles automáticos y manuales. Se deben especificar de manera clara los requerimientos de Seguridad Digital, Seguridad y Privacidad de la Información en los proyectos, garantizando el balance entre seguridad, funcionalidad y los demás objetivos establecidos.

11.3. Políticas internas de Seguridad de la Información.

Por el presente Manual de Seguridad de la Información se adoptan políticas internas alineadas a lo descrito en la Norma ISO/IEC 27002[7], así:

1. Política para dispositivos móviles.
2. Política para teletrabajo.
3. Política para control de acceso.
4. Política para controles criptográficos.
5. Política para la gestión de llaves.
6. Política para seguridad física y del entorno
7. Política de escritorio y pantalla limpia.
8. Política para transferencia de información.
9. Política para desarrollo seguro.
10. Política para relaciones con los proveedores.
11. Política para privacidad y protección de información de datos personales.

Estas políticas se comunican a los servidores públicos, contratistas y proveedores y a las demás partes interesadas a través de los canales y mecanismos institucionales dispuestos

[7] Ídem pie de nota No. 1

para estos fines. Además, deberán ser incluidas en las iniciativas de generación de cultura en seguridad de la información de la **Auditoría General de la República – AGR**

11.3.1. Política para dispositivos móviles

El uso de medios de dispositivos móviles (ejemplo: teléfonos inteligentes o smartphones sean institucionales o personales, tabletas, portátiles sean institucionales o personales, discos duros externos, memorias), sobre la infraestructura para la generación, administración, procesamiento, modificación y custodia de los datos e información de la **Auditoría General de la República – AGR** se encontrarán autorizados para todos los servidores públicos, contratistas y proveedores por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información de la Entidad y serán responsabilidad directa de cada autorizado su buen uso y la fuga de datos y/o información que se llegase a presentar.

Oficina de Planeación Grupo de Tecnologías y Sistemas de Información tiene la responsabilidad de diseñar, validar, verificar y monitorear aplicando de manera correcta el ciclo completo de: P-H-V-A a los respectivos controles que se encuentran definidos y aplican en la Entidad para el uso correcto de los dispositivos móviles autorizados y así mismo, será la responsable de implementar estos controles para asegurar que el ingreso a los sistemas de información y el uso de los medios de almacenamiento removibles definidos en la Entidad sea realizado únicamente por los servidores públicos, contratistas y proveedores autorizados o que cuenten con una vinculación laboral vigente con la Entidad.

Así mismo, los servidores públicos, contratistas y proveedores que hagan uso de alguno de los dispositivos enunciados en este numeral, se comprometen a proteger y asegurar física y lógicamente el dispositivo físico autorizado con el de objeto de no poner en riesgo los datos e información de la Entidad que éste contenga.

11.3.2. Política para teletrabajo

Las actividades de teletrabajo que se autoricen en la **Auditoría General de la República – AGR** se podrán llevar a cabo siempre y cuando éstas cumplan con los controles de seguridad que se encuentran definidos y alineados con las políticas de seguridad de la información y los cuales están descritos en el numeral *11.4. Controles definidos y que apoyan tanto a las Políticas Internas como a la Política de Seguridad Digital, Seguridad y Privacidad de la Información de la Auditoría General de la República – AGR* del presente documento y también se encontrarán alineados con lo establecido por la Dirección de Talento Humano acorde con el procedimiento que se lleve a cabo para el reconocimiento de la calidad de teletrabajador, sin dejar de lado el respectivo análisis del riesgo.

11.3.2.1. Condiciones Obligatorias

Con el fin de conservar las características de integridad, disponibilidad y confidencialidad de los datos e información en el desarrollo de las actividades de teletrabajo, se establecerán e implementarán de manera obligatoria, las siguientes condiciones:

- Mecanismos de seguridad física y lógica a los equipos y documentos que maneje el

teletrabajador durante el periodo establecido por la Dirección de Talento Humano.

- Previo análisis de riesgos, se adoptarán mecanismos de control para la protección de los datos e información, aplicaciones y sistemas de información de la Entidad que son accedidos por el teletrabajador durante el periodo definido por la Dirección de Talento Humano.
- Antes de llevar a cabo cualquier actividad de teletrabajo se definirán entre la Entidad y el servidor público, los alcances de las actividades a desarrollar y la información a acceder, así como los sistemas y servicios de la Entidad que se utilizarán.
- Los permisos serán establecidos por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información establecerá los accesos solicitados a partir de lo establecido por la Dirección de Talento Humano y los cuales son autorizados por el jefe directo o quien haga sus veces.
- Para los temas de teletrabajo relacionados con contratistas o proveedores de la Entidad, también se definirán los respectivos alcances de las actividades a desarrollar, los datos e información a consultar, aplicaciones y sistemas de información a acceder y los servicios a utilizar entre los respectivos supervisores de contrato y los contratistas y proveedores y éstos serán establecidos a través de lo solicitado por medio de las directrices emitidas por la Dirección de Talento Humano y el supervisor directo del contrato.

11.3.3. Política para control de acceso

Con la finalidad de preservar la Confidencialidad, Integridad, Disponibilidad y Privacidad de los datos e información que se generan, modifican, custodian y almacenan en los activos de información y son accedidos o se encuentran a cargo de los servidores públicos, contratistas y proveedores debido a su cargo y/o responsabilidades, se han establecido controles que permitan regular el acceso a las redes, datos e información, así como la implementación de perímetros de seguridad física y lógica para la protección de las instalaciones, especialmente aquellas clasificadas como áreas seguras, tales como los centros de procesamiento de información, áreas de almacenamiento de información física y lógica, cuartos de suministro de energía eléctrica, aire acondicionado, entre otras.

La Entidad llevará a cabo la gestión sobre el control de acceso a través de la atención de solicitudes sobre creaciones/cancelaciones/inactivaciones de usuarios que sean informadas por la Dirección de Talento Humano y/o la Oficina Jurídica acorde con la vinculación o desvinculación del personal a la Entidad, lo cual permitirá tener en cuenta al interior de las bases de datos que soportan los sistemas de información los aspectos lógicos como físicos que permitan garantizar la trazabilidad de las acciones realizadas, identificando, entre otros, datos relevantes tales como: quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso, accesos denegados, entre otros. Para tal efecto, se aplicará lo indicado en los documentos: **TH.232.P1 Provisión de cargos de libre nombramiento y remoción carrera administrativa y provisionalidad, TH.232.P21 Retiro, traslado, reubicación o permuta de funcionarios** y **GJ.110P14 Contratación.**

Una vez se apruebe el acceso a la información, los servidores públicos, contratistas y proveedores deben abstenerse de realizar modificaciones sobre la información sin la debida autorización, o acciones que vulneren los controles de seguridad establecidos por la Entidad; así mismo, deben guardar confidencialidad de la información a través de los acuerdos de confidencialidad que firmen sean servidores públicos o contratistas, a la cual tienen acceso e informar a la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información acerca de las debilidades y/o eventos/incidentes de seguridad que se identifiquen.

11.3.3.1. Responsabilidades de la Administración

- La información de naturaleza pública de la **Auditoría General de la República – AGR** estará disponible para los servidores públicos, contratistas, proveedores, ciudadanos, entres de control y/o autoridades, siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.
- Se establecerán controles para que sólo los servidores públicos, contratistas y/o proveedores responsables de su actualización puedan acceder a su modificación, incorporando los nuevos datos que se produzcan.
- El acceso tanto a los datos e información como a las aplicaciones y sistemas de información será restringido conforme a los roles y responsabilidades asignados a cada uno de los servidores públicos, contratistas y proveedores de la **Auditoría General de la República – AGR**
- Como responsables de los datos e información las partes interesadas deberán administrar y hacer cumplir los controles de seguridad digital, seguridad y privacidad de la información establecidos en el presente documento, con el fin de evitar accesos no autorizados, pérdidas y/o utilización indebida de los datos e información almacenados en los activos de información.
- Los servidores públicos, contratistas y proveedores de la **Auditoría General de la República – AGR** son responsables de velar por la Confidencialidad, Integridad y Disponibilidad de los datos e información, los activos de información, los sistemas de información, aplicaciones y bases de datos para los cuales han sido designados y/o autorizados, asegurándose que éstos sólo sean utilizados para el desarrollo de las labores encomendadas.
- Tanto el responsable del área restringida como el Encargado del manejo del activo de información tienen la responsabilidad de realizar al menos una revisión anual (o cuando sea requerido/necesario) sobre los derechos de acceso de los usuarios autorizados en intervalos regulares y definidos por el responsable de la Gestión el Modelo de Seguridad y Privacidad de la Información – MSPI, con el fin de mantener un control eficaz de acceso a los datos e información y a los servicios de información que ofrecen los sistemas de información, aplicaciones y/o bases de datos.
- La responsabilidad de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información se basa en el establecimiento y aplicación de parámetros de seguridad y privacidad de la información para los recursos de red compartidos en la Entidad.
-
- Para las oficinas que cuentan con sistemas de información y su administración, es

responsabilidad de cada una de ellas mantener y garantizar el control de acceso de usuarios sobre estos sistemas y sus respectivas bases de datos.

11.3.3.2. Responsabilidades de los usuarios

- Todos los servidores públicos, contratistas y proveedores cuentan con un usuario y contraseña único, personal e intransferible y asumen la responsabilidad de los eventos y/o incidentes que puedan ocurrir bajo su autenticación sobre los activos de información a los cuales acceden y procesan dentro del desarrollo de sus funciones y responsabilidades.
- Se debe dar uso adecuado a los activos de información y deben ser usados únicamente bajo las condiciones netamente laborales.
- No está permitido divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar la contraseña de acceso asignada para el acceso a la plataforma tecnológica de la Entidad, correo electrónico, dispositivos, bases de datos, equipos de cómputo, servidores públicos, aplicaciones, sistemas de información y similares.
- Todos los servidores públicos, contratistas y proveedores, que requieran tener acceso a los sistemas de información de la **Auditoría General de la República – AGR** deben estar debidamente autorizados por el jefe y/o director y debe acceder a dichos sistemas haciendo uso de un usuario y contraseña y cumplir los siguientes lineamientos:
    - No divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar la(s) contraseña(s) de usuario(s) por los que accede a la plataforma tecnológica en ninguna circunstancia.
    - Cambiar la contraseña en intervalos de tiempo regulares.
    - Construir contraseñas seguras que incluyan como mínimo:
        - 1 carácter especial.
        - 1 carácter en Mayúscula.
        - 1 carácter numérico.
        - Debe contener una longitud mínima de 8 caracteres.
    - No utilizar contraseñas de fácil identificación, como: años de nacimiento, nombres de hijos.
    - La contraseña no puede ser el mismo usuario.
    - No escribir la contraseña en medios físicos, digitales y/o electrónicos.

- Los servidores públicos, contratistas y proveedores no deben realizar cambios en los equipos de escritorio o portátiles en la configuración y los cuales les sean asignados ya que éstos son entregados completos y configurados a nivel de: conexiones de red, usuarios locales, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios son realizados únicamente por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información.

11.3.3.3. Validación periódica control de acceso

- De manera trimestral se realiza la validación de usuarios existentes en las aplicaciones / plataformas soportadas por la Dirección de Planeación – Grupo de Tecnologías.
- El listado de funcionarios reportado por la Dirección de Talento Humano y el listado de contratistas reportado por la Dirección Jurídica serán los soportes formales de validación. Para inicial el proceso de validación de usuarios, estos deberán ser solicitados o descargados de fuentes autorizadas.
- Se realiza la validación de usuarios activos en cada aplicación / plataforma para determinar las desviaciones respecto de los listados de validación.
- Se reportarás las desviaciones al administrador de la plataforma respectiva, para validación y ejecución de las acciones correspondientes (inactivación de accesos, ajuste de información de soporte que permita una correcta validación, entre otras)
- El administrador debe dejar trazabilidad de las acciones tomadas a través del CAU para posterior validación, informando al área o responsable de tomar las acciones que permitan que no presenten desviaciones o inconsistencias en la validación.
- Es deseable que todas las fuentes de información usadas puedan contar con un campo de identificación único para el usuario, y este sea diligenciado en las aplicaciones o plataformas con cada modificación que se realice para el control de acceso. Esto con el fin de aumentar el asertividad en el proceso de validación periódica de usuarios.

11.3.3.4. Derechos de Acceso Privilegiado aplicaciones y servicios TI

- La asignación y el uso de derechos de acceso privilegiado para la administración, soporte y mantenimiento de las plataformas y sistemas que soportan las aplicaciones y servicios TI, serán autorizado por el Coordinador del Grupo de Gestión TIC cumpliendo con todas las demás condiciones para el control de acceso

11.3.4. Política para controles criptográficos y gestión de llaves

Con el fin de proteger la confidencialidad, integridad, autenticidad y no repudio de la información, la **Auditoría General de la República – AGR** establece el uso de protocolos y controles criptográficos para transmitir o transferir información, enlaces de comunicaciones, conexión remota a través de asignación de VPN firmas electrónicas y digitales con Entidades externas. Estos accesos se conceden a través del establecimiento de VPN site-to-site y se establecen convenios interadministrativos para llevar a cabo la respectiva configuración del mencionado canal con Entidades del Orden Nacional o Territorial.

De igual forma, es responsabilidad directa tanto de los servidores públicos o contratistas de la Entidad hacer uso correcto de los certificados digitales, firmas electrónicas, firmas digitales, y los respectivos token’s para firma digital con que cuentan los accesos a los servicios y páginas web en la Entidad y a otras Entidades que requieren este tipo de autenticación.

11.3.5. Política para seguridad física y del Entorno.

Con el objetivo de garantizar la respectiva seguridad física de las instalaciones de la **Auditoría General de la República – AGR** las puertas de acceso a cada una de las oficinas, oficinas, salas de capacitación y similares deben permanecer cerradas bajo ausencias temporales. Los respectivos centros de cableado, data center y cuartos técnicos en general deben permanecer cerrados y con acceso restringido para personal no autorizado. El centro de datos ubicado en el piso 17 cuenta con control de acceso biométrico (lector de huella) para las personas con permiso a éstos y que han sido autorizados por el Asesor de Despacho – Coordinador TIC, así mismo, las personas que llevan a cabo labores de aseo en las oficinas ingresan acompañados durante el tiempo que dure la labor de aseo en el Centro de Datos.

Por tanto, la Entidad cuenta con el establecimiento y asignación de permisos de acceso a las oficinas, salas de capacitación y similares únicamente a los servidores públicos, contratistas y proveedores autorizados para su acceso.

Así mismo, todas las áreas destinadas al procesamiento o almacenamiento de información sensible, centros de datos, cuartos técnicos, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, son áreas de acceso restringido y en consecuencia cuentan con control de acceso y/o biométrico (lector de huella). Los Centros de Datos, cableado y cuartos técnicos de la Entidad cuentan con mecanismos adecuados contra las amenazas ambientales (temperatura, humedad, fuego, etc.), y se encuentran protegidos con una UPS de respaldo para sostener la operación de la Entidad.

También es responsabilidad de los servidores públicos, contratistas y proveedores no afectar la disponibilidad de los equipos que componen la infraestructura tecnológica en el momento de beber y/o consumir cualquier tipo de alimento cerca de ellos. Se encuentra prohibido ingresar alimentos y/o bebidas a los cuartos técnicos eléctricos y Centros de Datos de la Entidad.

11.3.6. Política de escritorio y pantalla limpia

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los servidores públicos, contratistas y proveedores que tengan un vínculo laboral sea directo o a través de contrato de prestación de bienes y/o servicios para con la **Auditoría General de la República – AGR** deben mantener la información clasificada con acceso restringido o confidencial bajo llave en sus escritorios y/o sitios de trabajo, sea cuando se retiren temporalmente de sus puestos de trabajo o en horas no laborales. Estos documentos incluyen: documentos impresos, dispositivos de almacenamiento, almacenamiento en la nube-cloud, medios removibles en general y similares.

Así mismo, todos los equipos de escritorio y portátiles propios de la **Auditoría General de la República – AGR** deberán usar el papel tapiz y el protector de pantalla corporativo, el

cual se activará automáticamente una vez se bloquee la estación o después de cinco (5) minutos de inactividad, la cual se podrá desbloquear únicamente con la contraseña del usuario.

11.3.7. Política para transferencia de información

La **Auditoría General de la República – AGR** firmará acuerdos de confidencialidad con los servidores públicos, contratistas, proveedores, entidades y ciudadanos que por diferentes razones requieran conocer o intercambiar información restringida y/o confidencial de la Entidad. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo servidor público, contratista y tercero será responsable por proteger la confidencialidad e integridad de la información. Se tendrá especial cuidado con el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiera intercambiar son responsables de definir los niveles y perfiles de autorización para el acceso, modificación y eliminación de ésta, garantizando siempre la privacidad de los datos e información, y los custodios de esta información es responsables de implementar los controles que garanticen el cumplimiento de los criterios de Confidencialidad, Integridad y Disponibilidad requeridos y así mismo, contempla el cumplimiento que se determine y se encuentra asociado al Gobierno de Datos de la Entidad

11.3.8. Política para desarrollo seguro

Las nuevas aplicaciones, desarrollos, y/o sistemas operativos o modificaciones a estos y que soporten los sistemas de información, solamente deben ser implementados en el ambiente de producción después de un protocolo de pruebas adecuado que involucre aspectos funcionales, de seguridad, de compatibilidad con otros sistemas de información y facilidad de uso.

Los desarrollos realizados por la Auditoría General de la República deben cumplir lo descrito en el procedimiento de desarrollo de software en la Guía para el desarrollo de software TI.120.P05. A 01 y deben tener en cuenta los lineamientos dados por OWASP.

Los administradores de las plataformas de producción son los responsables de controlar el acceso y uso de los programas fuente de los sistemas y/o de las aplicaciones que operan en ellas, así como de coordinar y/o ejecutar las actualizaciones programadas. El acceso de los servidores públicos, contratistas y proveedores a los sistemas de producción sólo es permitido para realizar labores de soporte o mantenimiento, previa autorización.

11.3.9. Política para relaciones con proveedores.

La **Auditoría General de la República – AGR** identifica y solicita la respectiva creación de controles de seguridad de la información específicamente con el acceso de los proveedores a los datos e información de la Entidad.

Así mismo, las partes interesadas de la Entidad deben tener conocimiento de sus responsabilidades relacionadas con la seguridad de la información y esta responsabilidad se debe ver reflejada en los contratos que ejecute la **Auditoría General de la República – AGR**

11.3.10. Política para privacidad y protección de información de datos personales.

La Entidad se rige por la Resolución que se encuentre activa sobre Protección de Datos Personales y la cual se encuentra desarrollada para la aplicabilidad de la Ley de Protección de Datos Personales en Colombia en la ruta: **Política de Protección de Datos Personales.**

11.4. Controles definidos y que apoyan tanto a las Políticas Internas como a la Política de Seguridad Digital, Seguridad y Privacidad de la Información de la Auditoría General de la República – AGR

A continuación, se detallan los controles asociados al cumplimiento no solamente de las políticas definidas en el presente documento, sino también para dar cumplimiento a lo establecido en la Norma **ISO/IEC 27001:2022 en su Anexo A**, para garantizar la Confidencialidad, Integridad y Disponibilidad de los datos e información que se almacenan en los activos de información de la **Auditoría General de la República – AGR** que es quien administra, custodia, controla, produce, procesa y modifica en pro del cumplimiento de las funciones y objetivos para lo cual fue creada la Entidad.

11.4.1. Política de Seguridad Digital, Seguridad y Privacidad de la Información.

- Gestionar los riesgos de Seguridad y Privacidad de la Información identificados en la Entidad.
- Cumplir con los niveles de Confidencialidad, Integridad y Disponibilidad establecidos por la Entidad.
- Sensibilizar y apropiar la gestión de Seguridad y Privacidad de la Información en los servidores públicos, contratistas y proveedores de la Entidad.
- Verificar el cumplimiento de las políticas, procesos, procedimientos, instructivos y anexos que integran el Modelo de Seguridad y Privacidad de la Información – MSPI en la Entidad.

11.4.2. Organización de Seguridad de la Información.

11.4.2.1. Organización Interna.

- Todos los servidores públicos, contratistas y proveedores de la **Auditoría General de la República – AGR** deben conocer y dar cumplimiento al Modelo de Seguridad y Privacidad de la Información – MSPI establecido en la Entidad.
- Los servidores públicos que en ejercicio de sus labores tengan acceso a: datos e información, infraestructura tecnológica, aplicaciones, bases de datos y sistemas de

información, deben contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y privilegios establecidos sobre los activos de información que almacenan los datos e información, con el objeto de minimizar el uso o modificación no autorizada sobre los activos de información de la Entidad.

- Todos los sistemas de disponibilidad crítica o media de la Entidad cuentan con reglas de acceso las cuales cuentan con segregación de funciones entre quien las administra, opera, realiza mantenimiento y audita.
- Todos los servidores públicos, contratistas y proveedores son responsables de proteger la información a la cual acceden y procesan, para evitar su pérdida, alteración, destrucción o uso indebido.
- Es responsabilidad de todos los servidores públicos, contratistas y proveedores de la **Auditoría General de la República – AGR** reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los activos de información que se presente en la Entidad a través del CAU.
- No está permitido el uso de los recursos tecnológicos para difundir o participar en actividades de partidos y movimientos políticos ni sociales.

11.4.2.2. Dispositivos móviles.

- Los dispositivos móviles que hagan uso de información de la Entidad o que se conecten a la red se acogerán a las políticas y controles establecidos de seguridad de la información definidas en el presente manual.
- Los dispositivos móviles asignados por la Entidad a servidores públicos, contratistas y/o proveedores autorizados serán configurados por el CAU para su uso a nivel de acceso a correo electrónico y datos e información almacenados en las carpetas de almacenamiento que utilice el servidor público.
- Se restringe la conexión de dispositivos móviles tales como smartphones y/o tablets a las redes principales de la Entidad, a excepción de los dispositivos que sean propiedad de la Entidad o cuenten con autorización expresa del jefe o director de cada oficina.
- Cualquier servidor público, contratista y proveedor tendrá acceso a la información desde las redes externas mediante un proceso de autenticación sobre el uso de conexión segura y cumpliendo los respectivos requisitos de seguridad de los equipos desde donde se accede por medio de conexión VPN autorizada por el Grupo de Tecnologías y Sistemas de Información de la Entidad y la cual se encuentra solicitada y aprobada a través de la solicitud realizada a través del CAU.
- La asignación de dispositivos móviles institucionales está a cargo de la Dirección de Recursos Físicos a los servidores públicos indicados para utilizar estos medios.
- Se permite el uso y conexión de dispositivos móviles que adquiera la Entidad y el cual se encuentre identificado dentro de los inventarios de ésta sobre la infraestructura tecnológica de la **Auditoría General de la República – AGR** siempre y cuando éstos sean utilizados para cumplir con las actividades y funciones de la Entidad y sean revisados por el servidor público o contratista asignado por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y utilizando la herramienta de revisión para software malicioso.

11.4.2.3. Teletrabajo.

- El teletrabajador debe realizar la conexión a través del canal VPN autorizado para acceder a los datos, información, aplicativos web y servicios de nube de la Entidad de una manera segura y conexión privada y a través del equipo asignado por ésta.
- El teletrabajador debe cumplir a cabalidad con lo establecido en el acuerdo de confidencialidad para el uso de la VPN y el acceso a los datos e información de la Entidad.
- El teletrabajador debe reportar cualquier incidente de seguridad y privacidad de los datos e información en la **Auditoría General de la República – AGR** a través del CAU para que sea atendido por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y brinde la(s) solución(es) respectivas a lo reportado.
- En caso de que ocurra pérdida o hurto de un equipo asignado por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información en el cual se lleven actividades de teletrabajo, será de cargo del teletrabajador responsable de este evento, informarlo de forma inmediata a través del CAU o cuenta de correo centrodeservicio@auditoria.gov.co objeto de aplicar las medidas de seguridad adecuadas para la protección de los datos e información contenida.
- Toda información gestionada por la **Auditoría General de la República – AGR** y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.

11.4.3. Seguridad en los Recursos Humanos.

11.4.3.1. Antes de asumir el empleo

- Todos los servidores públicos, contratistas y proveedores de la **Auditoría General de la República – AGR** aceptan las cláusulas de confidencialidad definidos por la Entidad antes de asumir su contratación y/o cualquier prestación de servicios, dicha cláusula hará parte integral en cada uno de los contratos y/o documentos de vinculación a la Entidad.
- Se llevan a cabo las respectivas validaciones definidos por la Dirección de Talento Humano y la Oficina Jurídica de acuerdo con la contratación de terceros, para la verificación de antecedentes de todos los posibles candidatos a servidor público o contratista y/o proveedor en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos en la pertinente verificación realizada.
- Como parte de su obligación contractual los contratistas y proveedores deben aceptar y firmar los términos y condiciones de su contrato de prestación de servicios, en el cual se establecen sus responsabilidades y las acciones a tomar si no se cumple con los términos y condiciones contractuales y las de la Entidad cumpliendo con los establecido en el Modelo de Seguridad y Privacidad de la -información – MSPI.
- Para los servidores públicos, la obligación se encuentra de acuerdo con la posesión de cargo y de acuerdo con lo establecido por la Dirección de Talento Humano en los documentos TH.232.P1 Provisión de cargos de libre nombramiento y remoción carrera administrativa y provisionalidad y TH.232.P21 Retiro, traslado, reubicación o permuta de funcionarios.

11.4.3.2. Durante la ejecución del empleo

- Todos los servidores públicos, contratistas y proveedores ya sean nuevos o antiguos deben recibir el apropiado conocimiento y capacitación en temas de Seguridad y Privacidad de la Información, Protección de Datos Personales, una vez al año y/o cuando se considere necesario y sea definido en conjunto entre la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y la Dirección de Talento Humano o por separado.
- Los servidores públicos de la Entidad cuando incurran en alguna falla que incurra o atente contra la Confidencialidad, Integridad y Disponibilidad de los datos, información, activos de información que se encuentren asignados para el desarrollo de las funciones y responsabilidades asignadas, se les aplicará lo indicado en el documento GJ.110.P13.P Procedimiento para investigar la conducta de los sujetos disponibles dentro de la AGR a través del documento GJ.110.P13.F01_Formato Control Procesos Disciplinarios.pdf.
- Para el caso de los contratistas, estos se regirán por lo establecido en la Ley 1952 de 2019 "Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario." y se traslada a la Procuraduría General de la Nación en caso de incurrir o que atente contra la Confidencialidad, Integridad y Disponibilidad de los datos, información, activos de información que se encuentren asignados para el desarrollo de las funciones y responsabilidades asignadas.

11.4.3.3. Terminación y/o cambio de empleo

- La Dirección de Talento Humano, la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información, la Dirección de Recursos Físicos y el Jefe Inmediato del servidor público y/o supervisor tanto del proveedor, contratista o servidor público, serán los encargados en el proceso de terminación de la vinculación laboral y/o terminación de contratos asegurar que todos los activos físicos y de información propios de la Entidad sean devueltos, los accesos físicos y lógicos sean eliminados, y los datos e información pertinente sea transferida, de acuerdo con los procedimientos que se encuentran establecidos en el Sistema Integrado de Gestión.
- En caso de que un servidor público, contratista o proveedor tenga un cambio de funciones, se deben seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de éstos, acorde con su nuevo rol o contrato de prestación de servicios, asegurando la Seguridad y Privacidad de los Datos e Información.
- Los retiros de los permisos del personal vinculado de manera directa por la Entidad o los contratistas o proveedores son informados a la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información a través del documento de Paz y Salvo emitido en el momento de la finalización de la relación contractual para con la Entidad.

11.4.4. Gestión de Activos.

- La **Auditoría General de la República – AGR** cuenta y aplica el documento **Activos**

de Información para identificar y clasificar los activos de información de todos los procesos al interior de la Entidad.

11.4.4.1. Responsabilidad por los activos de información

- La **Auditoría General de la República – AGR** dispone de un inventario de activos de información clasificado bajo los criterios de Confidencialidad, Integridad y Disponibilidad de la información, así como la clasificación respectiva sobre información pública, información pública clasificada e información pública reservada, actualizado una vez al año.
- Todos los servidores públicos, contratistas y proveedores deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su contrato y/o cada vez que el mismo haga cambio de oficina o responsabilidades al interior de la Secretaría General.
- Es responsabilidad de cada una de las oficinas llevar a cabo la implementación de los controles establecidos con la finalidad de mitigar la materialización de los riesgos identificados y asociados a los Activos de Información.

11.4.4.2. Uso y devolución de los activos de información en la Entidad

Los activos de información que sean asignados a los servidores públicos funciones y responsabilidades y para los contratistas y/o proveedores para la ejecución de las funciones y obligaciones durante la relación laboral para con la Entidad serán utilizados única y exclusivamente para el desarrollo de lo mencionado. No podrán usarse para temas diferentes y que no se encuentren relacionados con las responsabilidades de la Entidad. De igual forma, cada servidor público, contratista o proveedor deberá firmar el respectivo documento sobre el acuerdo de confidencialidad para salvaguardar los datos e información que generen, administren, modifiquen y custodien durante la relación laboral para con la Entidad.

Así mismo, cuando el servidor público o contratista se retire de la Entidad, deberá hacer la respectiva devolución de los activos de información a su cargo, así como la entrega de las credenciales de acceso a las cuentas de correo electrónico, sistemas de información y almacenamiento en la nube donde repose los datos e información que durante su vinculación laboral generó, administró, modificó y custodio para el desarrollo de las funciones y responsabilidades asignadas.

11.4.4.3. Manejo de medios removibles

- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información tiene implementado a través de la consola antivirus el escaneo de medios removibles que son conectados para la búsqueda de virus o malware en éstos de manera automática.
- Los servidores públicos, contratistas y proveedores se comprometen a asegurar física y lógicamente el dispositivo a fin de no poner bajo ningún riesgo, la información de la Entidad y los demás activos de información bajo su custodia.
- Cuando se solicita el reintegro de un equipo sea de escritorio o portátil al almacén, la Dirección de Recursos Físicos notificará a la Oficina de Planeación Grupo de

Tecnologías y Sistemas de Información a través de una solicitud registrada en el CAU para que se realice el proceso de respaldo y borrado información correspondiente.

- Para los medios electromagnéticos y/o digitales donde haya reposado información considerada como información confidencial y/o sensible, y así mismo, la información que el servidor público para el desarrollo de sus funciones y responsabilidades y para los contratistas y/o proveedores corresponde a la ejecución de las funciones y obligaciones y deben ser borrados, eliminados y/o destruidos de forma segura cuando cambien de propósito o sean devueltos por garantía o cuando termine su vida útil.

11.4.4.4. Disposición y transferencia de medios físicos

- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información realiza el debido respaldo de la información sobre los medios que serán dados de baja o reasignados entre servidores públicos y/o contratistas e informará a Dirección de Recursos Físicos para que sean ubicados en el inventario de baja o cambie de responsable y quede actualizado en el respectivo inventario físico de la Entidad acorde con lo establecido en el documento

11.4.5. Control de Acceso.

- En caso de observar posibles eventos/incidentes de seguridad sobre los activos de información o los datos o información estos deben ser reportados a través de las cuentas de correo centrodeservicio@auditoria.gov.co.
- El responsable de las áreas restringidas como Centros de Datos, cuartos técnicos y Despacho del Auditor General asignará los controles necesarios para limitar el acceso a éstos, determinará los mecanismos de registro, datos de identificación servidor público, contratista o proveedor que accede al área restringida, el motivo del ingreso, el tiempo empleado para el desarrollo de la actividad, la información consultada si es del caso, y cuidará que un responsable del área acompañe a la persona durante su estancia en ella.
- En caso de que existan identificadores de usuarios genéricos en cualquier sistema operacional, base de datos, o aplicación, deben estar debidamente individualizados los responsables, validados y gestionados los respectivos riesgos de seguridad digital, seguridad y privacidad de los datos e información y de esta manera, encontrarse aprobados los controles respectivos por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información.

11.4.5.1. Acceso a redes y servicios de red

- Ningún servidor público, contratista o proveedor está autorizado para conectar equipos de escritorio, equipos portátiles y demás recursos tecnológicos a la red que no sean propiedad o bajo el dominio de la **Auditoría General de la República – AGR**, de manera cableada o inalámbrica. Esta conexión se realiza únicamente a través de las solicitudes realizadas a través del CAU.
- Los accesos a la red inalámbrica deberán ser autorizados por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información, previa verificación de que cuente con las condiciones de seguridad, estableciendo mecanismos de control necesarios

para proteger la infraestructura y los datos e información de la Entidad.

- Sólo personal autorizado por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información realizará actividades de administración remota a dispositivos móviles, equipos de escritorio o portátiles, equipos de infraestructura y de procesamiento de información de la **Entidad,** así mismo, las conexiones establecidas para este fin utilizan esquemas y herramientas de seguridad los cuales son definidos y administrados por la mencionada oficina.
- No está permitido el uso de aplicaciones y servicios interactivos como: Team Viewer, TightVNC, RemoteVNC, Chrome Remote Desktop, Join.me, Ammy Admin, Putty, WinSCP, Screen Leap, Vyew, Croos Loop, Skype y similares, los cuales permiten realizar conexiones con cualquier dispositivo y estos atentan contra la seguridad y privacidad de los datos e información que se almacenan en los activos de información de la **Entidad.** Estos bloqueos se realizan a través del Firewall de la Entidad y monitorean el uso del canal de navegación.
- Los equipos de terceros que requieran acceder a la red de la Entidad deben cumplir con lo descrito en los documentos: **TI.120.P03.P Atención a usuarios de la plataforma** tecnológica y **TI.120.P01.P Administración de la infraestructura tecnológica** antes de conceder el acceso solicitado para conectar a la red de la Entidad.
- Los equipos de terceros sólo cuando han sido autorizados para acceder a las redes de datos de la Entidad solo podrán hacerlo una vez haya cumplido con el escaneo para determinar si cuenta con software defectuoso, malicioso y/o que pueda afectar la operación de la Entidad al realizar la conexión a la red, y así mismo cuando se termine la vinculación laboral, debe pasar por la revisión respectiva para proceder a la eliminación de información de la Entidad.
- Los equipos que se conecten a la red y sean propiedad de contratistas o terceros que sean autorizados por el Grupo de Tecnologías y Sistemas de Información deben garantizar que su equipo se encuentra libre de posibles amenazas que atenten contra la confidencialidad, integridad y disponibilidad de los datos e información que administren procesen, genere, modifican y utilizan en la Entidad.
- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información es la única oficina encargada de proveer el servicio de acceso a internet, así como de vigilar su correcto uso y funcionamiento.
- Los accesos para navegación, así como los respectivos permisos para la utilización de los diferentes servicios de TI: correo electrónico, autenticación en Directorio Activo y acceso a sistemas de información, aplicaciones y bases de datos se otorgan acorde a lo indicado por la Dirección de Talento Humano para el caso de servidores públicos y para contratistas y/o proveedores lo realiza el supervisor del contrato.
- El seguimiento y vigilancia se realiza a través de la seguridad perimetral – Firewall y su respectivo uso
- La Oficina de Planeación - Grupo de Tecnologías y Sistemas de Información asignará los permisos de acceso conforme a la necesidad que requiera para la ejecución de las labores de los servidores públicos, contratistas y proveedores a través de las políticas definidas y establecidas en el Firewall perimetral y antivirus de la Entidad.

- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información, cuenta con la facultad para bloquear todos aquellos sitios de Internet que considere que no son compatibles con las labores de los servidores públicos, contratistas y proveedores.
- No está permitido el uso e ingreso a paginas relacionas con pornografía, drogas, terrorismo, segregación racial, hacking, chat, redes sociales, correos electrónicos personales, Web, YouTube, música, videos, TV, juegos y similares que promuevan y atenten contra los principios de Confidencialidad, Integridad, Disponibilidad y Privacidad de los datos e información, salvo que dicha información se requiera para el ejercicio de las funciones al cargo y no exista otro medio para consultarla.
- El acceso a redes sociales en donde tenga presencia la **Auditoría General de la República - AGR** se permite el respectivo acceso.
- No se tiene permitido el uso de programas utilitarios como: editores, depurador de código y/o programa para recuperar datos perdidos o borrados accidentalmente en el disco duro entre otros sin justificación y autorización expresa por parte del Grupo de Tecnologías y Sistemas de Información.
- No está permitido el uso y conexión de dispositivos alternos, que proveen servicio a internet y/o configurar los dispositivos de la Entidad para el acceso a estos medios alternos.
- No está permitido el uso de cuentas de usuario de otros servidores públicos para el ingreso a páginas de internet a las cuales no tiene permisos con el usuario asignado.
- El uso de Internet está permitido exclusivamente para actividades institucionales, los usuarios utilizarán únicamente los servicios para los cuales están autorizados. Este uso de internet se medirá de manera mensual para conocer los sitios con mayor visita y tomar acciones preventivas para minimizar la llegada de correos maliciosos a la Entidad

11.4.5.2. Registro y Cancelación de Usuarios

- El acceso a las plataformas, aplicaciones, servicios y en general a cualquier recurso de datos e información de la **Auditoría General de la República – AGR** cuenta con las autorizaciones de los dueños de procesos propietarios de éstos para su acceso y con los permisos concedidos a través del documento **GJ.110.P13.F01_Formato Control Procesos Disciplinarios.pdf** para servidores públicos mientras que para los contratistas o proveedores será solicitado por el supervisor designado para el contrato.
- Los privilegios de acceso se asignan a los usuarios de acuerdo con las necesidades y eventos, sólo y durante el tiempo requerido y aprobado para ello acorde con lo solicitado en el documento **GJ.110.P13.F01_Formato Control Procesos Disciplinarios.pdf** para servidores públicos mientras que para los contratistas o proveedores será solicitado por el supervisor designado para el contrato.
- Toda asignación de permisos de acceso cuenta con previa autorización del jefe, de área la oficina responsable y se soporta a través de la herramienta que gestiona y administra el CAU por medio del documento **GJ.110.P13.F01_Formato Control Procesos Disciplinarios.pdf** para servidores públicos mientras que para los contratistas o proveedores será solicitado por el supervisor designado para el contrato.
- La entrega de las credenciales del usuario (cuenta y contraseña de red), se entrega a

través del CAU, quien indica una contraseña genérica y de esta última, el usuario realiza el cambio inmediatamente de la contraseña. El usuario y la contraseña se entregan al supervisor del contrato en caso de contratistas o al jefe directo en caso de servidor público y éste la entrega a la persona indicada.

- El servidor público o el contratista al contar con el usuario y contraseña entregado ya sea por el supervisor del contrato o jefe directo encontrará el mensaje de bienvenida para el uso correcto de la cuenta de correo asignada.
- Todos los servidores públicos, contratistas y/o terceros tendrán un identificador único (ID del usuario) para su uso personal e intransferible que les permita acceder y hacer buen uso de los datos e información, sistemas de información e instalaciones.
- Los accesos tanto físicos como lógicos asignados a los servidores públicos, contratistas y/o proveedores deberán ser desactivados y/o modificados una vez terminados los vínculos contractuales con la **Auditoría General de la República – AGR**, teniendo en cuenta los respectivos paz y salvo que llegan a la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información para su respectivo proceso de desactivación.
- Las solicitudes de creación de usuarios para servidores públicos, contratistas y/o proveedores se realizará a través de una solicitud radicada ante el CAU con el documento remitido por la Dirección de Talento Humano o Supervisor de contrato previamente firmada por el jefe directo.
- Cuando el usuario solicita el cambio de la contraseña y se encuentre fuera del dominio o la red, lo realiza a través de solicitud al CAU para una nueva asignación de contraseña y esta se envía por medio de la herramienta establecida, la cual cuenta con la opción ***privado,*** y es sólo visualizada por el usuario solicitante.
- Los derechos de acceso de todos los servidores públicos, contratistas y proveedores para acceder a los datos e información y a los servicios de procesamiento de información se retiran al terminar el vínculo laboral y/o se deben ajustar cuando existan cambios de oficinas y/o responsabilidades.

11.4.5.3. Control de acceso a sistemas y aplicaciones

- La creación de usuarios de ciertos aplicativos se encuentra a cargo de los líderes funcionales o la oficina que administre o tenga el control correspondiente del aplicativo.
- Se cuenta con el control de acceso limitado y controlado a los datos e información que se encuentran en los sistemas de información y aplicaciones ubicados en los ambientes de desarrollo y productivos por parte de los desarrolladores internos o externos que se encuentren laborando para la Entidad.
- Se cuenta con el control hacia el acceso al código fuente de los programas, sistemas de información y el software desarrollado por la **Auditoría General de la República – AGR** solo al personal autorizado y así mismo, se lleva el respectivo control de los cambios autorizados y realizados al código fuente de éstos.

11.4.6. Criptografía.

- La administración de claves criptográficas y certificados digitales estará a cargo de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información quien realiza la entrega respectiva acorde con las solicitudes realizadas a la Jefatura de la

mencionada oficina.

11.4.7. Seguridad Física y del Entorno.

11.4.7.1. Perímetros de Seguridad Física

- Se establecen y asignan permisos de acceso a las oficinas, centros de cableado, data center, salas de capacitación y similares únicamente a los servidores públicos, contratistas y proveedores autorizados para su ingreso.
- Las puertas de acceso a cada una de las oficinas, centros de cableado, data center, salas de capacitación y similares permanecen cerradas y en lo posible bajo llave en ausencias temporales y/o totales.

11.4.7.2. Controles de Acceso Físico

- Todas las personas deben portar el carnet que los acredita como servidores públicos, contratistas y proveedores de la Entidad en un lugar visible y durante su permanencia en la Entidad.
- Los servidores públicos, contratistas y proveedores cuentan con la respectiva tarjeta de proximidad para el ingreso a las instalaciones de la **Auditoría General de la República – AGR**
- Todos los servidores públicos, contratistas y proveedores portan el carné vigente de la Entidad en un lugar visible y durante su permanencia en la Entidad.
- La tarjeta de proximidad es gestionada y entregada por la Dirección de Talento Humano, así como el respectivo carnet que identifica al servidor público, contratista y/o proveedor es entregado por la mencionada dirección u Oficina Jurídica de acuerdo con la resolución de nombramiento o contrato de prestación de servicios que diera lugar.
- Todas las áreas destinadas al procesamiento y/o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido y en consecuencia cuentan con controles adecuados para el control de acceso.
- El ingreso a los Centros de Datos de la Entidad se realiza a través de la tarjeta de proximidad (si aplica) y con bitácora de ingreso de visitantes. Los visitantes ingresan solamente en compañía de una persona del grupo de infraestructura tecnológica de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información.
- La información sensible o confidencial de la **Auditoría General de la República – AGR** se recoge de las impresoras de manera inmediata una vez ésta sea impresa. El uso del servicio de impresión y que se encuentran conectadas a la red utilizan la identificación del funcionario o contratista para autorizar la impresión del documento.
- Todos los terceros se registran al ingreso y portan el desprendible que lo acredita como visitante y el carnet de la Entidad de la cual proviene en un lugar visible y durante su permanencia en ésta, y así mismo ingresan y están en acompañamiento en todo momento por un servidor público o contratista responsable de sus labores al interior de la Entidad.

11.4.7.3. Seguridad de oficinas, recintos e instalaciones

- Los servidores públicos, contratistas y proveedores sólo podrán acceder a las instalaciones físicas portando el respectivo carnet que los identifica con alguna relación laboral con la Entidad.
- Los visitantes sólo ingresarán a las oficinas donde se encuentra el Despacho del Auditor General únicamente con la autorización y acompañamiento pertinente directo desde esas oficinas.
- Se debe registrar el ingreso a los Centros de Datos los visitantes, servidores públicos y contratistas en una bitácora ubicada a la entrada de estas áreas de forma visible.
- Todos los terceros ingresan y están acompañados durante la ejecución de las actividades por un por un servidor público, contratista y/o tercero de la Entidad a los Centros de Datos, cableado y cuartos técnicos de la Entidad.
- Se modifica de manera inmediata los privilegios de acceso físico al centro de cómputo, cableado y cuartos técnicos, en los eventos de desvinculación o cambio en las labores de un servidor público o contratista autorizado.

11.4.7.4. Protección contra amenazas externas y ambientales

- Los Centros de Datos de la **Auditoría General de la República – AGR** cuentan con mecanismos adecuados contra las amenazas ambientales: temperatura, humedad, fuego, entre otras) especificados por los fabricantes de los equipos que albergan.
- No se permite albergar, mantener y/o guardar elementos inflamables dentro de las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones.

11.4.7.5. Trabajo en áreas seguras

- Las áreas seguras se encuentran delimitadas a través de la designación de los espacios de Centros de Datos y cuartos técnicos o eléctricos en la Entidad, a los cuales sólo se puede acceder mediante la debida autorización por medio de biométrico (lector de huella) o acompañado a cada área designada como segura.
- Las personas que llegan de visita a las oficinas de la Entidad ubicadas en el Edificio Elemento PH son debidamente anunciadas a través de la oficina de Correspondencia y ésta autoriza el ingreso a las oficinas de acuerdo con la previa autorización del visitado.

11.4.7.6. Áreas de despacho y carga

- Las áreas de despacho y carga se encuentran delimitadas por la Administración del Edificio Elemento PH acorde a los procedimientos establecidos por éstos para realizar despacho de elementos o recibir elementos que ingresan para la Entidad, por lo tanto, se rige por éstos.

11.4.7.7. Ubicación y protección de los equipos

- Los Centros de Datos de la **Auditoría General de la República – AGR** cuentan con mecanismos adecuados contra las amenazas ambientales: temperatura, humedad,

fuego, entre otras). Adicionalmente se deben cumplir los requisitos de acceso establecidos, para estos y los cuartos de cableado y/o eléctricos.
- No se permite ingresar alimentos y/o bebidas a los cuartos técnicos eléctricos y Centros de Datos de la Entidad.
- También es responsabilidad de los servidores públicos, contratistas y proveedores no afectar la disponibilidad de los equipos que componen la infraestructura tecnológica en el momento de beber y/o consumir cualquier tipo de alimento cerca de ellos.

11.4.7.8. Servicios de suministro

- Los servicios de Centro de Datos cuentan con respaldo de suministro de energía en términos de UPS y Planta Eléctrica, por parte del proveedor de los servicios y Planta Electríca por parte de la administración del edificio donde se encuentran ubicadas las oficinas principales.
- La Entidad cuenta con respaldo de suministro de energía a través de UPS en el edificio donde se encuentran ubicadas las oficinas principales, que brindan seguridad al momento de surtir un corte de energía por parte del proveedor energético de la ciudad.

11.4.7.9. Seguridad del cableado

- El cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información permanecen protegidos a través de canaleta para evitar el deterioro y disponibilidad del servicio.
- Los Centros de Datos, cableado y cuartos técnicos permanecen debidamente asegurados para reducir riesgos por manipulación.

11.4.7.10. Mantenimiento de Equipos

- Se debe planificar e implementar la infraestructura tecnológica teniendo en cuenta los estándares de seguridad (hardening), para su respectivo funcionamiento.
- Durante las actividades de mantenimiento preventivo se mantiene la concordancia con los intervalos y especificaciones del proveedor. Asimismo, se generan los registros a través del CAU a que haya lugar en donde se realiza la trazabilidad de las fallas, personas involucradas y actividades desarrolladas.
- Los respectivos mantenimientos que se realizan a los distintos elementos tecnológicos que soportan las aplicaciones y servicios TI, se realizan acorde con la programación que se maneja en el Grupo de Tecnologías y Sistemas de Información.

11.4.7.11. Retiro de Activos

- El retiro de los equipos puede ser llevado a cabo por cualquier servidor público de la Entidad, ya que éstos cuentan al ingreso a la Entidad con una cláusula de responsabilidad con inventarios y los equipos se encuentran amparados con póliza y está asociado al procedimiento de inventarios.

11.4.7.12. Seguridad de equipos y activos fuera de las instalaciones

- Los servidores públicos, contratistas y proveedores que utilizan los equipos institucionales en préstamo se comprometen a no divulgar los datos e información de

la Entidad mediante la firma del respectivo acuerdo de confidencialidad al momento del ingreso a la Entidad.

- Los equipos portátiles cuentan con su respectivo seguro, que se activa cuando es reportado el incidente de pérdida o robo por parte del usuario que lo tiene a cargo.
- Sin perjuicio de lo anterior, se debe tener en cuenta las siguientes directrices para la protección de los equipos que almacenan o procesan información fuera de las instalaciones de la organización:
    - No dejar el equipo y los medios de almacenamiento sin supervisión en lugar públicos y no protegidos
    - Mantener las condiciones ambientales para proteger el equipo en todo momento (agua, calor, humedad, polvo, campos electromagnéticos fuertes, entre otros)
    - Tomar las medidas de protección contra la visualización de información de acceso o información de la Entidad, por parte de personas no autorizadas.
    - Almacenar la información en los repositorios asignados por la Entidad.
    - Reportar de manera inmediata al CAU cualquier novedad / incidente que se presente con el equipo y la información que puede ser accedida a través de él.

11.4.7.13. Disposición segura o reutilización de equipos

- Todos los equipos que contengan información sensible y/o confidencial en sus medios de almacenamiento deben pasar por un procedimiento de respaldo de la información y posterior borrado seguro de los medios de almacenamiento, que es ejecutado por el Grupo de Gestión TIC antes de su reutilización o finalización de su vida útil.

11.4.7.14. Equipos de usuario desatendidos

- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- Los servidores públicos, contratistas y proveedores son responsables de mantener el escritorio del equipo de cómputo libre de información sensible, confidencial y de uso diario (Carpetas, archivos, accesos directos y similares), para evitar el fácil acceso a la información.
- Todos los servidores públicos, contratistas y proveedores bloquean la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario.
- Al finalizar las actividades laborales, los servidores públicos, contratistas y proveedores cierran todas las aplicaciones y dejan los equipos apagados.

11.4.8. Seguridad en las Operaciones.

11.4.8.1. Procedimientos de operación documentados

- La Entidad cuenta con los siguientes procedimientos y documentos de apoyo para la gestión y administración de la plataforma tecnológica:

- **TI.120.P06.P Procedimiento Respaldo (backup) de información de los servidores y bases de Datos de la AGR**
- TI.120.P06.FI02 Formato Registro Restauración de Backups
- TI.120.P06.FI01 Formato Registro Programación de Backups
- TI.120.P06.ID_Inventario Documental
- **TI.120.P05.P Procedimiento desarrollo de software**
- TI.120.P05.F01 Formato de Pruebas de software
- TI.120.P05.A 01 Guía para el desarrollo de software
- TI.120.P05.ID_Inventario Documental
- **TI.120.P04.P_Procedimiento Gestión de Cambios**
- TI.120.P04.IP_Instructivo General
- TI.120.P04.ID_Inventario Documental
- **TI.120.P03.P_Procedimiento Atención de usuarios de la plataforma tecnológica**
- TI.120.P03.A01_Anexo 1_Prestación Soporte Técnico
- TI.120.P03.ID_Inventario Documental
- TI.120.P03.FI02_Formato Planilla de Registro
- **TI.120.P01.P_Procedimiento Administración de la Infraestructura tecnológica**
- TI.120.P01.I_Instructivo Procedimiento
- TI.120.P01.ID_Inventario Documental
- TI.120.P01.A05_Anexo 5 Plan Recuperación
- TI.120.P01.A02_Anexo 2 Estándares Tecnológicos
- TI.120.P01.A03_Funciones Infraestructura Tecnológica
- I.120.P01.A04 CONFIDENCIAL
- TI.120.P01.A06_Anexo 6_Manual de sistemas_Confidencial

11.4.8.2. Gestión de Cambios

- Es responsabilidad del Grupo de Tecnologías y Sistemas de Información las revisiones periódicas, aprobaciones y evaluación de errores de los cambios programados a nivel de las aplicaciones antes, durante y después de su ejecución y debe existir una aprobación previa de las oficinas interesadas para la ejecución del cambio.
- Es responsabilidad del Grupo de Tecnologías y Sistemas de Información las revisiones periódicas, aprobaciones y evaluación de modificaciones de los cambios programados a nivel de las aplicaciones antes, durante y después de su ejecución y debe existir una aprobación previa de las oficinas interesadas para la ejecución del cambio.
- El mantenimiento y el copiado de las librerías fuente de programas deben estar sujetos a un procedimiento estricto de control de cambios.
- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información deberá mantener actualizados los manuales y guías de los Sistemas de Información, aplicativos y sitios web con los que cuenta la **Auditoría General de la República – AGR**

11.4.8.3. Gestión de Capacidad

- Es responsabilidad del Grupo de Tecnologías y Sistemas de Información monitorear, revisar, proyectar y dar soporte oportuno para el uso y desempeño aceptable de capacidad sobre la infraestructura tecnológica, realizando una revisión periódica sobre la capacidad de lo mencionado, tomar las acciones que se consideren necesarias para mantener la operación de la Entidad y dejar trazabilidad de la revisión y las acciones correspondientes.

11.4.8.4. Separación de los ambientes de desarrollo, pruebas y producción

- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información cuenta con direccionamiento IP a nivel de sistemas operativos Windows y Linux de manera separados para los ambientes de desarrollo, pruebas, taller y producción al interior de la Entidad.
- Por seguridad de la infraestructura, los respectivos listados del direccionamiento IP que se encuentran asignados a: ambiente de pruebas, ambiente de desarrollo y ambiente productivo para garantizar la confidencialidad, integridad y disponibilidad de los datos e información que se administran y gestionan en los mencionados ambientes.

11.4.8.5. Controles contra códigos maliciosos

- Es responsabilidad de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información que todos los activos de información tipo Hardware cuenten con un sistema de antivirus y antispyware instalado y actualizado activamente para la protección contra códigos maliciosos.
- Los equipos de terceros que son autorizados para conectarse a la red de datos de la Entidad deben contar con las medidas de seguridad apropiadas para la gestión, administración, modificación y custodia de los datos e información de la Entidad.
- Únicamente el administrador de la plataforma de antivirus o el CAU cuentan con los permisos necesarios para deshabilitar, remover, eliminar y/o desinstalar el software de antivirus, estas actividades se llevan a cabo bajo autorización previa del jefe de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información.
- Se realizan escaneos a intervalos regulares como control del estado de la infraestructura tecnológica a través de las herramientas de monitoreo Solarwind, Nagios, VMWare para determinar acciones de mejora que sean implementadas y garantizar la operación de la infraestructura tecnológica.
- Los servidores públicos, contratistas y proveedores que cuenten con equipos de escritorio y/o portátiles asignados por la Entidad no deben realizar cambios en la configuración del software de antivirus instalado en los mencionados equipos.
- Los archivos descargados de las cuentas de correo institucionales son revisados a través de la herramienta de escaneo de antivirus. Así mismo, los archivos que se descargan de páginas web son escaneados por la herramienta de antivirus que tiene la Entidad. Este escaneo sólo se aplica a los equipos de escritorio y/o portátiles asignados a los servidores públicos, contratistas y proveedores con asignación de equipo por parte de la Oficina de Planeación Grupo de Gestión TIC para el desarrollo de las funciones y obligaciones asignadas durante el periodo de la relación contractual.

- Ante cualquier sospecha o detección de alguna infección por software malicioso se notifica a la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información a través del CAU para que se tomen las medidas de control correspondientes.
- Los permisos son asignados a través de los grupos que están creados en el Directorio Activo para el funcionamiento en **Auditoría General de la República – AGR**
- A través de la consola antivirus se validan los puertos, servicios y prestaciones similares instaladas en los equipos de escritorio, portátiles o equipos de red que no se requieran específicamente para la funcionalidad de la Entidad y se deshabilitan o en otros casos, se retiran.

11.4.8.6. Respaldo de la Información

- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información genera las respectivas copias de respaldo y almacenamiento de la información almacenada en los sitios autorizados para ésta, de acuerdo con lo definido en el documento **TI.120.P06.P Procedimiento Respaldo (backup) de información de los servidores y bases de Datos de la AGR**.
- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información almacena los medios magnéticos que contienen información de la Entidad en una ubicación diferente a las instalaciones donde se encuentra disponible. El sitio externo donde se resguardan las copias de respaldo cuenta con los controles de seguridad física y medioambiental apropiados.
- Para la restauración de los backups, los administradores funcionales de las oficinas que tengan su backup dentro del software destinado por la Entidad para realizar las copias de respaldo, solicitan una restauración trimestral con el fin de que el administrador de copias de respaldo seleccione la cinta aleatoria del trimestre y la información sea entregada al administrador funcional, para que verifique la autenticidad la restauración de la información.
- El documento **TI.120.P06.P Procedimiento Respaldo (backup) de información de los servidores y bases de Datos de la AGR** explica los pasos a seguir para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

11.4.8.7. Registro de eventos

- Se activa la generación de registros en sistemas y plataformas que soportan las aplicaciones y servicios de TI; estos registros asociados a cambios de configuración, cambios en la asignación de privilegios, información de acceso, intento de uso de recursos, uso de privilegios, transacciones ejecutadas, entre otras y según aplique.
- Para los nuevos sistemas desarrollados in-house o por un proveedor, se producen registros de las actividades de auditoría, excepciones, eventos, fallas y se conservan bajo el periodo establecido por el área funcional y de acuerdo con el Grupo de Tecnologías y Sistemas de Información.

11.4.8.8. Protección de la información de registro (log Information)

- Todos los accesos de usuarios a los sistemas, aplicaciones y redes de datos se

registran y/o conservan con el fin de facilitar las labores de auditoría, en las aplicaciones que ameriten este control de auditoría.
- Se hacen copias de respaldo de información a los sistemas de información que tienen implementado eventos de auditoría, con el fin de que estén disponibles en el caso que se presente un incidente de seguridad de la información

11.4.8.9. Registros del administrador y del operador
- Los sistemas de información de la Entidad registran los cambios realizados por usuario administrador.
- Los accesos de usuarios a los sistemas, aplicaciones y redes de datos se registran y/o conservan con el fin de facilitar las labores de auditoría, en las aplicaciones que ameriten este control de auditoría.

11.4.8.10. Sincronización de relojes
- Todos los relojes de los sistemas de procesamiento de información de la **Auditoría General de la República – AGR** están configurados según lo descrito para los distintos sistemas operativos.
- La configuración se encuentra descrita en el documento **TI.120.P01.A06_Anexo 6_Manual de sistemas_Confidencial.**

11.4.8.11. Instalación de software en sistemas operativos (Operational Systems)
- El software instalado en la Entidad cuenta con su respectiva licencia de validez y legalidad en el mercado.
- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información, verifica el normal funcionamiento de los aplicativos que se entregan a producción o están en producción, con el objetivo de no afectar la integridad, disponibilidad y desempeño de estos.
- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información se asegura que para las aplicaciones desarrolladas internamente o por terceros se realicen las respectivas pruebas antes de salir a producción, lo cual se apoya en lo descrito en los documentos **TI.120.P05.A 01 Guía para el desarrollo de software y TI.120.P05.P Procedimiento desarrollo de software**.
- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información autoriza los accesos temporales y controlados a los terceros para realizar las actualizaciones sobre el software, así como monitorea las actualizaciones, en caso de ser necesario.

11.4.8.12. Gestión de las vulnerabilidades técnicas
- Se realizan análisis de vulnerabilidades en intervalos programados sobre toda la infraestructura tecnológica para evaluar los riesgos a los cuales se encuentra expuesta la mencionada infraestructura para generar los planes de tratamiento apropiados en pro de la mitigación de riesgos.

11.4.8.13. Restricciones sobre la instalación de software
- La instalación de cualquier tipo de hardware y/o software en los equipos de escritorio o

equipos portátiles de la Entidad es responsabilidad de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y por tanto son los únicos autorizados para llevar a cabo esta labor.

- Para las oficinas que solicitan la instalación de software libre, la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información realiza el análisis, verificación y la aprobación para la correspondiente instalación.
- Los medios de instalación de software son los proporcionados por la **Auditoría General de la República – AGR** a través de la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y es de aclarar que cuando se encuentre software instalado en los equipos que no esté debidamente licenciado, el servidor público, contratista o proveedor del equipo es responsable de las consecuencias que se presenten ante la materialización eventos o incidentes de Seguridad.
- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información define y actualiza de manera periódica la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los equipos de la Entidad.

11.4.8.14. Controles sobre auditorías de sistemas de información

- Se realizan revisiones internas programadas o por intermedio de terceros, con el fin de determinar si las políticas, procesos, procedimientos y controles establecidos dentro del Modelo de Seguridad y Privacidad de la Información – MSPI se encuentran conforme con los requerimientos institucionales, requerimientos de seguridad, regulaciones aplicables, y si éstos se encuentran implementados y mantenidos eficazmente.
- Estas auditorías se ejecutan según lo establecido en el programa de auditorías definido por la Entidad y en caso de ser necesario se pueden programar revisiones parciales o totales sobre una o varias líneas de acción o trabajo, oficina, etc., con el fin de verificar la eficacia de las acciones correctivas.
- En caso de requerirse acceso a las aplicaciones o sistemas por parte de los auditores, estos deben ser otorgados de consulta y en condiciones que impidan afectación de la disponibilidad o rendimiento requerido por las aplicaciones o sistemas.
- La información extraída o entregada como parte del proceso de auditoria será gestionada salvaguardando las condiciones de seguridad de información de la misma.

11.4.8.15. Inteligencia de Amenazas

- La **Auditoría General de la República – AGR** se encuentra inscrita a los boletines de seguridad que llegarán al correo tecnología@auditoria.gov.co de COLCERT / CSIRT(GOV-PONAL). En caso de que estos no sean recibidos, se realizará la consulta de los reportes con periodicidad mensual en los siguientes links:
  - **COLCERT** https://www.colcert.gov.co/800/w3-propertyvalue-412601.html
  - **CSIRT PONAL** https://cc-csirt.policia.gov.co/alertas-tips/2023
  - **CSIRT GOBIERNO** https://gobiernodigital.mintic.gov.co/portal/Boletines/

- Estos boletines permitirán tener visibilidad de los eventos de seguridad reportados por dichas entidades y deben ser redirigidos a la persona / equipo responsable del análisis, escalamiento y definición de acción según aplique.

11.4.8.16. Gestión de Configuración

- Las configuraciones de seguridad, hardware, software, servicios que soportan las aplicaciones y servicios TI deben establecerse y respaldarse cuando ocurran cambios en la infraestructura o servicios que las afecten.
- Cuando se ejecute el procedimiento de Gestión de Cambios, se realiza la actualización de la configuración del o los elementos tecnológicos incluidos en el cambio, en el repositorio dispuesto para tal fin por parte de la Dirección de Planeación – Grupo de Gestión TIC.

11.4.8.17. Prevención de Fuga de Datos

- Se realiza control de acceso de puertos USB de los equipos con el fin de restringir copia de información en medios removibles.
- Toda la documentación y archivos de trabajo propios de la labor realizada por los funcionarios y contratistas debe ser almacenada en el repositorio corporativo definido por la **Auditoría General de la República – AGR**. No se debe almacenar información en las unidades de almacenamiento de los equipos.
- Si es necesario el envío de información de la Entidad a través de correo electrónico a personas o entidades externas, esta debe tener como único objetivo el obligatorio desarrollo de las actividades o funciones asignadas dentro del rol o cargo que se desempeñe. No debe reenviarse información a cuentas personales o de terceros que no sean parte interesada para el desarrollo de las actividades asignadas.

11.4.9. Seguridad de las Comunicaciones.

11.4.9.1. Controles de redes

- Únicamente los servidores públicos, contratistas y proveedores autorizados por el Asesor de Despacho – Coordinador del grupo de Tecnologías y Sistemas de Información, previa solicitud a través del CAU por parte de la oficina que lo requiera se conecta a la red inalámbrica de la **Auditoría General de la República – AGR** siempre y cuando el equipo de cómputo sea propiedad de la Entidad. En algunos casos excepcionales por solicitud del Despacho del Auditor General si se suministra una contraseña temporal a eventos especiales como reuniones de alto nivel que involucran personas de otras Entidades.
- La conexión a redes inalámbricas externas para servidores públicos, contratistas y proveedores con equipos portátiles de propiedad de la **Auditoría General de la República – AGR** que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de la Entidad deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información como lo es la conexión autorizada a través de VPN.
- La solicitud de VPN se realiza a través del CAU de la Entidad y se procede a la atención de la solicitud radicada.

11.4.9.2. Seguridad de los servicios de red

- Se realiza el monitoreo de los canales de comunicación, con el fin de establecer en los niveles de operación y desempeño de los mismos y generar los mecanismos de control a que haya lugar.
- Se utilizan conexiones via VPN o protocolos de enrutamiento que establezcan canales privados de comunicación, con el fin de mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito a través de ellas.
- Se definen autorizaciones a través del directorio activo y controles de gestión de acceso con el fin permitir el acceso a servicios o aplicaciones específicas.
- Se define que los servicios de red inalámbrica y de VPN realizarán autenticación previa al uso de los mismos,

11.4.9.3. Separación en las redes

- Se configuraron las reglas específicas en el Firewall, teniendo en cuenta únicamente los servicios, puertos, origen y destino necesarios y expresamente autorizados acorde a lo establecido en las autorizaciones realizadas a los servidores públicos o contratistas o Entidades que se encuentren asociadas a través de los convenios interadministrativos.
- Se tiene distribuida la red conforme a los roles y responsabilidades de los servidores públicos, contratistas y proveedores de la Entidad haciendo uso de VLANs, y se restringe el acceso remoto de las plataformas por medio del uso de VPN previamente autorizadas y de acuerdo con lo establecido en el presente documento.
- Los servicios de información, usuarios y sistemas de información se segregan en las redes.

11.4.9.4. Políticas y procedimientos para transferencia de información

- La política definida para la transferencia de información se encuentra detallada en el numeral **11.3.7. Política para transferencia de información.**
- El único servicio de correo electrónico controlado por la **Auditoría General de la República – AGR** es el asignado directamente por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información, el cual cumple con todos los requerimientos técnicos y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la **Auditoría General de la República – AGR** y de cada responsable, el cual debe mantener únicamente los mensajes relacionados con el desarrollo de sus actividades.

11.4.9.5. Acuerdos sobre transferencia de información

- La comunicación entre Entidades internas y externas a través de accesos dedicados, conmutados y/o públicos, se monitorea en todo momento.
- Se deben establecer y hacer firmar acuerdos para la transferencia de información, confidencialidad o no divulgación para la transferencia de información con las partes interesadas.

11.4.9.6. Mensajería electrónica

- La herramienta autorizada de mensajería instantánea (remoto, chats, llamadas y video conferencias) en la Entidad, es administrada por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información y son los responsables de velar por su actualización y correcto funcionamiento.
- Para iniciar sesión se debe ingresar con las credenciales autorizadas y entregadas por el Grupo de Tecnologías y Sistemas de Información al ingreso en la Entidad y que se encuentran creadas en el directorio activo a solicitud ya sea de la Dirección de Talento Humano o el supervisor del contrato.
- La configuración y seguridad de los chats y reuniones se encuentran incluidos en la confidencialidad e integridad de la herramienta, las cuales pueden ser visualizadas por los usuarios de la Secretaría General.

11.4.9.7. Acuerdos de confidencialidad o de no divulgación

- Los respectivos acuerdos de confidencialidad para el manejo y no divulgación de los datos e información que se conocen a través del desarrollo de las funciones y actividades se establece con la firma y aceptación de conocimiento del presente documento y la respectiva política de seguridad y privacidad de la información que se encuentran relacionadas en los acuerdos de confidencialidad para servidor público y contratista.

11.4.9.8. Filtrado Web

- Se realiza configuración de políticas en el equipo de seguridad perimetral para categorías de navegación relacionadas con pornografía, violencia, racismo, drogas ilegales, actividades ilegales, entre otros.
- A través de la herramienta End-Point es posible aplicar políticas de bloqueo que impidan el acceso a diferentes sitios web.

11.4.10. Adquisición, Desarrollo y Mantenimiento de Sistemas.

11.4.10.1. Análisis y especificación de requisitos de seguridad de la información

- La solicitud de los requerimientos para los sistemas nuevos y/o mejoras en los sistemas existentes especifican los requerimientos de los controles de seguridad cuando los hubiere.
- Se aplica lo establecido en el documento **TI.120.P05.P Procedimiento desarrollo de software.**

11.4.10.2. Seguridad de servicios de las aplicaciones en redes públicas

- El suministro de la información para prueba de aplicaciones es validado por el área usuaria de la aplicación para asegurar que la data es correcta y apropiada. Se validan los acuerdos de confidencialidad para asegurar la respetiva eliminación de dicha información.
- Se apoya la seguridad a través del respectivo análisis de vulnerabilidades que se realiza a la infraestructura tecnológica durante el desarrollo (ambiente de pruebas) y el paso a producción (ambiente de producción) para la identificación de posibles puertas

abiertas y generar la respectiva remediación.

11.4.10.3. Protección de transacciones de los servicios de las aplicaciones (application Services)

- La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en la Auditoría General de la República – AGR cuentan con la respectiva identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información aplicando **TI.120.P05.A 01 Guía para el desarrollo de software**.

11.4.10.4. Procedimientos de control de cambios en sistemas

- Los desarrolladores deshabilitan las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores aseguran que no se permitan conexiones concurrentes a los sistemas de información con el mismo usuario.

11.4.10.5. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

- Se garantiza el control de cambios a los sistemas, sitios web y aplicativos: este control está asegurado mediante una herramienta de control de código fuente para todos los sistemas, sitios web y aplicativos de la **Auditoría General de la República – AGR** De igual manera, cuando hay actualizaciones, mejoras o funcionalidades nuevas a los que están en ambiente productivo, se documenta el control de ese cambio mediante el formato que la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información tiene definido para el efecto, el cual debe contar con la aprobación tanto de la oficina funcional como de la mencionada Oficina. Esto se realiza aplicando **TI.120.P05.A 01 Guía para el desarrollo de software**.

11.4.10.6. Restricciones en los cambios a los paquetes de software

- Los desarrolladores suministran opciones de desconexión o cierre de sesión de los aplicativos (logout) que permiten terminar completamente con la sesión o conexión asociada, las cuales se encuentran disponibles en todas las páginas protegidas por autenticación.

11.4.10.7. Principios de construcción de sistemas seguros

- Se monitorea el desarrollo de software donde se cuenta con el acuerdo de licenciamiento el cual especifica las condiciones de uso del software y los derechos de propiedad intelectual. Esto se lleva a cabo aplicando **TI.120.P05.A 01 Guía para el desarrollo de software**.

11.4.10.8. Ambiente de desarrollo seguro

- Los desarrolladores garantizan que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, se implementan mensajes de error

genéricos.

- El Grupo de Tecnologías y Sistemas de Información cuenta con la separación debida de ambientes: para desarrollo, para pruebas, taller y para producción, acorde con lo establecido e identificado a través del direccionamiento IP a nivel de sistema operativo Windows y sistema operativo Linux.

11.4.10.9. Desarrollo contratado externamente

- Se aclaran los acuerdos sobre: las licencias, propiedad de los códigos y derechos de propiedad intelectual y convenios a que haya lugar en caso de falla de la tercera parte, derechos de acceso para auditar la calidad y exactitud del trabajo realizado, requisitos contractuales para la calidad y la funcionalidad de la seguridad del código, ejecución de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.
- El seguimiento respectivo se apoya en lo descrito en los documentos: **TI.120.P05.P Procedimiento desarrollo de software** y **TI.120.P05.A 01 Guía para el desarrollo de software**.

11.4.10.10. Pruebas de seguridad de sistemas

- Se incorporan chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.
- Se cumplen con las revisiones entre el usuario funcional y desarrollador, realizando pruebas de calidad antes de desplegar aplicaciones o correcciones en producción
- Adicionalmente se gestionan las autorizaciones de despliegue por parte de los usuarios funcionales y se guardan las evidencias de dicho proceso.
- Se implementan los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y pruebas hacía ambiente de producción hayan sido aprobadas tanto por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información como por el área usuaria del sistema o aplicativo en cuestión.

11.4.10.11. Prueba de aceptación de sistemas

- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información en conjunto con los propietarios de los aplicativos realizan las pruebas necesarias: prueba de desarrollo y prueba funcional, para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción.
- La respectiva aceptación de los sistemas se realiza a través de una lista de chequeo que aprueba el dueño funcional del sistema de información, aplicación nueva o cambio que se presente en ella.

11.4.10.12. Protección de datos de pruebas

- No se permite el uso y copia de información operacional como datos de pruebas, salvo autorización previa del rol del Oficial de Seguridad de la Información y el responsable del activo, o previa ejecución de procesos de anonimización de ésta. Esta autorización se solicite cada vez que se requiere realizar la copia información operacional en un sistema de aplicación de prueba; de igual forma, la información operacional se borra

de los sistemas de aplicación de prueba inmediatamente después de haber completado la prueba; se registra el copiado y uso de la información operacional para proporcionar un rastro de auditoría.
- Se certifica que la información entregada a los desarrolladores para realizar las pruebas no revela información confidencial de los ambientes de producción.

11.4.10.13. Seguridad de la información para el uso de servicios en la nube

- Los procesos de adquisición, gestión y salida en producción de servicios en la nube, aplica lo establecido en el **Procedimiento Desarrollo de Software y la Guia de Desarrollo de Software** en cumplimiento de los requisitos de seguridad de la información.

11.4.11. Relaciones con los proveedores.

11.4.11.1. Tratamiento de la seguridad dentro de los acuerdos con proveedores

- Dentro de los acuerdos de servicios con terceras partes se incluye una cláusula la cual autoriza a la **Auditoría General de la República – AGR** a realizar auditoría para validar los controles utilizados por los terceros para el manejo de la información.
- La Oficina Jurídica realiza la respectiva identificación y documentación del proveedor con el cual la Entidad tiene o va a tener una relación contractual.
- Se firman los acuerdos de confidencialidad con relación a transferencias de la información entre la Entidad y terceras partes.
- Mantener un proceso y un ciclo de vida para la gestión de las relaciones con los proveedores.
- La definición de los tipos de acceso a la información que se le brinden al proveedor permitirá realizar el seguimiento y el control del acceso a los sistemas de información, aplicaciones y bases de datos.

11.4.11.2. Cadena de suministro de tecnología de información y comunicación

- Cualquier acceso por parte de un tercero a los recursos tecnológicos o a la información de la Entidad, debe haber cumplido con las autorizaciones respectivas y además contar con los acuerdos o cláusulas de confidencialidad respectivos.
- La resiliencia y si son necesarias, las disposiciones sobre recuperación y contingencias para asegurar la disponibilidad de la información o el procesamiento de la información suministrada por cualquiera de las partes.
- Es obligatorio cumplir con lo indicado en la Política para el control de acceso de terceros que hagan parte de la cadena de suministro TIC.

11.4.11.3. Seguimiento y revisión de los servicios de los proveedores

- Los supervisores de contrato permitirán que los proveedores tengan disponible la información relacionada con el MSPI de la entidad incluidos los procesos y procedimientos para dar cumplimiento de los requisitos de seguridad de la información establecidos. Adicionalmente aprobarán los accesos a otorgar de acuerdo con el tipo de proveedor.
- A cada proveedor de servicio se le diligencia el documento

OI.120.P04.FI04_Evaluación comportamiento proveedores, a través del cual se realiza el seguimiento y posterior evaluación del servicio prestado por los diferentes proveedores de la Entidad.

11.4.11.4. Gestión de cambios en los servicios de los proveedores

- Al momento de terminar las relaciones contractuales con un tercero el cual maneje información de la Entidad, el tercero debe dejar para la Entidad toda la información entregada o construida durante el desarrollo del contrato y eliminar copias en repositorios o equipos externos a la Entidad . Esta validación la realiza la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información a través del Paz y Salvo que se encuentre diligenciando el proveedor.
- La formación, para toma de conciencia del personal de la Entidad involucrado en contratación, relativa a políticas, procesos y procedimientos aplicables sobre Seguridad Digital, Seguridad y Privacidad de la Información.

11.4.12. Gestión de incidentes de Seguridad de la Información.

La atención y gestión de los incidentes reportados a través del CAU se realiza de acuerdo con lo establecido en el documento **Guía Gestión de Incidentes** con la que cuenta la Entidad.

11.4.12.1. Responsabilidades y procedimientos

- El Grupo de Tecnologías y Sistemas de Información cuenta con el respectivo registro en la herramienta de gestión del CAU en donde se encuentra el detalle de la detención, contención, erradicación y recuperación en la Entidad.

11.4.12.2. Reporte de eventos de seguridad de la información

- El CAU se encuentra disponible para el reporte formal de eventos que son reportados por los servidores públicos, contratistas y proveedores que sean posiblemente sospechosos de incidentes de seguridad y privacidad de la información para ser registrado en la respectiva herramienta de gestión y escalado al Oficial de Seguridad de la Información (o quien haga sus veces) de la Entidad.
- Todos los servidores públicos, contratistas y proveedores de la Entidad conocen que deben realizar el reporte de eventos posiblemente sospechosos como incidentes de seguridad y privacidad de la información a través del CAU directamente por la herramienta de gestión o por medio de la cuenta de correo: centrodeservicio@auditoria.gov.co.

11.4.12.3. Reporte de debilidades de seguridad de la información

- Es deber y responsabilidad de todos los servidores públicos, contratistas y proveedores que fungen como usuarios de los sistemas y servicios de información, reportar cualquier evento o incidente que atente contra la seguridad de los activos de información.

11.4.12.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos

- Se cuenta con las categorías de los incidentes de seguridad y conforme a la criticidad, se establecen los mecanismos de atención adecuados para su solución.

11.4.12.5. Respuesta a incidentes de seguridad de la información

- Cuando se realiza el escalamiento, atención y contención del incidente de información reportado a través del CAU, éste se realizará bajo los parámetros establecidos en el documento **Guía Gestión de Incidentes** con el cual cuenta la Entidad.

11.4.12.6. Aprendizaje obtenido de los incidentes de seguridad de la información

- Se toman acciones correctivas oportunas ante los eventos e incidentes de seguridad reportados, con base en el aprendizaje obtenido en la gestión de incidentes de seguridad en la Entidad.

11.4.12.7. Recolección de evidencia

- Se mantienen las evidencias necesarias para establecer el reporte del incidente de seguridad para toda acción de seguimiento contra una persona y/o Entidad. Así mismo se cuenta con los soportes que sean exigidos por una acción legal (sea civil o criminal).

11.4.13. Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio.

11.4.13.1. Planificación de la continuidad de la seguridad de la información

- La **Auditoría General de la República – AGR** dentro de la planificación del Plan de Recuperación de Desastres, se definen la adaptación de los controles de seguridad de la información durante la interrupción de las operaciones.
- El plan de Recuperación de Desastres, realiza la identificación de los procesos críticos de la Entidad, llevando a cabo un análisis de impacto para determinar los procesos y procedimientos más relevantes para la continuidad del negocio.
- Basado en el análisis de impacto realizado, se define la estrategia de Respuesta y Recuperación para los procesos / servicios TI más relevantes para la continuidad del negocio y cumplimiento de la misionalidad de la Entidad.
- Se realiza la planificación de actividades preparatorias, de implementación, de prueba y de ejecución, una vez activado, el Plan de Recuperación de Desastres .
- Lo anterior, lo ejecuta a través del documento Plan Recuperación de Desastres.

11.4.13.2. Implementación de la Continuidad de la Seguridad de la Información

La **Auditoría General de la República – AGR de acuerdo con la Estrategia de Respuesta y Recuperación realiza las activid**ades de implementación de la misma para las aplicaciones y servicios TI que soportan la continuidad de los procesos misionales de la Entidad.

Lo anterior, lo ejecuta a través del documento Plan Recuperación de Desastres.

11.4.13.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información

- La **Auditoría General de la República – AGR** revisa en intervalos programados y regulares definidos por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información la ejecución efectiva del documento TI.120.P01.A05_Anexo 5 Plan Recuperación.

11.4.13.4. Disponibilidad de instalaciones de procesamiento de información

- La **Auditoría General de la República – AGR** revisa y aplica en intervalos programados y regulares definidos por la Oficina de Planeación Grupo de Tecnologías y Sistemas de Información la ejecución efectiva del documento TI.120.P01.A05_Anexo 5 Plan Recuperación

11.4.14. Cumplimiento

11.4.14.1. Identificación de la legislación aplicable y de los requisitos contractuales

- La Entidad cuenta con el respectivo normograma en donde se encuentra el detalle de la legislación actual y requisitos contractuales que se aplican al Modelo de Seguridad y Privacidad de la Información – MSPI) en el documento TI_Normograma en el Sistema Integrado de Gestión de la Entidad.

11.4.14.2. Derechos de propiedad intelectual

- La **Auditoría General de la República – AGR** realiza el respectivo registro de los Sistemas SIA y sus respectivos desarrollos/versiones ante la Dirección Nacional de Derechos de Autor y la marca SIA ante la Superintendencia de Industria y Comercio – SIC, tal como lo indica la Ley de Derechos de Autor en Colombia.
- La **Auditoría General de la República – AGR** identifica y garantiza el cumplimiento adecuado a la legislación vigente y/o requisitos legales aplicables (derechos de propiedad intelectual, protección de registros, privacidad y protección de la información de datos personales, reglamentación de controles criptográficos) relacionados con seguridad de la información.
- Se definen, documentan y actualizan todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la Entidad que son relevantes para cada sistema de información al menos una vez al año y/o cada vez que estos sean requeridos.
- Se asegura que el software que se instala y se utiliza en la Entidad cumple con los requisitos de derechos de autor, licenciamiento de uso y es original.
- La Oficina Jurídica y/o el Grupo de Tecnologías y Sistemas de Información establecen en los contratos cláusulas donde se obligue a no divulgar la información restringida o confidencial de la Entidad, a su vez a utilizar la información únicamente para el desarrollo el objeto del contrato

11.4.14.3. Protección de registros y actividades de seguimiento

- Los registros de los sistemas y plataformas que soportan las aplicaciones y servicios TI se protegen y almacenan de acuerdo con las reglas de respaldo.

- Los registros son transferidos a la Plataforma de Monitoreo para la gestión correspondiente de acuerdo con lo definido.
- Se debe contar con la asignación de privilegios correspondiente para el acceso a los sistemas o herramientas de monitoreo que permiten la visualización de registros.
- La Oficina de Planeación Grupo de Tecnologías y Sistemas de Información realiza la validación periódica de los registros almacenados y documenta las acciones realizadas (si aplica) en las aplicaciones y sistemas críticos de la Entidad.

11.4.14.4. Privacidad y protección de información de datos personales

- Se apoya en lo indicado en el numeral **11.3.10. Política para privacidad y protección de información de datos personales** del actual documento.

11.4.14.5. Revisión independiente de la Seguridad de la Información

- Los sistemas de información se chequean de manera regular en cada vigencia para el cumplimiento con los estándares de implementación de la seguridad.
- Con relación a los procedimientos relacionados con el análisis, desarrollo y mantenimiento de las aplicaciones, se realizan revisiones técnicas con lo cual se determina el incumplimiento de los controles establecidos para tomar acciones de mejora sobre éstos.

11.4.14.6. Cumplimiento con las políticas y normas de seguridad

- La **Auditoría General de la República – AGR** cuenta con revisiones periódicas en cada vigencia para revisar y garantizar el cumplimiento de los controles de seguridad frente al marco regulatorio y los objetivos de la Entidad, a través de la programación de auditorías internas y externas en los intervalos planificados por parte de la Oficina de Control Interno.
- El Comité Institucional de Gestión y Desempeño de **Auditoría General de la República – AGR** apoya y promueve las revisiones del cumplimiento de las políticas de seguridad de la información definidas en el presente documento y/o cualquier otro requerimiento de seguridad.

11.4.14.7. Revisión del cumplimiento técnico

- La Oficina de Control Interno Interna realiza revisiones periódicas al cumplimiento de las políticas de revisión y retención de registros de auditoría y elaboran los informes que permiten la toma de acciones oportunas o corregir situaciones no deseables para la seguridad.

12. GLOSARIO.

Activo de información: Este tipo de activo hace relación a los datos o información que tiene para la Entidad valor en los procesos del modelo de negocio, independientemente de su ubicación. Puede ser un documento físico, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad.
Amenaza informática: Es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS), de la **Auditoría General de la República – AGR**
Análisis de riesgos: Uso sistemático de una metodología para estimar los riesgos de los activos o bienes de información e identificar sus fuentes.
Autenticación: Validación de que un el servidor público es quien realmente se autentica en el sistema al cual está intentando ingresar, se realiza a través de la validación de directorio activo de la **Auditoría General de la República – AGR**
Ciberdefensa: Es el empleo de las capacidades militares ante amenazas o actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales.[8]
Ciberespacio: Es el ambiente, tanto físico como virtual, compuesto por sistemas computacionales, programas y aplicaciones (software), redes de telecomunicaciones incluido el internet, datos e información y la infraestructura física asociada que es utilizada para la interacción entre usuarios, entre máquinas y entre máquinas y usuarios.[9]
Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la Entidad en el ciberespacio.[10]
Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, Entidades o procesos no autorizados.
Continuidad del negocio: Plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, ya sean de carácter administrativo, técnico o legal.
Copia de seguridad: Copia de respaldo de la información.
Criticidad: Medida del impacto que tendría la Entidad debido a un incidente de seguridad de un sistema y que éste no funcione como es requerido.
Custodio: Ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.
Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada.
Encargado de Activo de Información: Individuo, cargo, grupo de trabajo o proceso designado por la Entidad para administrar y hacer efectivos los controles que el responsable

[8] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

[9] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Adaptación Resolución CRC.**

[10] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Adaptación Resolución ITU.**

del activo haya definido, con base en los controles de seguridad disponibles en la Entidad.
Equipo de Cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
Evento de Seguridad de la Información: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.
Gestión de claves: Actividad dirigida a establecer y aplicar los controles que se realizan mediante la implementación de claves criptográficas.
Gestión de incidentes de seguridad de la información: Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión de riesgos: Actividades coordinadas para dirigir y controlar una Entidad con respecto al riesgo. Se compone de la identificación, evaluación y el tratamiento de riesgos.
Habeas data: Derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.
Incidente de Seguridad de la Información: Cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).
Impacto: El costo para la empresa a causa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
Infraestructura: Conjunto de elementos o servicios que se consideran necesarios para la creación y funcionamiento de una Entidad cualquiera.[11]
Infraestructura Cibernética (IC): Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO).[12]
Infraestructura Crítica (IC): Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.[13]
Infraestructura Crítica Cibernética (ICC): Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.[14]
Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

[11] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

[12] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

[13] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Adaptación Ley 8/2011-Gobierno de España.**

[14] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

Infraestructura Estratégica (IE): Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales.[15]

Infraestructura Estratégica Cibernética (IEC): Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y Tecnologías de Operación (TO), sobre las que se soporta el funcionamiento de los servicios esenciales.[16]

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del **Modelo de Seguridad y Privacidad de la Información – MSPI**, que tengan valor para la Entidad y necesiten por tanto ser protegidos de potenciales riesgos.

Medio removible: Medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB, o similares que a futuro llegaren a utilizarse para este fin.

Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una Entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o Entidad.

Parte interesada externa: Ente de control definido dentro del contexto Gubernamental y que se encuentre autorizado para realizar revisiones a través de auditorías o, actúe como asesor para el monitoreo, revisión y actualizaciones del Modelo de Seguridad y Privacidad de la Información – MSPI de la **Auditoría General de la República – AGR**

Parte interesada interna: servidor público que pertenezca a cualquier oficina de la **Auditoría General de la República – AGR**, así como sus proveedores y usuarios finales de los servicios de la Entidad.

Tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario/responsable: Individuo, cargo, grupo de trabajo o proceso, designado por la Entidad, que tiene la responsabilidad de identificar, definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información a su cargo.

Responsable de activo de información: Es el servidor público debe velar porque la información a su cargo sea protegida de manera adecuada.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una

[15] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Adaptación Ley 8/2011-Gobierno de España.**

[16] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

combinación de la probabilidad de un evento y sus consideraciones.
Segregación de tareas: Reparto de tareas sensibles entre distintos servidores públicos para reducir el riesgo del mal uso, deliberado o por negligencia, de los sistemas o información.
Seguridad de la información: Preservación de la Confidencialidad, Integridad y Disponibilidad de la información.
Sensibilidad: Nivel de impacto que una divulgación no autorizada podría generar.
Servicio: Es cualquier acto o desempeño que la Entidad o sus servidores públicos pueden ofrecer a otras personas, en desarrollo de su objeto y funciones.
Soportes físicos: Datos en soporte papel (cartas, informes, normas, contratos) o en medios de almacenamiento físico.
Terceros: Toda persona jurídica o natural, que se relacionan con la **Auditoría General de la República – AGR** como proveedores, proveedores o consultores, que proveen servicios o productos a la Entidad.
Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad.
Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

CONTROL DE CAMBIOS			
ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	**DETALLE DE LOS CAMBIOS EFECTUADOS**	**FECHA DEL CAMBIO**	**VERSIÓN**
Creación del Documento	Se crea el documento		1.0
Documento Inicial	Se incluyen los numerales asociados a los nuevos requisitos de la normal ISO27001:2022 Se ajustan numerales existentes de acuerdo a la validación realizada a nivel operativo.	Septiembre 2023	2.0