Manual

DIR-M-2

Manual de políticas de seguridad y privacidad de la información

Instituto Caro y Cuervo

Grupo de Planeación y Relacionamiento con el ciudadano

07/10/2024

TABLA DE INFORMACIÓN DEL DOCUMENTO

Versión	Fecha de aprobación	Elaborado	Revisado	Aprobado	Descripción del cambio
1.0	20/05/2021	Heilin Guarnizo Rodríguez Contratista-oficial de seguridad de la información	Cristian Velandia Coordinador del Grupo de Planeación y Relacionamiento con el Ciudadano	Comité Institucional de Gestión y Desempeño (CIGD)	Inclusión de la política denominada "5.2.1 gestión de proyectos" Se actualiza la política 5.3.3 terminación y cambio del empleo Se actualiza la política 5.10.2.1 correo electrónico Se articula lo desarrollado en las versiones del documento denominado: ORG-M-04 MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2.0	07/10/2024	Alix Lorena Moreno Córdoba Contratista – Oficial de seguridad de la información	Cristian Armando Velandia Mora - Coordinador del Grupo de Planeación y Relacionamiento con el Ciudadano	Comité Institucional de Gestión y Desempeño (CIGD)	Inclusión de requisitos adicionales de la norma ISO 27001:2013 no especificados en la versión 1.0 de este documento. Inclusión de puntos de control para cada una de las políticas de seguridad de la información basados en los controles descritos de la norma ISO 27001:2013

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las políticas de seguridad y privacidad de la información tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar el adecuado uso de los activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

El presente manual está diseñado en alineación con la política general de seguridad de la información y las políticas específicas que respaldan el Sistema de Gestión de Seguridad de la Información (SGSI). Estas políticas deben ser conocidas y aceptadas por todos los usuarios con acceso a los servicios tecnológicos y a los activos de información de la Entidad.

Este documento tiene como objetivo estructurar y actualizar las políticas del SGSI en el ICC, relacionándolas con los controles establecidos en el Anexo A de la norma NTC-ISO-27001:2013, incluyendo los objetivos de control correspondientes. Todo lo anterior se realiza con el propósito de garantizar el cumplimiento de las políticas de gobierno y seguridad digital establecidas en el Modelo Integrado de Planeación y Gestión (MIPG).

1 OBJETIVO

Establecer los lineamientos para proteger los activos de información y los datos personales teniendo en cuenta los requisitos legales y la norma ISO 27001:2013, con el fin de asegurar el cumplimiento de los principios de privacidad, integridad, disponibilidad y confidencialidad de la información.

1.1 Objetivos específicos

- Implementar el sistema de gestión de seguridad y privacidad de la información soportado en políticas y procedimientos.
- Definir los roles y responsabilidades que el Instituto Caro y Cuervo (ICC) requiere para apoyar el desarrollo de los lineamientos del SGSI y que permita el cumplimiento de las políticas de este.
- Informar a los usuarios de los servicios tecnológicos sobre normas y mecanismos que deben cumplir y utilizar para proteger el hardware, software, canal de comunicaciones, recursos TIC institucionales, así como la información que es procesada, almacenada y transmitida en estos.
- Comprometer a todo el personal de la entidad, mediante charlas de concientización, que se darán a través del plan de sensibilización del SGSI y como parte integral de la charla de inducción para nuevos perfiles sin importar el tipo de vinculación (funcionarios, contratistas, practicantes, entre otros).

- Proporcionar las pautas para la protección, tratamiento y uso de los datos personales y sensibles que reposen en las bases de datos y archivos del Instituto.
- Establecer criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales.

2 ALCANCE

Las políticas de seguridad y privacidad son aplicables a todos los funcionarios, contratistas, docentes, estudiantes, consultores eventuales y otros colaboradores de la entidad, que tengan acceso a la información del ICC de manera local o remota a los de equipos de cómputo, infraestructura tecnológica, canales de comunicación de la entidad, bases de datos, sistemas de Información y documentos físicos.

3 TÉRMINOS Y DEFINICIONES

- **Acción correctiva:** Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.
- **Acción preventiva:** medida de tipo proactivo dirigida a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.
- **Activo:** Cualquier elemento que tenga valor para la organización y el contexto de seguridad digital. Son activos, los elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información –TI–, tecnologías de operación –TO–.
- **Acuerdo de confidencialidad:** Documento en el que funcionarios, contratistas y/o terceras partes de la entidad manifiestan su voluntad de mantener la confidencialidad de la información del ICC, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso, en virtud de la labor que desarrollan.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Bases de datos personales:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Controles:** Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También se utiliza como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Comité Institucional de Gestión y Desempeño (CIGD):** Instancia orientadora del Modelo Integrado de Planeación y Gestión (MIPG), el cual integra las políticas de gobierno y seguridad digital, por lo que se establece entre sus funciones asegurar la implementación y desarrollo de políticas de gestión en materia de seguridad digital y de la información.
- **Confidencialidad:** Propiedad o característica consistente en que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

- **Datos personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Datos personales sensibles:** Aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
- **Disponibilidad:** Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.
- **Encargado del tratamiento de datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del tratamiento.
- **Evento de seguridad de la información:** Presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles o una situación previamente desconocida que puede ser pertinente para la seguridad.
- **Gestión documental:** Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación.
- **Gestión de incidentes:** Conjunto de acciones y procesos tendientes a brindar a las organizaciones fortalezas y capacidades para responder en forma adecuada a la ocurrencia de incidentes de seguridad informática que afecten real o potencialmente sus servicios.
- **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar a seguridad de la información.
- **Información pública:** Toda información que un sujeto obligado genere obtenga, adquiera o controle en su calidad de tal, que ha sido declarada legalmente o por su propietario de conocimiento público y accesible a cualquier persona. Ejemplo: rendición de cuentas.
- **Información pública clasificada:** Información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.
- **Información pública reservada:** Información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses

públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

- **Integridad:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **No conformidad:** Ausencia o fallo de uno o varios requerimientos de la norma ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible o representa un riesgo inaceptable.
- **No repudio:** El emisor no podrá negar el conocimiento de un mensaje de datos ni los compromisos adquiridos a partir de este.
- **Plan de continuidad:** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.
- **Política:** Toda intención y directriz expresada formalmente por la Dirección.
- **Privacidad:** Derecho que tienen todos los titulares de la información, en relación con aquella que involucre datos personales y la clasificada que estos hayan entregado o esté en poder de la entidad, en el marco de las funciones que a ella le compete realizar y que generan en las entidades la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Responsabilidad demostrada:** Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual, a petición de la Superintendencia de Industria y Comercio, deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del tratamiento de datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
- **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 organización para establecer una política y unos objetivos de seguridad de la información, para alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de tratamiento.
- **Tratamiento de datos personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **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 puede ser explotada por una o más amenazas.

4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se relacionan las políticas del Sistema de Gestión de Seguridad de la Información (SGSI) del ICC, estructuradas conforme a los controles establecidos en el Anexo A de la NTC-ISO-27001:2013 y en cumplimiento de las políticas de gobierno y seguridad digital del MIPG.

4.1 Orientación de la dirección para la gestión de la seguridad de la información

Objetivo:

Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos de la entidad y con las leyes y reglamentos pertinentes.

4.1.1 Política General para la Seguridad de la Información

Responsable del control: Todos

En la presente Política de seguridad y privacidad de la información la Dirección General del ICC declara su posición y compromiso respecto al cumplimiento de los requisitos aplicables relacionados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de los activos de información que soportan los procesos de la entidad y apoyan la definición, implementación, operación y mejora continua del SGSI, por medio de la generación y publicación de sus políticas, procedimientos, guías, manuales e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información en el marco de la norma NTC ISO/IEC 27001.

Para asegurar la dirección estratégica el ICC establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Definir roles y responsabilidades con el fin de crear compromisos en la protección de la información.
- Identificar e implementar la tecnología necesaria para fortalecer la seguridad de la información.
- Implementar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Proteger los activos de información, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Proteger la privacidad de los datos personales de los funcionarios, contratistas y terceros administrados y recolectados por el ICC.
- Fortalecer la cultura de seguridad y privacidad de la información en los funcionarios, contratistas y terceros del ICC.
- Garantizar la continuidad del negocio frente a incidentes.

- **Alcance/Aplicabilidad:** Esta política aplica a toda la entidad: funcionarios, contratistas y a los terceros, que tengan acceso a los activos de información.

- **Cumplimiento:** Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento del 100% de la política. Se establecen los diez (10) principios de seguridad que soportan el SGSI del ICC:

1. El ICC decide definir, implementar, operar y mejorar de forma continua un SGSI, con base en lineamientos claros, alineados a las necesidades de la entidad y a los requerimientos regulatorios que le aplican a su naturaleza.
2. El ICC define, comparte y publica los roles y responsabilidades frente a la seguridad y privacidad de la información, aplicables a funcionarios, contratistas o terceros.
3. El ICC identifica, califica y valora sus activos, como base para analizar los riesgos, vulnerabilidades y amenazas a los que están expuestos y así seleccionar e implementar los controles necesarios para reducir los riesgos a un nivel aceptable.
4. El ICC protege la información generada, administrada o custodiada por los procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales, mediante la aplicación de controles, de acuerdo con la calificación de la información de su propiedad o en custodia.
5. El ICC protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. El ICC implementa controles de acceso a la información, sistemas y recursos de red.
7. El ICC exige que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
8. El ICC gestiona los incidentes de seguridad y realiza procesos de auditoría interna que permitan una mejora continua del SGSI.
9. El ICC garantiza la disponibilidad de sus procesos de negocio y la continuidad de su operación, con base en el impacto que pueden generar los incidentes.
10. El ICC garantiza el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

La Dirección General se compromete a proporcionar los medios necesarios para la consecución de los objetivos de seguridad establecidos y asume la responsabilidad de motivar y formar en el conocimiento y cumplimiento de esta Política.

- **Incumplimiento:** El incumplimiento a la Política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.
- **Sanciones por incumplimiento:** Una vez detectada la utilización irregular de las cuentas de acceso a través de las herramientas de monitoreo y análisis de tráfico por parte del Grupo de TI se procederá de la siguiente forma:

Previa verificación de la incidencia de seguridad se suspende el acceso al activo de información afectado y de forma temporal o definitiva el ingreso a internet o los servicios tecnológicos proporcionados por parte del Grupo de TI, según las circunstancias del hecho.

- Tratándose de servidores públicos, deberá informarse por escrito al jefe inmediato del servidor con copia al líder del proceso Disciplinario en aras de verificar, realizar seguimiento y determinar si hay lugar a iniciar acción disciplinaria.
- Cuando se trata de contratistas se informará por escrito al supervisor del contrato con copia al líder del proceso de Adquisiciones y al rol jurídico quienes decidirán acerca de las acciones a seguir, de conformidad con las estipulaciones contractuales y la normatividad legal sobre la materia.

❖ **Punto de Control:** *Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.*

4.1.2 Revisión de la política para la seguridad de la información

Responsable del control: Comité Institucional de Gestión y Desempeño (CIGD).

Esta política se revisa anualmente o cuando se identifiquen cambios en la entidad, su estructura, sus objetivos o alguna condición que afecte la política; para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

Punto de control: *Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.*

5 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.1 Organización interna

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.

5.1.1 Roles y responsabilidades para la seguridad de la información

Responsable del control: Dirección General y Grupo de Planeación y Relacionamiento con el Ciudadano - SGSI

El ICC establecerá los roles y responsabilidades que involucran la administración y operación del SGSI para funcionarios y terceros en el manual del SGSI y las correspondientes a la alta dirección se encuentran en el acto administrativo por el cual se crea y conforma el CIGD.

A continuación, se muestra la matriz de roles y perfiles diseñada para el ICC

Tabla 1 Roles y perfiles ICC

Roles	Responsabilidades
Dirección General	Aprobar roles y funciones relacionadas con la seguridad de la información en los diferentes niveles jerárquicos.
	Asignar los recursos pertinentes para la aplicación eficaz de las Políticas de Seguridad de la Información de la institución.
Usuario final	Cumplir la presente política de acuerdo con su rol como colaborador, así como, personal externo que realice labores en el ICC.
	Asistir a las capacitaciones o sensibilizaciones sobre Seguridad de la Información, de tal forma que tenga conocimiento respecto a las Políticas de Seguridad de la Información.
	Aceptar la responsabilidad de proteger la información contra pérdida, modificaciones y accesos no autorizados de terceras personas.
	Entender claramente su rol y responsabilidad frente al acceso y uso de los sistemas de información.
	Utilizar la información exclusivamente para fines laborales, quedando prohibido explícitamente cualquier uso comercial y/o privado no autorizado.
	Los terceros (contratistas o proveedores) que interactúan con el ICC no deben hacer copias del software suministrado, ni podrán transferirlo a otro equipo por medio de la red, sin previa autorización.
Unidad de Control Interno	Auditar la presente Política de Seguridad de la Información.
	Incluir la seguridad de la información, dentro de los planes de auditoría institucionales.
	Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información
Comité de Seguridad de la Información (Comité Institucional de Gestión y Desempeño)	Revisar y proponer la actualización de Políticas de Seguridad de la Información, funciones, controles y actualizaciones que se deriven del Sistema de Gestión de Seguridad de la Información.
	Definir las necesidades de capacitación que se presenten en el ICC
	Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
	Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

Roles	Responsabilidades
	Garantizar que la seguridad sea parte del proceso de planificación de la información.
	Promover la difusión y apoyo a la seguridad de la información dentro del ICC
	Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
	Coordinar el proceso de administración de la continuidad de las actividades de la entidad.
	Revisar y proponer a la alta dirección del ICC para su aprobación, las políticas y procedimientos generales en materia de seguridad de la información.
	Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
Oficial de Seguridad de la Información	Generar el Plan de la implementación del Modelo de Seguridad y privacidad de la información.
	Actualizar, documentar, sensibilizar y aplicar las normas y estándares aplicables para el mantenimiento de Sistema de Gestión de Seguridad de la Información.
	Reportar al Comité de Seguridad de la Información o quien haga sus veces, la definición, actualización y mantenimiento de los activos de información y riesgos de seguridad digital.
	Mantener y documentar los contactos con las autoridades en materia de ciberseguridad y otros entes especializados para que puedan ser contactados en caso de presentarse un incidente de seguridad de la información que requieran de asesoría, acompañamiento o intercambiar conocimientos para mejorar el sistema de gestión de seguridad de la información y mejorar la respuesta ante incidentes.
	Definir la estrategia de uso y apropiación de la Seguridad de la Información, entrenando en aspectos relacionados con la seguridad de la información a los empleados y contratistas como parte del proceso de inducción y capacitación.
	Establecer indicadores de gestión de Seguridad de la Información en la Entidad.
	Impulsar el mejoramiento continuo de los procedimientos de Seguridad de la Información en la Entidad.
	Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
	Asegurar que los controles de seguridad están de acuerdo con la clasificación de la información.

Roles	Responsabilidades
	Colaborar en la clasificación de la información de la entidad.
	Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
	Asegurar que los incidentes de seguridad del personal sean reportados.
Grupo de Talento Humano	Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan.
	Informar al Grupo de Tecnologías de la Información (TI), el inicio, la terminación o transferencia, licencias y vacaciones de empleados.
	Incluir responsabilidades tanto directas como indirectas en cuanto a Seguridad de la Información en el manual de funciones.
Acompañamiento Jurídico y Contractual	Verificar que el Sistema de Gestión de Seguridad de la Información emitido por la Entidad cuente con el sustento legal que permita su formalización, aplicación y obligatorio cumplimiento previa publicación y difusión.
	Asesorar al ICC en el cumplimiento de las normas legales locales y/o internacionales que afecten a la Entidad
	Alertar al Líder de Seguridad de la Entidad cuando hay cambios en la legislación que afecten la vigencia o haga necesarios ajustes al Sistema de Gestión de Seguridad de la Información de la Entidad.
	Aprobar los acuerdos de confidencialidad de la información con terceros.
	Informar al Grupo de TI, el inicio y la terminación de los contratos de prestación de servicios.
	Incluir las cláusulas de confidencialidad, integridad y disponibilidad de la información en la vinculación contractual.
	Asesorar a la Entidad y a Control Interno Disciplinario, cuando en una investigación aparezcan situaciones que puedan resultar en un litigio que la comprometa.
	Asesorar en la modificación de los contratos de prestación de servicios y en el manual de contratación para que incluyan responsabilidades de Seguridad de la Información.
Grupo de Tecnologías de la Información (TI)	Definir los requerimientos de seguridad, criterios de acceso y respaldo de los activos
	Realizar evaluaciones periódicas de seguridad de la plataforma tecnológica
	Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Control Interno Disciplinario	Definir el proceso disciplinario para el incumplimiento de las políticas de seguridad.

Roles	Responsabilidades
Grupo de Recursos Físicos	Asegurar el control del acceso físico al ICC.

Punto de control: *Se deben definir y asignar todas las responsabilidades de la seguridad de la información.*

5.1.2 Separación de deberes

Responsable del control: Grupo de Gestión Contractual, Grupo de Talento Humano y Grupo de TI.

La separación de deberes define los roles, responsabilidades y niveles de autoridad en la interacción de la seguridad y privacidad de la información, en concordancia con el Manual específico de funciones y competencias laborales; sin perjuicio de lo anterior se establecen los siguientes lineamientos:

- Todo el personal que tenga acceso a la información del ICC debe tener definidos sus deberes frente a la gestión de la seguridad de la información, con el fin de minimizar el uso no autorizado, indebido o accidental de los activos de información.
- En todos los sistemas de información de la entidad se deben implementar controles de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, cuando se tenga la posibilidad de acceder a los sistemas de información.
- El personal que realiza labores funcionales sobre sistemas de información, sean críticos o no, no pueden tener a su cargo labores de administración técnica sobre la plataforma que soporten los sistemas de información.
- El personal contratista del Grupo de TI y el proveedor de servicios de tecnologías de información y comunicación solo tendrá acceso a la plataforma tecnológica de la Entidad en el marco de su objeto contractual.

Puntos de control: *Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.*

5.1.3 Contacto con autoridades

Responsable del control: Grupo de Planeación y Relacionamiento con el Ciudadano y Relacionamiento con el Ciudadano – SGSI

El ICC, debe mantener los contactos actualizados de las autoridades competentes para el cumplimiento de la ley; como los organismos de control (Procuraduría General de la Nación (PGN), Contraloría General de la República (CGR), Fiscalía General de la Nación (FGN)), Fuerzas Militares (Policía Nacional, Comando Conjunto Cibernético).

El Oficial de Seguridad de la Información, debe definir, actualizar y publicar el listado de autoridades a contactar en caso de que se requiera su asesoría y acompañamiento frente a incidentes de seguridad de la información. Para mantener contacto con organismos de control y autoridades; los funcionarios y contratistas pueden consultarlo en este documento.

Tabla 2 Listado de autoridades a contactar

Entidad	Propósito	Contacto
Fiscalía General de la Nación (FGN)	Denuncias	Enlace al servicio de denuncia de la FGN
Policía Nacional Centro Cibernético Policial	Desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.	Enlace al Cai virtual Policía
CSIRT de Gobierno	Centro de coordinación de atención a incidentes de seguridad informática colombiano. Se encarga de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática.	Csirtgob@mintic.gov.co 01 8000 910742 Opción 3 Enlace a Centro de coordinación de atención a incidentes de seguridad informática colombiano
COLCERT	Respuesta a Emergencias Cibernéticas de Colombia	Enlace a la página web del Grupo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT
Superintendencia de Industria y Comercio (SIC)	Corresponde la protección de la competencia, propiedad industrial, protección de los datos personales	Enlace a la página de la Superintendencia de Industria y Comercio

Punto de control: *Se deben mantener contactos apropiados con las autoridades pertinentes.*

5.1.4 Contacto con grupos de interés especial

Responsable del control: Grupo de Planeación y Relacionamiento con el Ciudadano – SGSI y Grupo de TI.

El ICC, debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información, recibiendo comunicados de actualizaciones de software, notificaciones de ataques de vulnerabilidad día cero, avisos de ciberataques o ataques cibernéticos,

reporte de vulnerabilidades y amenazas nuevas. El principal contacto que el ICC tiene a nivel de entidad pública es el MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones).

Punto de control: *Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.*

5.1.5 Seguridad de la información en la Gestión de proyectos

Responsable del control: Grupo de Tecnologías de la Información (TI)

Todas las adquisiciones y proyectos que tengan cualquier componente tecnológico tal como licenciamiento, software, sistemas de información, dispositivos de red, computadores, impresoras, escáner, entre otros deben contar con la revisión y aprobación del Grupo de TI con el objetivo de garantizar la prestación y soporte de los servicios digitales dentro de los acuerdos de niveles de servicio de este grupo, es por esto que debe involucrarse al Grupo de TI desde la fase de planeación del proyecto.

Punto de control: *La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto***.**

5.2 Dispositivos móviles y teletrabajo

Objetivo: Garantizar la seguridad del uso de dispositivos móviles.

5.2.1 Dispositivos móviles

Responsable del control: Grupo de Tecnologías de la Información (TI)

Para los funcionarios y contratistas a quienes el ICC les asigna dispositivos móviles institucionales (portátiles, tabletas, celulares u otros) para el desempeño de sus labores, deben obedecer las siguientes directrices:

- El Grupo de TI tiene como función exclusiva el mantenimiento y la instalación de software en los computadores, que son propiedad del ICC; ellos son los únicos usuarios con credenciales de acceso para realizar este tipo de actividades.
- En los dispositivos móviles propiedad del ICC, no se permite guardar información personal, música o videos; tampoco debería guardarse información relacionada al Instituto.
- Los requerimientos tales como la instalación de un software adicional, configuraciones y/o soporte técnico se deben solicitar a través de la mesa de ayuda dispuesta por el Grupo de TI.
- El préstamo de computadores portátiles se debe tramitar a través de la mesa de ayuda con anticipación y se proveerá según disponibilidad.

- En caso de pérdida o robo de dispositivos móviles propiedad del ICC, se debe reportar a través de correo electrónico al coordinador del Grupo de Recursos Físicos y a las autoridades pertinentes.
- Los dispositivos móviles deben contar con un software antivirus instalado y actualizado.
- El Grupo de TI debe configurar únicamente perfiles institucionales, es decir, el ingreso a estos equipos debe realizarse mediante usuario y contraseña.
- Los dispositivos móviles que no sean propiedad del ICC tales como computadoras portátiles, celulares, tabletas, entre otros, pueden conectarse a la red pública dispuesta por la Entidad y deben obedecer las siguientes directrices:
    - Los dispositivos móviles personales como (portátiles, tabletas, IPad, cámaras y PDA) deben ser registrados en las porterías de la Entidad con el objetivo de poder realizar su retiro sin requerir autorización del Grupo de TI.
    - Se debe solicitar autorización al Grupo de TI para conectarse a la red cableada o a la red inalámbrica corporativa.
    - El dispositivo móvil debe tener instalado un software antivirus el cual debe encontrarse activo y actualizado, así como el cortafuegos (firewall) habilitado y la aplicación de parches.
- El Grupo de TI no prestará servicio de soporte técnico (revisión, mantenimiento, trámite de garantías y/o reparación de hardware) a equipos que no sean propiedad del ICC.
- El ICC no se hará responsable, en caso de pérdida o daño, de algún equipo informático de uso personal que haya sido ingresado a sus diferentes instalaciones.
- En caso de robo o pérdida del dispositivo móvil personal, el usuario está obligado a cambiar inmediatamente las contraseñas de acceso a los sistemas de información y aplicaciones de la Entidad, esto en aras de proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

Punto de control: *Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.*

5.2.2 Teletrabajo

Responsable del control: Grupo de Planeación y Relacionamiento con el Ciudadano – SGSI, Grupo de Talento Humano y Grupo de Tecnologías de la Información (TI).

Se establecen los lineamientos en materia del Sistema de Gestión de Seguridad de la Información que tiene los colaboradores que se acogen a la modalidad de Teletrabajo para el uso, administración, consulta y operación de los servicios en las áreas de teletrabajo, y para los contratistas que se acogen al trabajo remoto:

- El Grupo de Talento Humano debe realizar la verificación de las condiciones del lugar destinado al teletrabajo de funcionarios, para el cumplimiento de las condiciones de seguridad y salud en el trabajo con la asesoría de la Administradora de Riesgos Laborales.

- El grupo de TI deberá establecer y divulgar el uso de la información y los servicios tecnológicos necesarios para garantizar el adecuado funcionamiento de la modalidad de teletrabajo y trabajo remoto.
- Los computadores de propiedad de los colaboradores, se les debe realizar la verificación de los requerimientos tecnológicos del equipo previa solicitud al Grupo de TI.
- Los computadores propiedad de los colaboradores deberán cumplir con control de acceso (usuario – contraseña o PIN de seguridad en el inicio de sesión).
- El oficial de seguridad de la información será responsable de identificar los riesgos de seguridad de la información en la modalidad de teletrabajo y proponer los controles que sirvan para mitigarlos.
- El Grupo de TI deberá implementar los controles necesarios que permitan el acceso remoto a las aplicaciones o servicios tecnológicos a los colaboradores que realicen actividades en teletrabajo, las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la entidad. De igual modo, se deben tener en cuenta la revocación de servicios cuando el colaborador no continúe realizando actividades de teletrabajo.
- Cualquier funcionario o contratista, que requiera tener acceso a la información de la entidad desde redes externas, debe acceder remotamente mediante un proceso de autenticación y autorización de dirección IP pública; haciendo uso de conexiones seguras (https, VPN), y uso del instrumento *COM-G-8 Guía de orientación para la activación de doble factor de autenticación - Sophos VPN.*
- Toda información gestionada y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.
- En la modalidad del teletrabajo, la información debe ser procesada y almacenada en los repositorios en nube del ICC.
- El teletrabajador no debe ceder en ningún caso a terceras personas la información a la que tenga acceso.
- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y en ninguna circunstancia, en computadores públicos o de uso compartido

Punto de control: *Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo*

6 SEGURIDAD TALENTO HUMANO

6.1 Antes de asumir el empleo

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

6.1.1 Selección

Responsable del control: Grupo de Talento Humano y Grupo de Gestión Contractual

El Grupo de Talento Humano para el caso de los funcionarios y el Grupo de Gestión Contractual para el caso de los contratistas, deben llevar a cabo una verificación de los antecedentes de todos los candidatos a un empleo de acuerdo con la normatividad vigente.

Esta verificación debe incluir lo siguiente:

- Una verificación (completa y precisa) de la hoja de vida del solicitante.
- Confirmación de las certificaciones académicas y laborales.
- Una verificación más detallada, como la información de antecedentes penales.

Los grupos de Gestión Documental, Talento Humano y Gestión Contractual, deben establecer los mecanismos y controles necesarios para proteger la información contenida en las historias laborales y expedientes contractuales.

Para el contrato del rol de seguridad de la información específico, se deberá asegurar que el candidato tenga la competencia necesaria para desempeñar dicho rol.

Los servidores funcionarios, contratistas y terceros que desarrollen funciones u obligaciones contractuales en el ICC, estarán sujetos a clausulas o acuerdos de confidencialidad dados por la criticidad de los activos de información bajo su custodia.

Se debe asegurar que todos los funcionarios y terceros a los que se brinde información clasificada y/o reservada deben firmar un acuerdo de confidencialidad y no divulgación antes de obtener accesos a esta.

Se debe establecer las responsabilidades y derechos legales de los colaboradores con relación a leyes sobre derechos de autor o legislación sobre protección de datos.

Punto de control: *Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.*

6.1.2 Términos y condiciones del empleo

Responsable del control: Grupo de Talento Humano y Grupo de Gestión Contractual

Los acuerdos con funcionarios y contratistas deben establecer sus responsabilidades y las del Instituto en cuanto a seguridad de la información.

Se deben establecer acuerdos o compromisos donde se indiquen las responsabilidades en cuanto a la seguridad de la información.

- Firma del formato de autorización de tratamiento de datos personales.
- Se deberá incluir una cláusula en las minutas de contrato y manuales de funciones, en relación con el cumplimiento de la Política de Seguridad y Privacidad de la Información.

Punto de control: *Los acuerdos con empleados y contratistas deben establecer sus responsabilidades y las de la entidad en cuanto a la seguridad de la información.*

6.2 Durante la ejecución del empleo

Objetivo: Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

6.2.1 Responsabilidades de la dirección

Responsable del control: Dirección General

La Dirección General en su interés por proteger la información, fomentará la cultura de seguridad de la información, promulgando la presente política. Todos los funcionarios y contratistas deben cuidar no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Entidad.

El cumplimiento de las Políticas de Seguridad de la Información por parte de todos los funcionarios, contratistas, proveedores, terceros o cualquier persona que tenga una relación contractual o situacional con la Entidad, o que tengan acceso a los activos de información debe ser informado en el momento que inicie sus actividades laborales y/o contractuales desde el Grupo de Talento Humano y/o del Grupo de Gestión Contractual.

Punto de control: *La dirección debe exigir a todos los funcionarios y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la entidad.*

6.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Responsable del control: Grupo de Planeación y Relacionamiento con el Ciudadano – SGSI

El Grupo de Talento Humano, desde su Plan de Capacitaciones y actividades de inducción debe asegurar que los funcionarios y contratistas del ICC comprendan sus responsabilidades en relación con las políticas de seguridad de la información de la entidad y actúen de manera consistente frente a las mismas, para reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de esta.

El Grupo de Gestión de Talento Humano y el Grupo de Gestión Contractual, deben:

- Asegurar que los funcionarios y contratistas respectivamente conozcan y acepten la política de seguridad de la información, para esto deben informar al Oficial de Seguridad de la Información para que les indique las medidas a seguir para el acceso a esta política.
- Establecer los mecanismos para asegurar que los funcionarios asistan a las charlas de sensibilización en seguridad de la información brindadas. Se debe tener en cuenta el manejo de datos personales, clasificación de la información, solicitud de recursos tecnológicos, incidentes de seguridad de la información y puntos de información para asesoría sobre seguridad de la información.
- Dar a conocer a los funcionarios y contratistas o terceras partes que desempeñen funciones en la Entidad, las políticas, roles, responsabilidades y obligaciones en materia de seguridad y privacidad de la información, incluyendo la protección de datos personales.

Los programas de concientización y entrenamiento deben cubrir todas las dependencias, grupos y personas de la Entidad, iniciando desde la Alta Gerencia. Todos los funcionarios y contratistas de la entidad deben estar involucrados y participar activamente en el programa. Se debe garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente. En los casos en que así se establezca, este entrenamiento deberá extenderse al personal de contratistas o terceros, cuando sus responsabilidades así lo exijan.

Punto de control:
Todos los empleados de la entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos del ICC pertinentes para su cargo.

6.2.3 Proceso disciplinario

Responsable del control: Control Interno Disciplinario

El ICC debe contar con un proceso formal para emprender acciones contra funcionarios o terceros que hayan cometido una violación a la seguridad y privacidad de la información. Los funcionarios y terceros deben cumplir a cabalidad las políticas y procedimientos de seguridad y privacidad de la información, implementados en el ICC, entendiendo que cualquier incumplimiento puede conducir a procesos disciplinarios o sanciones de acuerdo con la normatividad vigente.

Es responsabilidad de los funcionarios y terceros proteger los activos que estén bajo su custodia contra acceso, divulgación, modificación, destrucción o interferencia no autorizada, haciendo cumplir las medidas de seguridad implementadas por la Entidad, cabe precisar que los responsables por propender el buen uso de los activos de información por parte de contratistas y terceras partes son los supervisores de contrato.

Punto de control: *Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.*

6.3 Terminación y cambio de empleo

Objetivo: Proteger los intereses del ICC como parte del proceso de cambio o terminación del empleo.

6.3.1 Terminación o cambio de responsabilidades de empleo

Responsable del control: Grupo de Talento Humano, Grupo de Gestión Contractual y Grupo de Tecnologías de la Información (TI).

El Grupo de Talento Humano y/o de Gestión Contractual debe reportar al Grupo de Tecnologías de la Información las novedades administrativas tales como: el retiro de un funcionario o una terminación o cesión de contrato para el caso de los contratistas para retirar credenciales de acceso a los diferentes sistemas de información, verificar la entrega de la información y supervisar la correcta devolución de los equipos y recursos asignados al usuario de la red.

El Grupo de Talento Humano debe reportar al Grupo de TI los movimientos internos de personal en la entidad, y así ajustar los nuevos roles, revocar los privilegios de acceso a los sistemas de información y datos sensibles de la dependencia o grupo a la que perteneció el funcionario.

Se debe comunicar al colaborador, las responsabilidades y deberes de seguridad y privacidad de la información que permanecen válidos después de la terminación o cambio de empleo o de contrato.

El Grupo de TI debe dar el visto bueno al proceso de paz y salvo después de validar que se han desactivado las cuentas de acceso a los servicios tecnológicos del ICC y que el jefe inmediato o supervisor ha recibido la copia de respaldo de la información. El paz y salvo debe ser requisito para completar el proceso de desvinculación.

Los usuarios de los servicios tecnológicos que terminen su vínculo contractual con la entidad, se les desactivará inmediatamente sus cuentas de acceso, incluyendo la del correo electrónico. El Grupo de Tecnologías de la Información dispondrá de una semana para realizar la copia de respaldo de la información del equipo y del correo en formato .pst. En caso de que la cuenta de acceso no tenga ningún tipo de actividad en un periodo de (5) cinco meses se eliminará dicha cuenta.

Para las cuentas de acceso de los funcionarios una vez recibido el acto administrativo por parte del Grupo de Talento Humano, el Grupo de TI, deben mantener activos los accesos por un lapso de 15 días hábiles dando cumplimiento a la Ley 951 del 2005 en las condiciones para la entrega del cargo.

Punto de control: *Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.*

7 GESTIÓN DE ACTIVOS

7.1 Responsabilidad por los activos

Objetivo: Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

7.1.1 Inventario de activos

Responsable del control: Todos

Los líderes de proceso son responsables de identificar y mantener actualizados los activos de información de su respectivo proceso, asignando a cada activo un responsable y un custodio, conforme al documento establecido para la gestión de activos, los activos deben quedar registrados en el sistema de información dispuesto por el Grupo de TI.

Se deben identificar, clasificar, valorar y mantener un registro actualizado y exacto de todos los activos de información, el cual debe ser actualizado al menos una vez por año por los líderes de cada grupo.

Punto de control: *Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.*

7.1.2 Propiedad de los activos

Responsable del control: Líderes de procesos

Los propietarios de los activos de información son responsables de establecer y revisar periódicamente las restricciones y privilegios de acceso lógico y físico a los activos de información. Adicional a ello; validar que los activos de información se encuentren clasificados apropiadamente. El propietario de un activo de información es responsable de validar que los activos a su cargo cuenten con los controles requeridos para preservar los objetivos de legalidad, finalidad, integridad, confidencialidad y disponibilidad. Todos los activos de información deben tener asignado un custodio que tiene la responsabilidad de hacer efectivos los controles de seguridad que el propietario del activo haya definido.

Punto de control: *Los activos mantenidos en el inventario deben tener un propietario.*

7.1.3 Uso aceptable de los activos

Responsable del control: Grupo de Gestión Documental y Grupo de Tecnologías de la Información (TI)

Los activos de información pertenecen al ICC, y el uso de estos debe emplearse exclusivamente con propósitos institucionales. El Grupo de TI controla el software y los equipos autorizados que podrán ser utilizados por los usuarios de la red de datos del ICC para la creación, edición y desarrollo de nuevos activos de información.

El Grupo de TI es la única dependencia autorizada para realizar la instalación y configuración de hardware y software. El ICC proporcionará al usuario los equipos informáticos necesarios para el cumplimiento de sus obligaciones y/o funciones, los datos y la información creados, almacenados y recibidos serán propiedad de ICC.

Los usuarios de la red de datos institucional son responsables del acceso a redes externas, deben verificar que todos los archivos o material recibido a través de medios electrónicos se encuentran libres de software malintencionado, mediante la ejecución de la herramienta de escaneo en busca de software malintencionado que poseen los antivirus para detectar posibles virus insertados.

Todos los funcionarios y terceros deben hacer buen uso de los activos de información a los cuales tienen acceso y que son propiedad del ICC, de igual forma son responsables de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.

7.1.3.1 Acciones prohibidas sobre el uso de los activos de información

A continuación, se mencionan actos de mal uso, sin embargo, estos no se limitan a:

- La utilización, transmisión o almacenamiento de cualquier archivo físico, digital o electrónico, dato o registro de información que viole la política de confidencialidad o las directrices o políticas en materia de gestión de la información está prohibido.
- Los servicios tecnológicos no podrán ser utilizados, para divulgar, propagar o almacenar contenido que razonablemente puede considerarse una amenaza, acoso u ofensa para cualquier persona, contenido de tipo personal o comercial de publicidad, promociones, ofertas, prácticas de juegos en línea, programas destructivos (virus), material político/religioso o cualquier otro uso que no esté vinculado con las labores institucionales.
- No se permite la navegación en internet a sitios de alto riesgo, de contenido: pornográfico, terroristas, racistas, comunidades sociales, o cualquier contenido que represente riesgo para la red de la Entidad.
- No se permite la manipulación de las impresoras, ni la apertura de los computadores, cualquier reporte para solución de fallas debe ser reportado a la mesa de ayuda al Grupo de TI.

- No se permite crear datos falsos o engañosos a través del uso de los servicios tecnológicos de la Entidad.
- Los usuarios no deben ofrecer acceso a los servicios tecnológicos (ej. Redes LAN o red WIFI) o poner a disposición datos a personas no autorizadas, la única dependencia que puede proveer acceso a los servicios tecnológicos es el Grupo de TI.
- No se permite dañar, borrar, deteriorar, alterar, ocultar o suprimir datos.
- No se permite el uso de peer-to-peer (P2P) para el intercambio de archivos a fin de obtener ilegalmente material con derechos de autor y la instalación de software que no ha sido aprobado para su uso.
- Realizar copias no autorizadas de material protegido por derechos de autor propiedad del ICC que incluye, pero no está limitado a información física, digitalizada o distribución de fotografías, audios o videos.
- Utilizar programas sin su respectiva licencia obtenidos a partir de otras fuentes puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que esta práctica no está autorizada.
- Suplantar o facilitar la cuenta de usuario, enviar correos electrónicos a nombre de otro usuario sin autorización o suplantándolo.
- Redireccionar los correos electrónicos institucionales a cuentas de correo personales.
- Burlar los mecanismos de seguridad, autenticación, autorización o de auditoría, de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

Punto de control: *Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.*

7.1.4 Devolución de los activos

Responsable del control: Todos

Al finalizar su empleo o contrato, los colaboradores deben devolver todos los activos de información que se encuentren a su cargo y que fueron suministrados por el ICC para el cumplimiento de sus funciones u objeto del contrato.

Punto de control: *Todos los empleados y usuarios de partes externas deben devolver todos los activos del ICC que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo*

7.2 Calificación de los activos

Objetivo: Asegurar que el ICC reciba un nivel apropiado de protección de acuerdo con su importancia para la entidad.

7.2.1 Clasificación de la información

Responsable del control: Líderes de procesos, rol Oficial de Seguridad de la Información, Grupo de Gestión Documental y Líder del SIG.

El ICC, definirá los niveles adecuados para clasificar su información de acuerdo con su sensibilidad donde se valorarán por confidencialidad o integridad o disponibilidad de la información. Estos niveles deberán ser oficializados y divulgados a los colaboradores. Toda Información perteneciente al ICC, deberá ser identificada y clasificada de acuerdo con los siguientes niveles los cuales son establecidos por la Ley 1712 de 2017 de Transparencia y Acceso a la Información Pública.

La calificación de los activos de información debe recibir un nivel apropiado de protección de acuerdo con la importancia para el proceso y la Entidad, la calificación proporcionada a los activos debe quedar registrada en el sistema integrado de gestión SIG.

Punto de control: *La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.*

7.2.2 Etiquetado de la información

Responsable del control: Grupo de Gestión documental, rol Oficial de Seguridad de la Información y Líder del SIG.

Se debe desarrollar e implementar procedimientos, mecanismos o herramientas para el etiquetado de la información física y digital, acorde con los niveles de clasificación definidos y adoptados, dichas etiquetas permiten reconocer fácilmente la importancia del activo. La información que se intercambie con otras entidades debe incluir la calificación correspondiente y se debe informar a su destinatario la interpretación de la calificación para que se asignen las protecciones necesarias.

Punto de control: *Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por el ICC.*

7.2.3 Manejo de activos

Responsable del control: Grupo de Gestión documental y Grupo de Tecnologías de la Información (TI)

Para la disposición final de los activos de información de tipo “información” se deberá seguir lo dispuesto en los lineamientos de Gestión Documental. Se deben realizar restricciones de acceso que soporten los requisitos de protección para cada nivel de clasificación:

- Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación.

- Registro formal de los receptores autorizados de los activos;
- Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original;
- Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes.
- Marcado claro de todas las copias de medios para la atención del receptor autorizado.

Punto de control: *Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la entidad.*

7.3 Manejo de medios

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

7.3.1 Gestión de medios removibles

Responsable del control: Grupo de Tecnologías de la Información (TI)

Los medios removibles son todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores, por ejemplo: memorias USB, discos duros externos, entre otros, el uso de estos puede ocasionalmente generar riesgos para la entidad al ser conectados en la red de la Entidad, ya que son susceptibles a la transmisión de virus.

Se debe procurar evitar el uso de medios removibles para custodiar información del ICC. Es responsabilidad del usuario hacer el cifrado de todo medio removible (incluso los de propiedad personal) en los cuales se almacene y transporte información del ICC y sea calificada como clasificada o reservada.

Para los equipos de cómputo que tienen habilitados los puertos USB y las unidades reproductoras de CD/DVD, se deben seguir las siguientes directrices:

- El escaneo automático de virus debe estar habilitado. En el software de antivirus debe configurarse el bloqueo de la reproducción automática de archivos ejecutables.
- El funcionario, colaborador o tercero que utilice medios de almacenamiento extraíbles con información del ICC, será responsable del buen uso, divulgación y distribución de esta.
- En caso de pérdida de un medio de almacenamiento extraíble debe informarse al Grupo de TI, precisando la criticidad de la información. En caso de ser crítica se debe realizar el denuncio ante autoridad policial.
- En caso de ser transportados los medios de almacenamiento extraíble, deben protegerse del acceso no autorizado o uso indebido.
- Todo medio removible propiedad del ICC (incluido token) que deba ser retirado de las instalaciones propias de la Entidad, deberá ser informado por su custodio al jefe inmediato o

supervisor de contrato para su respectiva autorización. En caso de que estos medios contengan información sensible, clasificada o reservada, deberán implementarse controles de seguridad como el cifrado del dispositivo o de información, de acuerdo con la política de Controles Criptográficos.

- Se prohíbe el uso de medios removibles de la Entidad para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionado con el cumplimiento de las funciones u obligaciones contractuales.
- Los funcionarios y contratistas deben hacer uso de los medios de almacenamiento en nube y servidores de datos disponibles por el Entidad, para guardar únicamente la información generada como parte de sus actividades laborales.
- Los funcionarios o contratistas que requieran los medios removibles habilitados de forma permanente deben tener una autorización firmada por su jefe inmediato o supervisor.
- En caso de olvido de la contraseña asignada para el cifrado del medio removible y pérdida de la clave de recuperación provista, el usuario responsable de uso del medio removible asumirá las consecuencias producto de la pérdida de la información institucional que se encuentre almacenada en dicho medio.
- Los medios removibles no son alternativa de respaldo de información, son de uso temporal; siendo responsabilidad de los usuarios mantener copias de la información en los repositorios institucionales.

Punto de control: *Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización*

7.3.2 Disposición de los medios

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI ejecutará el debido proceso para la eliminación de datos en los medios de almacenamiento que vayan a ser reemplazados, efectuando un proceso de borrado seguro y posteriormente la eliminación o destrucción en forma adecuada, con el fin de controlar que la información contenida en estos medios no se pueda recuperar.

El Grupo de TI establecerá los lineamientos necesarios para dar de baja el software y los equipos de cómputo que presenten obsolescencia o daño irreparable.

Las copias de seguridad de información se deben guardar en una ubicación alterna a la localización de los datos o aplicaciones para aumentar la seguridad ante posibles impactos de desastres ambientales, accidentes, incendios, etc.

Se debe realizar pruebas a las copias de datos para validar la integridad de la información.

Punto de control: *Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.*

7.3.3 Transferencia de medios físicos

Responsable del control: Grupo de Gestión documental

Los medios que contienen información (física o digital) se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte, siguiendo los lineamientos establecidos por el Grupo de Gestión Documental que controlan el servicio de envíos y entregas internamente entre la sede Yerbabuena y Casa Caro y Cuervo.

Cuando se requiera transferir un medio de almacenamiento de información del ICC a otras entidades se debe establecer un acuerdo de confidencialidad y seguridad, entre las partes. Cuando se requiera transferir un medio de almacenamiento se debe tener en cuenta el registro de contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y el recibido. El transporte para los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información del ICC.

Punto de control: *Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.*

8 CONTROL DE ACCESO

8.1 Requisitos del negocio para control de acceso.

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

8.1.1 Política de control de acceso

Responsable del control: Grupo de Tecnologías de la Información (TI), Grupo de Recursos Físicos, Líderes de procesos y Supervisores de contrato

El Grupo de TI debe implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, carpetas compartidas, bases de datos y servicios tecnológicos.

En cuanto a la definición de procedimientos para mantener el acceso controlado físico a las instalaciones de la Entidad el Grupo de Recursos Físicos es el responsable, estos procedimientos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

De igual manera, desarrollar una política de control de acceso lógico y físico que contenga:

- los requisitos de seguridad para las aplicaciones de la entidad;
- las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información;
- la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes;
- la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios;
- la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles;
- la separación de los roles de control de acceso (solicitud de acceso, autorización de acceso, administración del acceso);
- los requisitos para la autorización formal de las solicitudes de acceso;
- los requisitos para la revisión periódica de los derechos de acceso;
- el retiro de los derechos de acceso;
- el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente;
- los roles de acceso privilegiado.

Los Líderes de procesos y supervisores son los únicos autorizados para solicitar los accesos lógicos y físicos, la creación de las cuentas de usuario y la asignación de permisos a los diferentes servicios tecnológicos y sistemas de información para los integrantes de su grupo de trabajo, considerando el mínimo de privilegios necesarios para que contratistas y/o funcionarios puedan desempeñar sus obligaciones y/o funciones; de igual manera, deben solicitar la eliminación al Grupo de TI de dichos accesos cuando algún integrante de su grupo ya no lo requiera.

Punto de control: *Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información*

8.1.2 Acceso a redes y a servicios en red.

Responsable del control: Grupo de Tecnologías de la Información (TI)

La conexión remota a la red de área local del ICC debe realizarse a través de una conexión VPN segura suministrada por el Grupo de TI. El servicio de acceso remoto por VPN permite a los usuarios el acceso a los activos de información disponibles solo desde la red interna desde un sitio remoto a través de internet.

El Grupo de TI realizará un análisis de los equipos personales que requieran conexión VPN, con el fin de verificar que estos equipos cuentan con las condiciones necesarias de seguridad para conectarse a la red de área local de la entidad a través de operadores externos.

El ICC debe contar con un dispositivo de seguridad perimetral para la conexión a internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros. Los puntos de conexión de la red de datos del ICC son para uso exclusivo de los equipos propiedad de la entidad, la instalación, activación y gestión de los puntos de red es responsabilidad del Grupo de TI.

Punto de control: *Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.*

8.2 Gestión de acceso de usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

8.2.1 Registro y cancelación del registro de usuarios

Responsable del control: Grupo de Tecnologías de la Información (TI).

Los Líderes de procesos o supervisores de contrato deberán solicitar al Grupo de TI a través de la mesa de ayuda, la creación de las cuentas de usuario, la asignación de permisos a los diferentes servicios tecnológicos y sistemas de información para los integrantes de su grupo de trabajo y la cancelación del registro de usuarios. Se debe controlar el acceso a los sistemas y servicios de información estableciendo un procedimiento de novedades de los usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información.

Se debe mantener evidencia de cambios realizados a los identificadores de usuario (ID), perfiles y estado de las cuentas de usuario. Se debe retirar o bloquear inmediatamente los derechos de acceso a los funcionarios y/o contratistas que cambian de funciones o responsabilidades, de aquellos a los cuales se revoca la autorización de acceso, vinculación contractual o sufren pérdida o robo de credenciales de acceso.

Se debe definir y aplicar reglas para deshabilitar las cuentas de usuarios de red que no han cambiado la contraseña durante 90 días; igualmente, se debe definir qué cuentas deben quedar bloqueadas porque no fueron reactivadas y eliminar aquellas cuentas que no presentan ninguna actividad desde su creación.

Punto de control: *Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso*

8.2.2 Suministro de acceso de usuarios

Responsable del control: Grupo de Tecnologías de la Información (TI).

Los funcionarios y contratistas solo tendrán acceso a los datos y recursos autorizados por el ICC, y serán responsables disciplinaria y legalmente por la divulgación no autorizada de información que se clasifique como reservada o clasificada. Se debe definir y documentar un procedimiento para la creación, modificación, y cancelación de usuarios y privilegios. Ningún colaborador puede realizar solicitudes de acceso para sí mismo, salvo sea un cargo directivo.

No debe existir cuentas genéricas para el acceso o gestión sobre los sistemas tecnológicos de la entidad. Los administradores de recursos informáticos deben asignar un usuario único y exclusivo a las funcionarios y contratistas que ejercen funciones públicas cuyos privilegios de acceso a los recursos informáticos estarán determinados por el tiempo de vinculación con el organismo y así de esta manera poder mantener el control de acceso a dichos recursos con base a los diferentes formatos aprobados por la administración central.

Los accesos con privilegios especiales deben contar con la aprobación de la Coordinación del Grupo de TI y deben de estar debidamente justificados, los responsables del manejo de usuarios privilegiados deben aceptar su responsabilidad frente al uso del usuario asignado. Los usuarios de la red de datos del ICC contarán con las debidas credenciales de acceso a los equipos, sistemas y/o aplicativos informáticos necesarios para el correcto desempeño de sus actividades.

Punto de control: *Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.*

8.2.3 Gestión de derechos de acceso privilegiado

Responsable del control: Grupo de Tecnologías de la Información (TI).

La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar; el uso de usuarios tales como: “root”, “admin” “administrador” y “system”, entre otros, debe ser controlado por el Grupo de TI dejando registro de la trazabilidad de uso de estos accesos.

Para los usuarios con derechos de uso privilegiado utilizados para la administración de infraestructura, aplicaciones y sistemas de información, la coordinación del Grupo de TI debe controlarlos mediante un proceso formal de autorización, asignando credenciales diferentes para las actividades regulares, segmentados por cada sistema o proceso, donde se definan los requisitos para la expiración de estos, con especial atención a las cuentas configuradas para usuarios externos con propósitos específicos y por tiempo limitado.
Los cambios a las cuentas privilegiadas se deben controlar, registrar, conservar y realizar revisiones periódicas. Los privilegios de administración de cualquier equipo de cómputo (servidor, estación de trabajo, desktop, portátil, o equipo activo de red) deben ser asignados exclusivamente al CTO de cada organismo.

El Grupo de TI será la encargada de aprobar la asignación de acceso privilegiado a usuarios a los sistemas de información y aplicativos, teniendo en cuenta los siguientes lineamientos:

- Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Asignar los privilegios a funcionarios y contratistas sobre el principio del mínimo privilegio, es decir, el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

Punto de control: *Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.*

8.2.4 Gestión de información de autenticación secreta de usuarios

Responsable del control: Grupo de Tecnologías de la Información (TI).

El Grupo de TI suministrará a los usuarios las credenciales (usuario/contraseña) respectivas para el acceso a la información, los servicios de red y sistemas de información a los que hayan sido autorizados. La confirmación de la gestión del requerimiento y el envío de los datos de autenticación deben ser enviados usando un canal seguro. Esta entrega debe estar controlada por un proceso de administración formal que permita informar a los usuarios sobre el compromiso de cumplir con los lineamientos de seguridad establecidos para el buen uso de los datos de acceso (usuarios y contraseña) otorgados.

Punto de control: *La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.*

8.2.5 Revisión de los derechos de acceso de usuarios

Responsable del control: Grupo de Tecnologías de la Información (TI).

Se deben efectuar revisiones periódicas a los Identificadores de Usuarios (ID) identificando y cancelando cuentas redundantes o inactivas y comprobando la integridad de accesos modificados por las novedades de usuario reportadas. Las actividades de revisión periódica del estado, cambios de roles y bloqueo de usuarios serán responsabilidad del Grupo de TI.

Punto de control: *Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares*

8.2.6 Retiro o ajuste de los derechos de acceso

Responsable del control: Grupo de Tecnologías de la Información (TI), Líderes de procesos y Supervisores de contrato

Los derechos de acceso de un usuario se deben revisar y reasignar, ya sea por cambio de cargo, traslado de dependencia o grupo; o finalización del contrato. Se deberá informar al Grupo de TI, el período de vacaciones o si el funcionario se ausentará por más de 15 días, para que le sea bloqueado su usuario por el período de tiempo establecido. Para el caso de los contratistas, se debe retirar los derechos de acceso si el contratista solicita una cesión o suspensión del contrato; y si o si a la finalización de este.

Punto de control: *Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.*

Actualmente el ICC solicita ajuste de contraseña a los 30 días, se cuenta con los lineamientos de la *COM-G-6 Guía para la creación de cuentas de red y correo electrónico* y del procedimiento *COM-P-10 Gestión de accesos tecnológicos,* identificando como punto de control el diligenciamiento y la gestión del formato *COM-F-21 Creación de cuentas de usuario para los servicios tecnológicos del ICC.*

8.3 Responsabilidades de los usuarios.

Objetivo: Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.

8.3.1 Uso de información de autenticación secreta

Responsable del control: Todos

Todos los funcionarios y terceros deben mantener la confidencialidad de la información y cumplir con las políticas de seguridad de la información para el uso de información secreta para la autenticación (cuentas de acceso), asegurándose que no sea divulgada o compartida con otros colaboradores o personal externo.

Además, se debe dar cumplimiento a lo siguiente:

- Evitar escribir la información secreta (usuarios, contraseñas, etc.) en papeles o archivos electrónicos o almacenarla en los navegadores de internet.
- Todo usuario autorizado debe cambiar la contraseña cada vez que exista o haya algún indicio de una posible vulnerabilidad del sistema.
- Las claves o contraseñas de acceso a los sistemas de información deben poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.

- Evitar usar las mismas contraseñas para fines personales y laborales.
- Asegurarse de que los usuarios asignados y contraseñas establecidas no serán compartidos, con el fin de mantener la privacidad de la información
- El Grupo de TI debe implementar mecanismos para que los usuarios cambien su contraseña de acceso al usarla por primera vez en los sistemas de información o servicios a los que se les permita el acceso

Punto de control: *Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.*

8.4 Control de acceso a sistemas y aplicaciones.

Objetivo: Prevenir el uso no autorizado de sistemas y aplicaciones

8.4.1 Restricción de acceso a la información

Responsable del control: Todos y Grupo de Tecnologías de la Información (TI).

Cada usuario es responsable de la cuenta de usuario y clave que le ha sido asignada necesaria para acceder a la información, servicios tecnológicos y/o sistemas de información de la Entidad. Los usuarios y claves son personales e intransferibles y no deben prestarse, divulgarse, ni permitir que otros utilicen sus cuentas de usuario, ni utilizar las cuentas de usuario de otros usuarios. Los usuarios deben terminar las sesiones activas cuando finalice su actividad o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

El Grupo de TI debe restringir y controlar el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones, siguiendo las siguientes directrices mínimas:

- Usar procedimientos documentados de identificación, autenticación y autorización de los programas utilitarios.
- Limitar el uso de programas utilitarios al número mínimo de usuarios confiables y autorizados, teniendo en cuenta el tiempo de uso previsto.
- Retirar o inhabilitar todos los programas innecesarios.

El Grupo de TI debe controlar el acceso a códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de prueba y resultados), para evitar la introducción de funcionalidades no autorizadas o cambios involuntarios, así mismo, para mantener la confidencialidad de la propiedad intelectual.

- Las librerías de programas fuente, no deberían estar contenidas en los ambientes de producción.
- Se debe documentar y hacer cumplir los procedimientos establecidos para la gestión de códigos fuente y las librerías de los programas.

- Mantener un registro de auditoría de todos los accesos a la librería de fuentes de programas.
- Se debe llevar un control de cambios adecuado para el mantenimiento y copia de las librerías de fuentes de programas.

Punto de control: *El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.*

8.4.2 Procedimiento de ingreso seguro

Responsable del control: Grupo de Tecnologías de la Información (TI)

Los accesos a la información o sistemas de información no deben otorgarse por los administradores de base de datos y de aplicaciones del servicio hasta que se hayan completado los procedimientos de autorización. La selección de los mecanismos de control de acceso a las aplicaciones se define de acuerdo con la criticidad y/o sensibilidad de la información (procesada, almacenada, usada) utilizada por el proceso.

Las aplicaciones de la entidad deben contar con mecanismos para el manejo de contraseñas, los cuales sean interactivos y cumplan con los parámetros de seguridad definidos. Cada aplicación desarrollada en el ICC y las adquiridas a través de un tercero deben contar con un procedimiento de ingreso seguro, acorde a la política de control de acceso a la información.

Punto de control: *Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.*

8.4.3 Sistema de gestión de contraseñas

Responsable del control: Grupo de Tecnologías de la Información (TI)

Es responsabilidad de funcionarios y terceros utilizar contraseñas fuertes para realizar la autenticación y acceso a la información, las aplicaciones y/o los sistemas de información de la Entidad. El cambio de contraseña para inicio de sesión en cualquier sistema de información de la entidad solo podrá ser solicitado por el titular de la cuenta.

La contraseña de la cuenta de usuario asignada por primera vez debe ser inmediatamente cambiada en el primer inicio de sesión, cumpliendo con los siguientes requisitos:

- Las contraseñas deben estar compuestas al menos por diez caracteres alfanuméricos.
- Contener caracteres de las tres siguientes clases:
  - ✓ Caracteres en mayúsculas y minúsculas (es decir, Aa-Zz)
  - ✓ Base de 10 dígitos (es decir, 0-9)
  - ✓ Puntuación y otros caracteres (es decir, @#$%^&*() _+|~-= \ `{}[]:";'<>?,./).

- ✓ No pueden tener caracteres consecutivos (ABCD, 12345)

Las contraseñas se deben cambiar obligatoriamente cada treinta días, o cuando lo establezca el sistema de información. Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro, utilizando herramientas que permitan la protección de dichas claves. A esta herramienta solo debe tener acceso el coordinador del Grupo de TI y el apoyo designado.

Las cuentas de usuario y contraseña de administradores son de uso personal e intransferible. El personal del Grupo de TI deben emplear obligatoriamente contraseñas con un alto nivel de complejidad de acuerdo con el rol asignado.

El Grupo de TI debe implementar mecanismos que permitan a los sistemas de administración de contraseñas:

- El uso individual de contraseñas.
- Permitir al usuario el cambio de su contraseña.
- Exigir contraseñas de seguridad.
- Para cuentas administrativas incluir mínimo 12 caracteres y doble factor de autenticación en los sistemas que lo permitan.
- Exigir el cambio de contraseña cuando se ingresa por primera vez.
- Impedir el reúso de contraseña (a las 4 últimas).
- Implementar mecanismos de captcha en los sistemas o aplicaciones que lo permita.

Punto de control: *Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.*

8.4.4 Uso de programas utilitarios privilegiados

Responsable del control: Grupo de Tecnologías de la Información (TI)

El uso de herramientas o utilitarios propios de los sistemas operativos debe ser limitado a personal autorizado y su uso está restringido a casos específicos. Asimismo, debe disponerse de la trazabilidad de las operaciones realizadas en los casos que son autorizados.

Directrices para el uso de programas utilitarios:

- Utilizar procedimientos de identificación, autenticación y autorización incluyendo el uso de los programas utilitarios.
- Separar los programas utilitarios del software de aplicaciones.
- Limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados (usuarios privilegiados).
- Limitar la disponibilidad de los programas utilitarios.

- Registrar el uso de los programas utilitarios.
- Definir y documentar los niveles de autorización para los programas utilitarios.
- Retirar o deshabilitar todos los programas utilitarios innecesarios.
- No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.

Punto de control: *Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.*

8.4.5 Control de acceso a códigos fuente de programas

Responsable del control: Grupo de Tecnologías de la Información (TI)

Las librerías de fuentes de programas no se deben mantener en los sistemas operativos. El acceso al código fuente de los programas de la entidad debe estar limitado solamente a los desarrolladores y personal de soporte autorizado.

El Grupo de TI debe establecer un procedimiento y controles de acceso a los ambientes de desarrollo y producción; así mismo, debe limitar y controlar el acceso a datos o información que se encuentre en los ambientes de producción. La actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores solo se deben hacer una vez que se haya recibido autorización apropiada.

Los listados de programas y códigos fuente se deben mantener en un entorno seguro. Se debe conservar un registro de auditoría de todos los accesos a las librerías y códigos fuentes de programas. Se debe mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios. Se debe realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la Entidad.

Punto de control: *Se debe restringir el acceso a los códigos fuente de los programas.*

9 CRIPTOGRAFIA

10.1 Controles criptográficos

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

9.1.1 Política sobre el uso de controles criptográficos

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe definir e implementar lineamientos para la aplicación de controles criptográficos para la protección de la información y contar con un método seguro de gestión de llaves criptográficas. El Grupo de TI debe implementar técnicas de cifrado para la transferencia de información etiquetada como clasificada y/o reservada fuera del ICC con el propósito de proteger su confidencialidad e integridad.

Los desarrolladores internos y externos deben asegurarse de que los controles criptográficos, de los sistemas de información desarrollados para el ICC, cumplen con los lineamientos establecidos por el Grupo de TI. Se debe garantizar que el uso de controles criptográficos no entorpezca aquellos controles de seguridad basados en inspección de contenido, tales como filtrado web, antimalware, antispyware, entre otros.

Se debe desarrollar una política de controles criptográficos que incluya:

- Establecer el enfoque de la dirección con relación al uso de controles criptográficos en toda la entidad, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio.
- Realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido.
- Utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación.
- Gestionar las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas.
- Establecer roles y responsabilidades en cuanto a:
    - La implementación de la política.
    - La gestión de llaves, incluida la generación de llaves.
- Establecer las normas que se van a adoptar para la implementación efectiva en toda la entidad (procesos del negocio).
- Definir el impacto de usar información encriptada en los controles que dependen de la inspección del contenido.

Punto de control: *Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.*

9.1.2 Gestión de llaves

Responsable del control: Grupo de Tecnologías de la Información (TI).

El tamaño de las llaves criptográficas privadas y públicas debe proveer el nivel de seguridad requerido en la entidad y estar alineadas con estándares internacionales y buenas prácticas.

Se deben implementar mecanismos para la recuperación de información cifrada en caso de pérdida, compromiso o daño de las llaves y reemplazo de las llaves de cifrado. Se deben definir mecanismos que permitan gestionar las llaves criptográficas en todo su ciclo de vida (emisión, uso, expiración, eliminación, revocación, auditoria y copias de respaldo).

Punto de control: *Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida***.**

10 SEGURIDAD FÍSICA Y DEL ENTORNO

10.1 Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la entidad.

10.1.1 Perímetro de seguridad física

Responsable del control: Grupo de Recursos Físicos

El Grupo de Recursos Físicos debe establecer y comunicar los protocolos de seguridad física para el acceso a las instalaciones del ICC. El Grupo de Recursos Físicos debe definir perímetros de seguridad y usarlos para proteger áreas que contengan activos de información críticos (ejemplo: museos, biblioteca, Imprenta Patriótica, archivo central) e instalaciones de manejo de información (centro de datos), teniendo en cuenta lo siguiente:

- El techo, las paredes y los pisos deber ser de construcción sólida.
- Todas las puertas externas deberían tener mecanismos de control que eviten el acceso no autorizado.
- Las puertas y ventanas se deben mantener cerradas con llave cuando no hay supervisión.
- Para las ventanas se debe considerar protección contra acceso.
- Se debe contar con un área de recepción con vigilancia para controlar el acceso físico a las instalaciones, restringiendo el acceso únicamente para el personal autorizado.
- Se deben instalar sistemas para la detección de intrusos.
- Deben contar con mecanismos que permitan cumplir con los requerimientos ambientales de temperatura y humedad.

El Grupo de Recursos Físicos debe establecer un protocolo de seguridad para apoyar las actividades museográficas en las funciones de exhibición, difusión, custodia, conservación y administración de los bienes patrimoniales y valores que se encuentra en los depósitos de museos. Se debe contar con un registro de acceso a las áreas seguras con fecha, hora de entrada, hora de salida, nombre y firma de la persona autorizada.

Siempre que sea posible, las áreas restringidas deben evitar cualquier indicación sobre su propósito, omitiendo señales que identifiquen las actividades de procesamiento de información o la documentación que resguardan. No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la entidad, a menos que esté autorizado por escrito por el jefe de la dependencia restringida.

En las áreas que contengan activos de información críticos se debe indicar la prohibición de acceso no autorizado, no está permitido fumar, comer o beber dentro o cerca de estos.

Las áreas de despacho y carga de materiales se deben administrar de forma que el personal de despacho no tenga acceso a áreas de procesamiento de información, los materiales que ingresen se deben inspeccionar, para verificar la presencia de materiales peligrosos, todos los materiales que ingresen deben ser registrados de acuerdo con los procedimientos establecidos del Grupo de Recursos Físicos. Asimismo, todos los funcionarios deben portar, de forma visible, el carné que los identifica como miembros de la Entidad, y en el caso de los contratistas, llevar consigo el documento digital correspondiente, estos elementos deben utilizarse en todo momento mientras se permanezca dentro de las instalaciones.

Todos los visitantes que ingresen al ICC deben ser registrados y, en lo posible, portar una tarjeta que los identifique como visitantes en un lugar visible. Toda persona que tenga acceso a las instalaciones del ICC deberá registrar al momento de su entrada, el equipo de cómputo, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción el cual podrá retirar el mismo día firmando la salida del equipo.

Punto de control: *Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.*

10.1.2 Controles de acceso físicos

Responsable del control: Grupo de Recursos Físicos

Se debe mantener un registro de la fecha y hora de entrada y salida de los visitantes. Todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia. Se debe otorgar identificación a cada visitante. Todos los empleados, contratistas y partes externas deben portar algún tipo de identificación visible, y se deben notificar de inmediato al personal de seguridad si se encuentran visitantes no acompañados, y sin la identificación visible.
El personal de servicio de soporte de terceros (proveedores) se le debería otorgar acceso restringido a áreas seguras o a instalaciones de procesamiento de información confidencial solo cuando se requiera;

este acceso se debe autorizar y se le debe hacer seguimiento. Los derechos de acceso físico a áreas seguras se deben revisar y actualizar regularmente, y revocar cuando sea necesario.

10.1.2.1 Política de los centros de procesamiento de datos.

Responsable del control: Grupo de Tecnologías de la Información (TI).

El acceso a los centros de datos es permitido solo a personal autorizado. El Grupo de TI debe garantizar que las puertas de acceso estén protegidas por un sistema de control de acceso o por un sistema que permita el ingreso solo a personal que pertenece al personal autorizado.

Los centros de datos deben ser limpiados al menos una vez por semana para disminuir al máximo los niveles de polvo y de contaminación. Esta actividad debe ser supervisada por un funcionario del Grupo de TI, quien debe instruir al personal de limpieza respecto a los cuidados y precauciones mínimos a seguir durante esta actividad.

Los centros de datos deberán contar con un equipo de aire acondicionado que mantenga una temperatura no mayor a 21 grados centígrados, y con unidades de potencia ininterrumpida UPS, que proporcionen respaldo a los mismos, y garantizar el servicio de energía eléctrica durante una falla temporal del fluido eléctrico de la red pública y permitir el intercambio automático del sistema de energía redundante.

Los centros de datos deberán contar con un entorno físico que se rija a los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos en los equipos de telecomunicaciones y servidores. Deberán contar con un extintor especial para equipos de cómputo y con pisos elaborados en materiales no inflamables.

Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual para determinar la efectividad del sistema. El mantenimiento de los equipos de potencia ininterrumpida UPS estará a cargo del Grupo de TI y deberá incluirse en un su Plan Anual de Adquisiciones (PAA) para adelantar procesos de contratación de suministro de repuestos y mantenimientos preventivos y correctivos.

Los cables de potencia deben estar separados de los de comunicaciones, según las normas técnicas y los equipos de los centros de datos que lo requieran, y han de monitorearse para poder detectar las fallas que se puedan presentar.

Punto de control: *Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.*

10.1.3 Seguridad de oficinas, recintos e instalaciones

Responsable del control: Grupo de Recursos Físicos.

Por ningún motivo el visitante debe estar solo en áreas catalogadas como sensibles, para así garantizar la seguridad física del departamento. Solicitar a los visitantes el NO ingreso de teléfonos inteligentes, equipos fotográficos, de video, audio u otro equipo que registre información de los Centros de Procesamiento de Datos, protegiendo la confidencialidad de este. La excepción se permite en el caso de que el visitante forme parte de un proveedor de tecnología atendiendo un incidente; el cual tiene permitido el acceso con todos los recursos requeridos para resolver el incidente.

Se debe gestionar la implementación de la vigilancia de los Centros de Procesamiento de Datos por medio de circuito cerrado de televisión para verificar y registrar en medio digital los acontecimientos rutinarios y de excepción. Se debe controlar el ingreso y salida de recursos de TI de los Centros de Procesamiento de Datos registrando la entrada y la salida de los elementos, registrando la trazabilidad para evitar pérdidas de elementos TI.

Se debe entregar copias de las llaves de las cerraduras de los centros de cableado a los responsables de la vigilancia y solo podrá acceder a los Centros de Procesamiento de Datos el personal del Grupo de TI y aquellas personas que sean autorizadas a través de correo electrónico u oficio para garantizar soporte de alto nivel en cualquier horario.

Se deben mantener los gabinetes que hospedan los elementos de TI siempre cerrados con llaves para evitar acceso o daño a elementos de TI ahí hospedados. De igual manera los gabinetes y archivo donde se encuentre la información física debe estar bajo llave.

Punto de control: *Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones*

10.1.4 Protección contra amenazas externas y ambientales

Responsable del control: Grupo de Recursos Físicos.

Se debe gestionar la implementación de los controles para minimizar el impacto ante desastres naturales con elementos de control de incendios, inundación y alarmas para minimizar el efecto durante la materialización de riesgos como incendios e inundaciones. Se debe monitorear constantemente las condiciones de temperatura y humedad, registrando y analizando eventos y excepciones para evitar que se afecten los equipos dentro del centro de cómputo por cambios de temperatura.

Se debe garantizar razonablemente la seguridad física ante siniestros verificando que las paredes, pisos y techos NO contengan material inflamable para evitar incendios. Se debe evitar custodiar objetos que obstaculicen el paso de funcionarios en caso de emergencia dentro del Centro de Procesamiento de

Datos. Procurar el aseo y limpieza adecuado del Centro de Procesamiento de Datos, planificando jornadas de limpieza y organización para evitar el daño de recursos de TI por causa de exceso de polvo y suciedad en el área.

Punto de control: *Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.*

10.1.5 Trabajo en áreas seguras

Responsable del control: Grupo de Tecnologías de la Información (TI)

Los visitantes a los Centros de Procesamiento de Datos del ICC deben solicitar autorización previa para ingresar; el personal visitante debe ser acompañado durante todo el tiempo de su visita, por un funcionario del Grupo de TI. Todas las visitas realizadas al Centro de Procesamiento de Datos deberán ser registradas en el libro de bitácoras ingresando mínimo los siguientes datos: Nombre, apellido, fecha de ingreso, hora de entrada, hora de salida, funcionario del Grupo de TI que lo acompaña, asunto del ingreso y firma del personal que ingresa y del funcionario que acompaña la visita.

Evitar el consumo de bebidas y alimentos dentro del Centro de Procesamiento de Datos, para evitar daños en los equipos de TI alojados en ellos.

El trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas. No se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.

Punto de control: *Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.*

10.1.6 Áreas de despacho y carga

Responsable del control: Grupo de Recursos Físicos

El acceso al área de despacho y de carga se debe restringir al personal identificado y autorizado. Las áreas de cargue y descargue deberán estar señalizadas. Desde el área de despacho y carga, se puedan cargar y descargar elementos sin que el personal de despacho tenga acceso a otras partes del ICC.

Los puntos de acceso como el área de entrega y las zonas de carga deberán ser controladas y monitoreadas mediante CCTV (Circuito Cerrado de Televisión). El material que ingresa se deberá inspeccionar y examinar para determinar la presencia de materiales peligrosos tales como: presencia de explosivos y químicos inflamables. De igual manera la inspección debe determinarse como evidencia de

manipulación en caso de que exista dicho incidente. La manipulación debe reportarse de inmediato al personal de seguridad. El material que ingresa debe registrarse en las bitácoras de ingreso de elementos.

Punto de control: *Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado***.**

10.2 Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones del ICC.

10.2.1 Ubicación y protección de los equipos

Responsable del control: Todos.

Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, adoptando controles para minimizar el riesgo de amenazas físicas y ambientales como; robo, incendio, explosivos, humo, agua, polvo, vibración, interferencia en el suministro eléctrico o de comunicaciones, entre otros.

10.2.1.1 Política de uso de estaciones cliente.

Responsable del control: Todos y Grupo de Tecnologías de la Información.

Los funcionarios y contratistas de soporte técnico del Grupo de TI tienen como función exclusiva el mantenimiento y la instalación de software en los computadores, que son propiedad del ICC; ellos son los únicos usuarios con credenciales de acceso para realizar este tipo de actividades. Los usuarios podrán trabajar la información institucional en modo borrador sobre los discos locales del computador asignado, sin embargo, deberán realizar la copia de sus archivos en la nube institucional.

El préstamo de computadores portátiles se debe tramitar a través de la mesa de ayuda con anticipación y se proveerá según disponibilidad. Los equipos de cómputo que ingresan temporalmente a las diferentes instalaciones del ICC, que sean de propiedad de contratistas o terceros, deben ser registrados en las porterías de la entidad para poder realizar su retiro sin requerir autorización del Grupo de TI. El ICC no se hará responsable, en caso de pérdida o daño, de algún equipo informático de uso personal que haya sido ingresado a sus diferentes instalaciones. Los funcionarios del Grupo de TI no prestarán servicio de soporte técnico (revisión, mantenimiento y/o reparación de hardware) a equipos que no sean propiedad del ICC.

10.2.1.2 Política de uso de servicios de impresión.

Responsable del control: Todos y Grupo de Tecnologías de la Información (TI)

Para el uso de los servicios de impresión, los usuarios deben iniciar sesión con una cuenta válida en los equipos de cómputo asignados por el Grupo de TI del ICC. Para la impresión de documentos, servicios de escaneo o servicios de fotocopia, los usuarios deben contar con un código válido.

La impresión de documentos a color está permitida solo para los usuarios que adelantan tareas de diseño y creación de material gráfico. Los usuarios que por razones justificadas en el desarrollo de sus actividades institucionales requieran la habilitación de este servicio, deben solicitar al jefe o supervisor que formalice la activación de este servicio a través de la mesa de ayuda.

Las impresoras son para uso exclusivamente institucional. No se permite la impresión de documentos personales o trabajos ajenos a las funciones institucionales, por lo que es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión, escáner y fotocopiado, para que no se afecte su correcto funcionamiento.

Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta debe reportar a través de la mesa de ayuda.

10.2.1.3 Política dentro del área de procesamiento de Información.

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Centro de Procesamiento de Datos está protegido de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado por el Grupo de TI.

Se debe proteger contra descargas eléctricas atmosféricas (polo a tierra) y se deben colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas. De igual manera, se deben proteger los equipos para procesamiento de información para minimizar el riesgo debido a emanaciones electromagnéticas.

10.2.2 Servicios de suministro

Responsable del control: Grupo de Tecnologías de la Información (TI) y Grupo de Recursos Físicos.

Se debe evaluar regularmente la capacidad para el suministro de energía principal y de soporte. Se deben evaluar regularmente las condiciones ambientales y eléctricas de las áreas consideradas como seguras Se debe hacer uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deberán conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deberán

conectarse a la red eléctrica no regulada. Se deberán implementar mecanismos para regular el flujo de energía e interrupciones causadas por fallas en el soporte de los servicios públicos que puedan afectar los equipos de cómputo y procesamiento.

Punto de control: *Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.*

10.2.3 Seguridad del cableado.

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe garantizar la protección del cableado de la red contra interferencias, intercepción no autorizada y daños, implementando controles como el uso de ductos o evitando recorridos a través de áreas públicas. Para ello, se deben desarrollar las siguientes medidas:

- Utilizar canaletas de dos divisiones u otras soluciones disponibles en el mercado.
- Validar que las conexiones dentro de los centros de datos estén libres de contactos defectuosos o instalaciones eléctricas en mal estado.
- Etiquetar claramente los cables para facilitar la identificación de los elementos conectados y prevenir desconexiones accidentales.
- Deben existir planos que describan las conexiones del cableado.
- El acceso a los centros de cableado (Racks), debe estar protegido.
- El cableado estructurado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño
- Se debe cumplir con los requisitos técnicos vigentes dictados por las normas de seguridad de cableado.
- Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
- Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

Punto de control: *El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.*

10.2.4 Mantenimiento de los equipos.

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI es el responsable de liderar y gestionar el cumplimiento del plan de mantenimiento de todos los activos de la Entidad. Las actividades de mantenimiento de los servidores, elementos de comunicaciones o cualquiera que pueda ocasionar una suspensión en los servicios tecnológicos, deben ser programadas y realizadas por el personal autorizado por la coordinación del Grupo de TI.

Para los casos en que se requieran realizar actividades de mantenimiento de los sistemas eléctricos debe notificarse al Grupo de TI con antelación para la programación de ventanas de mantenimiento y garantizar la continuidad de los servicios tecnológicos.

El Grupo de TI debe mantener contratos de soporte y mantenimiento de los equipos críticos. Los equipos que requieran salir de las instalaciones del ICC por motivos de garantía o mantenimiento deben estar debidamente autorizados por el Grupo de TI y se debe garantizar que en dichos elementos no se encuentra información clasificada o reservada.

Cuando un dispositivo vaya a ser reasignado o dado de baja debe contar con aprobación del Grupo de TI, así mismo debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando procedimientos de borrado seguro.

Punto de control: *Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas*

10.2.5 Ingreso y retiro de los activos.

Responsable del control: Grupo de Recursos Físicos

Todo elemento que ingrese al ICC debe ser inspeccionado por el equipo de vigilancia con el objetivo de identificar material peligroso y a su vez debe ser revisado por el Grupo de Recursos Físicos con el fin de revisar que este coincida con su respectiva autorización de ingreso.

El Grupo de Recursos Físicos debe mantener el inventario de activos actualizado por lo que se le debe notificar todo elemento que ingrese o se retire del ICC siguiendo los procedimientos establecidos.
El traslado entre sedes y oficinas del ICC y/o retiro de todo activo de información está a cargo del Grupo de Recursos Físicos para el control de inventarios.

Punto de control: *Los equipos, información o software no se deben retirar de su sitio sin autorización previa.*

10.2.6 Seguridad de equipos y activos fuera de las instalaciones

Responsable del control: Grupo de Recursos Físicos y Grupo de Tecnologías de la Información (TI)

El encargado del retiro o traslado de equipos de cómputo propiedad del ICC, debe garantizar la seguridad durante este, manteniendo las buenas prácticas de seguridad para evitar riesgos informáticos que afecten la información o en el equipo.

En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo. Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

En caso de pérdida o robo de un equipo de la entidad, se debe poner la denuncia ante la autoridad competente e informar inmediatamente al jefe inmediato o supervisor de contrato al igual que al organismo encargado de los equipos para el trámite interno correspondiente. Se deben tener en cuenta los riesgos que conlleva el uso de equipos de la entidad fuera de las instalaciones del ICC. Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado de los equipos. Se mantendrá una adecuada cobertura mediante un seguro, para proteger los equipos que se encuentran fuera del ámbito de la entidad, cuando sea conveniente.

Deberá informarse al jefe inmediato sobre la salida de los elementos de cómputo de las instalaciones. En caso de ser necesario, se deberá encriptar el disco a través de la herramienta de bitlocker dispuesta por el sistema operativo una vez se ha borrado el disco, para evitar divulgar información.

Punto de control: *Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la entidad, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.*

10.2.7 Disposición segura o reutilización de equipos

Responsable del control: Grupo de Tecnologías de la Información (TI)

Todos los equipos de cómputo que vayan a ser reasignados o dados de baja, se les deberá realizar el borrado seguro de la información, con el fin de evitar recuperación no autorizada de la misma. En caso de ser necesario, se deberá encriptar el disco a través de la herramienta de BitLocker dispuesta por el sistema operativo una vez se ha borrado el disco, para evitar divulgar información.

Punto de control: *Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.*

10.2.8 Equipos de usuario desatendido.

Responsable del control: Todos

Es responsabilidad de funcionarios y terceros bloquear la sesión de su estación en los momentos en que no estén utilizando el equipo a través de las teclas Windows y L al mismo tiempo; o cuando, por cualquier motivo, deban dejar su puesto de trabajo, la cual se podrá desbloquear solo con la introducción de la

contraseña del usuario, al finalizar sus actividades deben cerrar todas las aplicaciones y apagar el equipo de cómputo. Se deben apagar los equipos de cómputo que utilizan para sus labores diarias cada que termine su jornada laboral para evitar que estos equipos sean utilizados para otro fin.

El Grupo de TI, debe implementar mecanismos para cierres de sesión después de 10 minutos de inactividad, y solo se podrán desbloquear con el usuario y contraseña asignada. Los usuarios finales, son responsables y asumen las consecuencias por la pérdida de información que esté bajo su custodia si no bloquean su sesión cuando no estén en su puesto de trabajo.

Se prohíbe el almacenamiento de información personal en los computadores de la entidad. Se debe utilizar el repositorio de OneDrive para el almacenamiento de la información producida en el ejercicio de las funciones u obligaciones contractuales.

Punto de control: *Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.*

10.2.9 Política de escritorio y pantalla limpia.

Responsable del control: Todos

Los usuarios del ICC deben conservar su escritorio libre de información propia de la entidad que pueda ser alcanzada, copiada, no respaldada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Se debe implementar la política de escritorio limpio en los lugares de trabajo para proteger la información crítica o sensible en medios impresos. Todos los funcionarios y contratistas del ICC deben conservar su escritorio libre de información propiedad de la entidad; que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento. Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

Se debe guardar bajo llave la información sensible o crítica de cada grupo cuando no está en uso, especialmente cuando no hay personal en la oficina. En los lugares de trabajo solo deben permanecer los documentos y elementos necesarios para la realización de las labores. No se deben dejar documentos originales, preliminares o finales con información reservada o clasificada a la vista de otras personas, o desatendidos en otro lugar diferente al sitio de trabajo.

Las copias de trabajo deben ser destruidos antes de ser arrojados a la basura. No se deben reutilizar documentos impresos que contengan información reservada o clasificada.

Se debe evitar el consumo de bebidas y alimentos que puedan provocar daños a la información o a los equipos. Se debe implementar la política de pantalla limpia en computadores y portátiles, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Los computadores deben cargar por defecto el fondo de pantalla definido por la entidad, este no debe ser modificado y debe permanecer activo.

Punto de control: *Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.*

11 SEGURIDAD DE LAS OPERACIONES

11.1 Procedimientos operacionales y responsabilidades

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

11.1.1 Procedimientos de operación documentados

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe documentar los procedimientos de operación para:

- Indicar como realiza el control de cambios sobre los servicios tecnológicos del ICC, identificándolos, planificándolos, poniéndolos a prueba y aprobándolos formalmente, así como valorando los impactos, tiempos de no disponibilidad de los servicios, comunicación a las áreas pertinentes e incluir procedimientos y responsabilidades para abortar cambios no exitosos, eventos no previstos y recuperarse de ellos.
- Especificar cómo realiza una gestión de capacidad de los recursos de red, de la infraestructura tecnológica y sistemas de información críticos, en el cual se deben definir los umbrales de alerta e identificar proyecciones de crecimiento que permita mantener la continuidad y la disponibilidad de los servicios tecnológicos.
- Desarrollar un procedimiento de separación de ambientes que permita realizar una transición de los diferentes sistemas desde el ambiente de desarrollo hacia el de producción, con el fin de evitar problemas operacionales que pueden desencadenar en incidentes críticos.

Punto de control: *Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.*

11.1.2 Gestión de cambios

Responsable del control: Grupo de Tecnologías de la Información (TI)

Para cada cambio a nivel de la infraestructura tecnológica en el ICC, debe realizarse:

- Registro del cambio a realizar, identificando el tipo de cambio.
- Citar reunión de cambios con las personas involucradas en el cambio para su comunicación y aprobación.
- Registrar el resultado del cambio y, en caso de no ser exitoso, realizar la reversión correspondiente.

Punto de control: *Se deben controlar los cambios en la entidad, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.*

11.1.3 Gestión de capacidad

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI definirá las actividades y herramientas específicas para monitorear, proyectar y asegurar la capacidad de la infraestructura de procesamiento de información, con el objeto de garantizar el buen desempeño de los recursos tecnológicos necesarios para la ejecución de los procesos.

La capacidad de los recursos debe ser ajustada periódicamente para garantizar la disponibilidad y eficiencia requerida de acuerdo con las necesidades actuales y futuras del ICC, establecidas en el Plan Estratégico de Tecnologías de la Información de la entidad (PETI).

Los umbrales óptimos de capacidad se pueden obtener incrementando la capacidad o reduciendo la demanda, lo cual incluye las siguientes posibles acciones que deberán ser llevadas a cabo por el Grupo de TI tales como:

- Eliminación obsoleta: relacionando el hardware, software, aplicaciones y sistemas de información, bases de datos o ambientes productivos en desuso.
- Optimización de procesos o tareas automáticas.
- Verificación del ancho de banda para servicios garantizando la disponibilidad.

Punto de control: *Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema*

11.1.4 Separación de los ambientes de desarrollo, pruebas, y operación

Responsable del control: Grupo de Tecnologías de la Información (TI)

Se deben establecer y mantener ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información. El ambiente de desarrollo se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código. Por su parte, el ambiente de pruebas se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas hacia el software teniendo como base los criterios de aceptación y los requerimientos de desarrollo.

No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso. Los cambios realizados sobre los sistemas de información deben ser probados en un ambiente diferente al de producción, garantizando la seguridad de la información y que se mantiene operativo el sistema.

Punto de control: *Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.*

11.2 Política de protección contra software malicioso

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

11.2.1 Controles contra códigos maliciosos

Responsable del control: Grupo de Tecnologías de la Información (TI).

Se debe tener instalado como mínimo un software antivirus debidamente licenciado, activo y actualizado que brinde protección contra código malicioso en todos los recursos informáticos de la Entidad, asegurándose que estas herramientas no puedan ser deshabilitadas.

El Grupo de TI debe documentar como se realiza la protección contra códigos maliciosos teniendo en cuenta los controles que utiliza (hardware o software), como se instalan y se actualizan las plataformas de detección, documentación sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo.

El Grupo de TI debe implementar controles que impidan la modificación de las configuraciones del equipo de cómputo o del software instalado con énfasis en el sistema operativo y antivirus. El software de antivirus debe estar realizando escaneos periódicos por demanda y profundos que garanticen que la infraestructura tecnológica está libre de malware.

Se prohíbe la instalación de software no autorizado por el Grupo de TI. Para garantizar el control; el grupo no debe otorgar a los usuarios privilegios de administrador.

Los equipos de cómputo deberían tener una aplicación para la detección de software no autorizado, o en su defecto en los mantenimientos desarrollados identificar y eliminar el software no autorizado encontrado como resultado de los mantenimientos.

Se debe implementar el uso de litas negras para controlar y evitar que los usuarios ingresen a sitios web maliciosos.

Los Servidores Públicos y contratistas, deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos; igualmente, no deben descargar archivos de internet de fuentes desconocidas, en caso de requerirlo, debe generar la solicitud al Grupo de TI.

Los archivos adjuntos que se descarguen de correos electrónicos deberán ser validados por el antivirus de cada equipo de cómputo y puesto en cuarentena si se detecta que contenga malware que comprometa al equipo. Los Servidores Públicos y contratistas que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato al Grupo de TI.

Dentro de los planes de continuidad, se deben incluir acciones para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación. Los contratistas que hagan uso de sus equipos portátiles personales en lo posible deben contar con un software antivirus licenciado y actualizado.

Punto de control: *Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.*

11.3 Copias de respaldo

Objetivo: Proteger contra la pérdida de datos

11.3.1 Respaldo de la información

Responsable del control: Grupo de Tecnologías de la Información (TI) y todos

El Grupo de TI debe contar con un procedimiento para la realización de las copias de respaldo: documentada, definida y publicada en el sistema integrado de gestión (SIG) para respaldar la información de todos los sistemas de información y repositorios de información institucional que así lo requieran.

Adicionalmente, el Grupo de TI deberá establecer mecanismos de restauración de copias de seguridad, los cuales serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado, teniendo en cuenta el procedimiento de restauración. Las copias de respaldo críticas deben almacenarse en un área diferente a la sede principal del ICC y con control de acceso, en aras de restaurar la información posterior a una amenaza o vulnerabilidad que comprometa la información digital.

Los diferentes grupos del ICC deben realizar una limpieza periódica de archivos y documentos obsoletos o inservibles en la nube, con el fin de optimizar el uso de los recursos de almacenamiento que ofrece la entidad a sus usuarios. Los funcionarios y contratistas deben almacenar su información institucional en el OneDrive. De esta manera el Grupo de TI garantizará el respaldo de la información y una eventual restauración en caso de ser requerida.

Los usuarios de la red de datos del ICC no podrán copiar información de tipo reservada sin la debida autorización de su jefe inmediato, de acuerdo con las normas de calificación de la información y los niveles de seguridad establecidos en el sistema de información dispuesto para ello. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución serán sancionadas de acuerdo con las normas y legislación vigentes.

El Grupo de TI deberá definir la periodicidad con la que realiza las copias de respaldo, la criticidad de la información custodiada y establecer la cobertura de las mismas: completas o diferenciales. Todas las copias realizadas a la información del ICC deberán ser cifradas para garantizar la confidencialidad de la información.

11.3.1.1 Política de retención y archivo de datos

Responsable del control: Grupo de Gestión Documental y todos

La política de retención de archivos debe establecer cuánto tiempo se mantendrán almacenados en formato físico y digital en el ICC la información, de acuerdo con las tablas de retención documental (TRD). Las reglas y los principios generales que regulan la función archivística del Estado se encuentran definidos por la Ley 594 de 2000, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.

La Ley 594 de 2000, en los artículos 19 y 21, prevé el uso de las TIC en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

Punto de control: *Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.*

11.4 Registro y seguimiento

Objetivo: Registrar eventos y generar evidencia.

11.4.1 Registro de eventos

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe definir una metodología para la revisión y custodia de eventos (Event Logs), que permita, identificar las actividades por usuario, excepciones, fallas y eventos de seguridad que no den espacio a la alteración, uso no autorizado o repudio, en caso de presentarse materialización del riesgo y ser utilizados como medio probatorio.

El Grupo de TI no debe modificar, borrar o desactivar registros (logs) de sus actividades propias, ni de los usuarios de los sistemas de información, de igual forma se deben realizar las configuraciones de seguridad necesarias para evitar la eliminación o cambios no autorizados a los registros (logs).

El Grupo de TI debe mantener los relojes de todos los equipos y dispositivos sincronizados a un único servidor NTP (Nertwork Time Protocol – protocolo de tiempo en la red), se debe restringir a los usuarios la administración de fecha y hora de los sistemas de información, aplicaciones o equipos de cómputo a su cargo.

Los registros de auditoría deberán incluir:

- identificar los usuarios;
- establecer las actividades del sistema;
- definir las fechas, horas y detalles de los eventos clave, (entrada y salida);
- identificar el dispositivo o ubicación, si es posible, e identificador del sistema;
- tener registros de intentos de acceso al sistema exitosos y rechazados;
- definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos;
- establecer los cambios a la configuración del sistema;
- definir el uso de privilegios;
- establecer el uso de utilitarios y aplicaciones del sistema;
- definir los archivos a los que se tuvo acceso, y el tipo de acceso;
- definir las alarmas accionadas por el sistema de control de acceso;
- activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión;
- registrar las transacciones ejecutadas por los usuarios en las aplicaciones.

Punto de control: *Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.*

11.4.2 Protección de la información de registro

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI, con el fin de proteger la información de registro de modificación no autorizada por parte de usuarios no autorizados, administradores u operadores de los sistemas de información, debe implementar mecanismos de copiado de logs en «tiempo real» a un sistema por fuera del control de administradores y operadores de los sistemas.

Los logs deben tener mecanismos de seguridad y control administrativo resistentes a ataques para evitar la adulteración de estos, también deben generar las capacidades suficientes para detectar y grabar eventos significativos en aspectos de seguridad de información.

Punto de control: *Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado***.**

11.4.3 Registros del administrador y del operador

Responsable del control: Grupo de Tecnologías de la Información (TI)

Se deben administrar y operar en tiempo real los Logs de los administradores y otras cuentas privilegiadas para evitar perdida o adulteración de estos y realizar auditorías periódicas a estas actividades. Se deben activar los mecanismos de auditoria en toda la infraestructura tecnológica que permitan registrar las actividades de los administradores, incluyendo evidencia de que estas cuentas no tienen privilegios para modificar o eliminar registros de eventos.

Punto de control: *Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.*

11.4.4 Sincronización de relojes

Responsable del control: Grupo de Tecnologías de la Información (TI)

Se debe contar con un mecanismo de sincronización de relojes de los diferentes equipos de cómputo, servidores, dispositivos de red, sistemas operativos bases de datos, sistemas de información y demás elementos de infraestructura utilizados por el ICC utilizando como referencia la hora oficial de Colombia (Instituto Nacional de Metrología) horalegal.inm.gov.co para la relación adecuada de eventos o para la investigación efectiva de incidentes.

Punto de control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la entidad o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.

11.5 Control de software operacional

Objetivo: Asegurar la integridad de los sistemas operacionales

11.5.1 Instalación de software en sistemas operativos

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe mantener un procedimiento de control de instalación y cambios de los sistemas operativos administrados por el grupo; para mantener operativas las aplicaciones basadas en estos y que permitan procedimientos de retroceso (RollBack) exitosos, en este procedimiento se debe incluir la elaboración de copias de respaldo que puedan responder a planes de contingencia. No se permite la descarga e instalación de software, archivos de audio, medios audiovisuales que atenten contra los derechos de autor, la infraestructura tecnológica y la seguridad de la información.

Punto de control: *Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.*

11.6 Gestión de vulnerabilidad técnicas

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas

11.6.1 Gestión de las vulnerabilidades técnicas

Responsable del control: Grupo de Tecnologías de la Información (TI).

Se debe contar con una metodología de identificación de vulnerabilidades técnicas en los sistemas de información y servicios tecnológicos del ICC, como resultado de estas deben elaborarse planes de mejoramiento que permita a los responsables aplicar los controles de mitigación que correspondan, previa evaluación en un ambiente de pruebas.

Se debe generar y ejecutar por lo menos una vez al año un análisis de vulnerabilidades y/o hacking ético para las plataformas críticas de la entidad cuya viabilidad técnica y administrativa lo permitan. Una vez se lleve a cabo la ejecución de escaneos de vulnerabilidad en la plataforma tecnológica de la entidad, las vulnerabilidades o hallazgos identificados se deben remediar de acuerdo con los lineamientos establecidos por los Procedimientos de Gestión de Vulnerabilidades.

Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, deben realizarse teniendo en cuenta las directrices establecidas en el Procedimiento de Gestión de Cambios cuando su aplicación se lleve al ambiente de producción.

Punto de control: *Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.*

11.6.2 Restricciones sobre la instalación de software

Responsable del control: Grupo de Tecnologías de la Información (TI)

Los funcionarios de la entidad no podrán instalar ningún software, programa o aplicativo en los equipos designados para su labor en la entidad. Solo el Grupo de TI, es la única autorizada para la instalación o actualización de software, sistemas operativos y otros, asegurando que esta tarea se lleve a cabo por personal capacitado. El Grupo de TI debe conservar la última versión estable del software como estrategia de contingencia ante la necesidad de un retroceso o rollback.

El Grupo de TI debe implementar controles para:

- Proteger todo el software y la documentación del sistema.
- Guardar solo los archivos de ejecución de los aplicativos en el ambiente de producción.
- Llevar un registro de las actualizaciones realizadas a los aplicativos.

Para la instalación de software se deben seguir las siguientes directrices:

- El software licenciado debe contar con su respectiva documentación (licencia) y, en el caso del software libre, debe estar permitido el uso comercial.
- El instalador debe ser descargado de la página oficial del fabricante.

El Grupo de TI debe comunicar a los funcionarios y contratistas sobre las consecuencias por el uso ilegal de software, y juntamente con la Oficina de Control Interno Disciplinario en el caso de funcionarios y supervisión de contrato en caso de contratistas, deben definir y establecer las sanciones que haya lugar para cumplir con la legislación vigente relacionada con los derechos de autor y datos personales.

Punto de control: *Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.*

11.7 Consideraciones sobre auditorías de sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

11.7.1 Controles de auditorías de sistemas de información.

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe planificar periódicamente actividades que involucren auditorías de los sistemas en producción. Para la ejecución de auditorías a los sistemas de información se deben tener en cuenta las siguientes consideraciones:

- establecer los requisitos de auditoría para acceso a sistemas y a datos, se debe acordar con el propietario del sistema de información;
- definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar;
- establecer las pruebas de auditoría: se debe limitar el acceso al software y datos únicamente para lectura;
- definir el acceso diferente al de solo lectura: solamente se debe prever para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría;
- definir los requisitos para procesos especiales y adicionales: se debe identificar y acordar;
- establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema: se deben realizar fuera de horas laborales;
- hacer seguimiento de todos los accesos y logueos para producir un rastro de auditoría.

El Grupo de TI debe documentar los resultados de las auditorias de los sistemas en producción.

Punto de control: *Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de la entidad.*

12 SEGURIDAD DE LAS COMUNICACIONES

12.1 Gestión de seguridad de redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

12.1.1 Controles de redes

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI es la responsable de mantener disponible toda la infraestructura de red que soportan los servicios tecnológicos en el ICC. Deberá disponer de una zona desmilitarizada o DMZ, entre la red interna y la red externa (internet) con el objetivo limitar conexiones desde la red interna hacia Internet y conexiones desde internet hacia la red interna del ICC:

- El tráfico de la red externa a la DMZ está limitado.

- El tráfico de la red externa a la red interna deberá estar restringido y monitoreado.
- El tráfico de la red interna a la DMZ está limitado.
- El tráfico de la red interna a la red externa está limitado

Por seguridad y para propósitos de mantenimiento, se podrá monitorear en cualquier momento el tráfico de la red. Esta labor será realizada solo por el personal autorizado por la coordinación del Grupo de TI, garantizando a los usuarios que no existirá revisión interna de archivos o documentos.

Las redes de datos y comunicaciones del ICC deben estar gestionadas y controladas para la protección de la información y sus aplicaciones, gestión de red y configuración de redes virtuales o creación de subredes que permitan separar los servicios de información, usuarios y sistemas.

La entidad proporciona a los funcionarios todos los recursos tecnológicos de conectividad necesarios, para que puedan desempeñar las funciones/actividades para las cuales fueron vinculados, por tal motivo no se permite conectar a las estaciones de trabajo o a los puntos de acceso corporativos, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el Grupo de TI.

Punto de control: *Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.*

12.1.2 Seguridad de los servicios de red

Responsable del control: Grupo de Tecnologías de la Información (TI).

Los colaboradores que requieran acceder a algunos recursos informáticos cuando se encuentren fuera de las instalaciones de la Entidad deberán realizarlo a través de una conexión de red virtual privada (VPN), solicitada al Grupo de TI o instalada de acuerdo con los lineamientos de la guía articulada al SIG. Se debe validar la desvinculación del usuario para realizar la desactivación de esta en el tiempo que se ha definido.

No se podrá conectar dispositivos celulares personales a la red wifi del ICC, salvo si es requerido para una situación especial. La conexión de dicho dispositivo debe ser realizado por el Grupo de TI.

El Grupo de TI debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos y también debe realizar de manera periódica el cambio de las claves de acceso a la red WIFI del ICC.

Todo proveedor de servicios de red debe ser monitoreado con regularidad y realizando seguimiento a las capacidades contratadas a través de auditorías. En los acuerdos de nivel de servicios se deben identificar los niveles de requisitos de seguridad necesarios para los servicios contratados.

Punto de control: *Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.*

12.1.3 Separación en las redes

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de alguna de las dos redes. La conexión a la red wifi institucional para funcionarios deberá ser administrada desde el Grupo de TI mediante un SSID (Service Set Identifier) único a nivel del ICC; la autenticación deberá ser con usuario y contraseña.

Punto de control: *Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.*

12.2 Transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una Entidad y con cualquier entidad externa.

12.2.1 Políticas y procedimientos de transferencia de información

Responsable del control: Grupo de Tecnologías de la Información (TI) y Grupo de Gestión Documental**.**

Los canales de red utilizados para la transferencia de información deberán contar con un mecanismo que no permita la fuga o interceptación de información, en su defecto la información que viaja por estos deberá estar cifrada. La información de la entidad puede ser intercambiada a través de los siguientes canales de comunicación electrónica: Office 365, descarga de archivos desde internet, transferencia de datos por medio de los sistemas de información misionales, administrativos o financieros, telefonía IP. Está prohibida la transferencia de información por mensajería instantánea personal como WhatsApp, salvo que ninguno de los medios descritos anteriormente esté en funcionamiento.

Está prohibido el uso del correo electrónico personal para el envío o recepción de cualquier tipo de información relacionada con la entidad. La información física, no se debe dejar abandonada en impresoras, en el puesto de trabajo o un área de circulación alta de personas.

Punto de control: *Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones*

12.2.2 Acuerdos sobre transferencia de información

Responsable del control: Grupo de Tecnologías de la Información (TI) y Grupo de Gestión Documental.

El ICC implementará los protocolos de seguridad necesarios para la transferencia de archivos. Cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad a través de un acuerdo de niveles de servicio. Para todo intercambio de información sensible se deben establecer acuerdos de confidencialidad.

El Grupo de TI deberá establecer procedimientos para la detección de software malicioso y protección en la transferencia de información, también deberá establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico del ICC.

El intercambio de información digital pública clasificada y pública reservada, debe realizarse por canales cifrados que garanticen la protección de la confidencialidad de la información y que cumpla con la política de controles criptográficos, esto debe quedar registrado en los convenios o acuerdos de intercambio de información que firmen las partes.

Para el transporte de medios físicos que contengan información digital o electrónica, se debe generar un registro de entrega de estos medios y recepción de estos y se debe transportar en un dispositivo con un sello de seguridad que garantice que en su desplazamiento no ha sido intervenido por un tercero.

Punto de control: *Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.*

12.2.3 Política de uso de mensajería electrónica

Responsable del control: Grupo de Tecnologías de la Información (TI)

El ICC debe ofrecer a sus estudiantes, funcionarios y contratistas un servicio que permita el intercambio de mensajes a través de una cuenta de correo electrónico institucional para facilitar el desarrollo de sus funciones, actividades u obligaciones. Por lo anterior, los usuarios del correo electrónico institucional son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

Las cuentas de correo electrónico institucional son propiedad del ICC, y son asignadas a usuarios que tengan algún tipo de vinculación con la entidad, bien sea como personal de planta, contratistas, profesores, estudiantes o egresados y deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la entidad.

Los servicios de correo electrónico institucional se emplean para una finalidad académica, operativa y administrativa institucional. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura tecnológica del ICC se consideran bajo el control de la entidad.

El servicio de correo electrónico institucional no debe utilizarse para el envío de mensajes masivos. Para las comunicaciones que requieran la divulgación a través de correo masivo, se debe realizar la solicitud a la cuenta de correo institucional comunicacioninterna@caroycuervo.gov.co, si el contenido requiere publicación de piezas graficas que incluyen el logo o imagen del ICC, deberá contar con la aprobación del líder del Equipo de Comunicaciones y Prensa. El servicio de correo electrónico institucional no debe ser utilizado para el envío de mensajes personales, de tipo cadena, ni mensajes de gran tamaño que puedan congestionar la red; para ello deben emplearse otros medios como, por ejemplo, los servicios de la nube de archivos digitales, tampoco se permite el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

Los usuarios del servicio de correo electrónico institucional deben habilitar el servicio de autorrespuesta en el evento en que se encuentren ausentes por largos periodos, ya sea por el periodo de vacaciones, incapacidades, licencia, etc. Los Líderes de Procesos y supervisores de los usuarios que terminan su vínculo laboral o contractual con el ICC deben indicar al Grupo de TI, cuál será el usuario/buzón delegado al que se redireccionarán las comunicaciones de las cuentas de correo electrónico que tienen acceso a plataformas externas y que puedan recibir información de interés para la Entidad, es decir la información de tipo misional o estratégica, si no lo hace el Grupo de TI deberá redireccionará los correos al jefe inmediato o supervisor.

Para las cuentas de correo electrónico de los egresados del ICC, se les mantendrá activa su cuenta y deberán cumplir las políticas de seguridad, sin embargo, si un egresado no hace uso de su cuenta de correo por un periodo de tiempo de (2) dos años o se evidencia un uso indebido del correo que comprometa la reputación de la Entidad o vaya en contra de las políticas de seguridad y privacidad de la información se suspenderá dicha cuenta.

La apariencia de la firma de correo electrónico está establecida por los parámetros de la imagen institucional de la entidad y ningún funcionario o contratista está autorizado para alterar la forma o la información contenida. Los correos electrónicos contienen una nota respecto al manejo del contenido y seguridad del mensaje enviado con la siguiente información:

"AVISO IMPORTANTE: *Toda información enviada desde el ICC a través de correos electrónicos deberá incluir en su pie de página la siguiente advertencia: "AVISO IMPORTANTE: Este mensaje de correo electrónico y sus anexos son únicamente para uso del destinatario ya que puede contener información pública reservada o información pública clasificada, las cuales no son de carácter público. Si usted no es el destinatario, le solicitamos no leer, copiar, reenviar, difundir, distribuir o guardar este mensaje y sus anexos. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida, por personas o entidades diferentes al propósito original de la*

misma, es ilegal. Si usted es el destinatario, le solicitamos dar un manejo adecuado a la información; en caso de que se identifique algún hecho extraño, por favor informarlo al correo tics@caroycuervo.gov.co."

Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo con la calificación de la información establecida por el ICC. Los mensajes de origen desconocido o con contenido sospechoso no deben ser respondidos, ni sus archivos adjuntos abiertos, ni establecer conexión con los enlaces que aparezcan en el mensaje ya que podrían contener códigos maliciosos (virus, troyanos, keylogger, gusanos, etc.). Se debe reenviar el correo a la cuenta tics@caroycuervo.gov.co con la frase "mensaje sospechoso" en el asunto.

12.2.3.1 Publicación de la dirección de correo electrónico como dato de contacto

Responsable del control: Todos

El ICC cuenta con dos tipos de correo, el primero es el correo institucional de las dependencias ejemplo (contactenos@caroycuervo.gov.co), el cual puede ser accedido y utilizado para finalidades netamente relacionadas con el grupo que corresponde, por los funcionarios y/o contratistas que el coordinador de la dependencia haya establecido. Todo envío sea interno o externo que se realice a través de este correo debe contar con el aval de su respectivo coordinador pues él es el responsable del uso y manejo que se le dé a dicha cuenta.

El segundo tipo de correo es el correo institucional personal ejemplo (pepe.correa@caroycuervo.gov.co) el cual contiene el nombre y apellido del titular de la cuenta y el único responsable del uso y manejo que se le dé a este servicio, por lo cual este acceso es personal e intransferible.

Para la atención y gestión de trámites, eventos, proyectos, servicios o procesos de actividad se deben vincular las cuentas de correo institucionales de las dependencias y grupos de trabajo, en lugar de las cuentas de correo institucionales personales, esto con el fin de mantener la continuidad del servicio y garantizar la disponibilidad de la información.

Se debe limitar la publicación de los correos electrónicos de funcionarios y/o contratistas, salvo las directrices estipuladas por la normatividad vigente tal es el caso del directorio publicado en el portal institucional y el aplicativo SIGEP, donde el usuario debe publicar su correo institucional personal y no el correo de la dependencia o grupo de trabajo.

12.2.3.2 Política de redes sociales

Responsable del control: Comunicaciones

El responsable de la comunidad virtual del ICC será el único que administre las cuentas de las redes sociales oficiales de la entidad, en ningún caso el contenido publicado podrá ser utilizado para beneficios

personales o de terceros, así como tampoco se permite que las publicaciones reflejen las opiniones o sentimientos personales del administrador. La información que se publique o divulgue por cualquier medio de internet, de cualquier funcionario o contratista del ICC, que sea creada a nombre personal, como redes sociales (X, Instagram, Facebook, YouTube, LinkedIn o blogs), se considera fuera del alcance del SGSI, y por lo tanto su confiabilidad, integridad, veracidad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

El responsable de las redes sociales, el Equipo de Comunicaciones y Prensa, y los servidores públicos deberán dar cumplimiento a los lineamientos dados por el gobierno nacional sobre el manejo y uso de redes sociales de acuerdo con lo estipulado en la circular N. 01 del 22 de marzo del 2019 por la Presidencia de la Republica.

12.2.3.3 Política para la gestión de contenidos de páginas WEB (Web máster)

Responsable del control: Comunicaciones

Los responsables de los contenidos de las páginas web (Web máster) son los únicos autorizados para realizar publicaciones en los sitios web de la entidad. El contenido web a publicar en los diferentes sitios web de la entidad, debe ser previamente revisado y aprobado por el líder del Equipo de Comunicaciones y Prensa, y por el corrector de estilo o quien haga sus veces.

- El web máster es responsable de mantener respaldo de los contenidos web.
- El web máster debe proporcionar las condiciones necesarias para la actualización de la versión del software, la cual será ejecutada por los administradores de los servidores y el equipo desarrollador.
- Los web máster debe disponer de un archivo actualizado con la información de la página inicial del sitio, en caso de que se requiera revertir los cambios o actualizaciones.
- Para la publicación de contenido en los sitios web, el web máster deben llevar un registro de publicaciones y coordinar con el administrador web del Grupo de TI los lineamientos técnicos y de diseño de los sitios web.
- Equipo de Comunicaciones y Prensa deberá contar con una “política editorial y actualización de contenidos web”, y, basados en esta política, mantener una bitácora que permita auditar la publicación o modificación de información oficial en las páginas web.
- Las claves de acceso a los sistemas de gestión de contenidos o CMS (Content Management System), que utilizan el web máster para la administración de los sitios Web, son estrictamente confidenciales, personales e intransferibles.

12.2.3.4 Política de uso de internet

Responsable del control: Todos

Los usuarios de la red deben ser conscientes del uso adecuado de internet, y deben evitar el acceso a sitios potencialmente peligrosos o que puedan afectar el buen desempeño de la red. El Grupo de TI inhabilitará el acceso a sitios web identificados como peligrosos o de alto consumo de ancho de banda, de acuerdo con su categoría, y serán clasificados en el documento correspondiente a fin de proteger y no comprometer la seguridad y el desempeño de la red y los recursos informáticos de la entidad.

No se permite la navegación a sitios con contenidos que representen peligro para la entidad como pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes asociadas a estos riesgos.

El acceso a sitios web con contenido calificado como potencialmente peligroso, con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del coordinador de grupo o el supervisor de contrato. Sin embargo, el Grupo de TI analizará el sitio web que deba ser habilitado para verificar que el mismo es seguro y que no representa un peligro para la red de datos de la entidad.

La descarga de archivos de internet debe hacerse con propósitos laborales y de forma razonable para no afectar el servicio de Internet y la red de datos en general.

12.2.3.5 Política de seguridad para la telefonía IP

Responsable del control: El Grupo de Tecnologías de la Información (TI), Grupo de Recursos Físicos y Subdirección Administrativa y Financiera (SAF).

El Grupo de TI administrará y gestionará el uso de las extensiones telefónicas y las configuraciones asociadas para planificar el crecimiento futuro, así como para atender oportunamente las averías y/o cambio de perfil de usuario. El Grupo de TI administra y gestiona los equipos de telefonía IP, así como los equipos de autoatención y correo de voz. La configuración o cambio de opciones en la grabación de autoatención, debe ser aprobada por la SAF.

El Grupo de TI mantendrá un inventario de los aparatos telefónicos para la gestión propia de esta oficina, sin perjuicio de los bienes devolutivos registrados en recursos físicos para la administración, reposición, detección de necesidades y resguardo de los bienes de la Institución. La solicitud del aparato telefónico debe hacerse al Grupo de Recursos Físicos del ICC y su asignación estará sujeta a la disponibilidad. La solicitud de creación de una nueva extensión debe gestionarse a través de la mesa de ayuda, y es el supervisor de contrato o el coordinador del grupo quien realiza dicha solicitud.

Las llamadas a larga distancia nacional, internacional y telefonía móvil están habilitadas solo a funcionarios autorizados por la SAF. Los usuarios deben notificar al Grupo de TI sobre cualquier anomalía en el servicio telefónico o cuando exista la sospecha del uso indebido del mismo.

Punto de control: *Se debe proteger adecuadamente la información incluida en la mensajería electrónica.*

12.2.4 Acuerdos de confidencialidad

Responsable del control: Grupo de Talento Humano y Grupo de Gestión Contractual.

Todo funcionario del ICC debe firmar en señal de aceptación el acuerdo de confidencialidad en el proceso de vinculación con la Entidad, para el caso de los contratistas y terceros el Grupo de Gestión Contractual deberá incluir cláusulas de confidencialidad en sus respetivos contratos.

Punto de control: *Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la entidad para la protección de la información.*

13 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

13.1 Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.

13.1.1 Análisis y especificación de requisitos de seguridad de la información

Responsable del control: Grupo de Tecnologías de la Información (TI) y Grupo de Investigaciones Académicas (desarrollo de software).

El Grupo de TI debe identificar durante la etapa de levantamiento de requerimientos funcionales los requisitos de seguridad de la información, incluyendo las configuraciones de red para proteger la información que se administra en las bases de datos y que son transmitidas, estos requerimientos deben quedar documentados como parte del proyecto de tecnologías de la información, esto aplica para nuevos o para mejoras de los sistemas de información y servicios tecnológicos existentes que se desarrollen en el ICC o que sean adquiridos a través de un tercero. Los requisitos de seguridad de la información deben estar presentes durante todo el ciclo de vida de desarrollo y mantenimiento.

La adquisición de aplicativos o software informático debe ser aprobado o adquirido por el Grupo de TI, en concordancia con la política de adquisición de bienes del ICC, según lo definido en el Proceso de Adquisiciones, y las necesidades específicas de cada proceso.

El Grupo de TI realizará periódicamente una revisión del software utilizado en cada uno de los grupos. Los desarrollos y proyectos que se deban adelantar en la entidad y que involucren componentes de TI, deben ser informados al Grupo de TI, a fin de contar con el acompañamiento apropiado y con la aprobación de

viabilidad para su ejecución. Si se omite esta política, la entidad no se hace responsable ante ningún tercero por los requerimientos que se generen en cuanto a la legalización de las licencias, servicios de soporte o mantenimiento de productos.

Dentro de los requisitos de seguridad de la información se debe:

- Establecer el nivel de confianza requerido para obtener los requisitos de autenticación de usuario.
- Definir los procesos de suministro de acceso y de autorización para usuarios de la entidad, al igual que para usuarios privilegiados o técnicos, por ejemplo, el suministro de datos de acceso por correo electrónico.
- Definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad; por ejemplo, cifrado de información almacenada y el envío de información por canales cifrados.
- Definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio, formularios de autenticación mediante HTTPS (Protocolo seguro de transferencia de hipertexto es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.), cifrado de contraseñas almacenadas y uso de firmas digitales.
- Establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).
- La implementación de segundos factores de autenticación y un sistema de gestión de contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar su reutilización.
- Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.
- La necesidad de exigir la implementación de metodologías de desarrollo seguro.
- Informar a los usuarios y operadores sobre sus deberes y responsabilidades frente a la seguridad de la información dentro de las actividades de adquisición, desarrollo y mantenimiento de sistemas.

Punto de control: *Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes*

13.1.2 Seguridad de servicios de las aplicaciones en redes públicas

Responsable del control: Grupo de Tecnologías de la Información (TI)

Los sistemas de información o servicios tecnológicos que transmitan y/o transfieran información sobre redes públicas deben incluir un mecanismo de cifrado de los datos que se transportan, así mismo se deben aplicar controles tales como el uso de métodos fuertes de autenticación, certificados digitales, autorización de documentos mediante firmas digitales, funcionamiento con certificados SSL y los demás que apliquen.

Directrices para la seguridad de servicios de las aplicaciones en redes públicas:

- Definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación).
- Establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales claves.
- Asegurar que las partes que establecerán la comunicación estén completamente informadas de sus autorizaciones para suministro o uso del servicio.
- Determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos (asociados con procesos de ofertas y contratos).
- Definir el nivel de confianza requerido en la integridad de los documentos clave.
- Establecer los requisitos de protección de cualquier información confidencial.
- Definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibido.
- Definir el grado de verificación apropiado de la información de pago suministrada por un usuario.
- Seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude.
- Definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido.
- Evitar la pérdida o duplicación de información de la transacción.
- Definir la responsabilidad civil asociada con cualquier transacción fraudulenta.
- Establecer los requisitos de seguros.
- De acuerdo con el estándar de NIST se deben usar mecanismos de chequeo de la integridad para verificar la integridad del software, firmware, e información.

Punto de control: *La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.*

13.1.3 Protección de transacciones de los servicios de las aplicaciones

Responsable del control: Grupo de Tecnologías de la Información (TI)

Los servicios o sistemas asociados a transacciones electrónicas se deben proteger para evitar transmisiones incompletas, alteraciones, envíos errados o divulgación no autorizada, utilizando controles para evitar la duplicación de información en las transacciones, a través de mecanismos o protocolos como uso de certificados SSL, el uso de criptografía y otros.

Directrices para la protección de transacciones de los servicios de las aplicaciones:

- Definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción;
- Establecer todos los aspectos de la transacción, es decir, asegurar que:

- Definir, validar y verificar la información de autenticación secreta de usuario.
- Definir que la transacción permanezca confidencial.
- Mantener la privacidad asociada con todas las partes involucradas
- Definir que la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada.
- Definir que todos los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados.
- Asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente (por ejemplo, en una plataforma de almacenamiento interno, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde internet).
- Utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas o certificados digitales).

La seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

Punto de control: *La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.*

13.2 Seguridad en los procesos de desarrollo y soporte

Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

13.2.1 Política de desarrollo seguro

Responsable del control: Grupo de Tecnologías de la Información (TI) y proveedores externos (desarrolladores de software)

El Grupo de TI debe asegurar que los sistemas de información o aplicativos informáticos que desarrolla internamente incluyen controles de seguridad, estén completamente documentados y que las diferentes versiones sean preservadas adecuadamente.

Los funcionarios o terceros que realicen desarrollos para el ICC deben aplicar los lineamientos de desarrollo seguro durante todo el ciclo de vida de estos. El Grupo de TI debe implementar procedimientos que permitan tener un control en la generación de cambios o mejoras en el código fuente de los sistemas de información y servicios tecnológicos de la entidad, igualmente debe cerciorarse de que los funcionarios o terceros que tienen el rol de programador posean acceso solo a la parte del código necesaria para desarrollar su trabajo.

Directrices de desarrollo seguro:

- Definir la seguridad del ambiente de desarrollo.
- Orientar la seguridad en el ciclo de vida de desarrollo del software.
    - Definir la seguridad en la metodología de desarrollo de software.
    - Establecer las directrices de codificación seguras para cada lenguaje de programación usado.
- Definir los requisitos de seguridad en la fase diseño.
- Definir los puntos de chequeo de seguridad dentro de los hitos del proyecto.
- Establecer los depósitos seguros.
- Definir la seguridad en el control de la versión.
- Establecer el conocimiento requerido sobre seguridad de la aplicación.
- Definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.

Punto de control: *Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la entidad.*

13.2.2 Procedimientos de control de cambios en sistemas

Responsable del control: Grupo de Tecnologías de la Información (TI) y proveedores externos (desarrolladores de software)

Cualquier tipo de cambio sobre los sistemas de información deberá seguir lo establecido en el Procedimiento del ICC y debe tener en cuenta la aceptación de las pruebas técnicas y funcionales dictaminadas por cada uno de los responsables a quienes afectaran los cambios que se realicen.

Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación. Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, post instalación y criterios de aceptación del cambio. En ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por el usuario, o un tercero externo que no haya sido contratado para ese propósito. Cualquier cambio que se requiera en los equipos de cómputo (repotenciación o reparación) se debe evaluar técnicamente y ser autorizado. La reparación técnica de los equipos, que implique la apertura de estos, únicamente puede ser realizada por el personal del Grupo de TI.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de manera acorde a los requisitos de seguridad existentes y autorizados por el Grupo de TI.
Cualquier tipo de cambio en la plataforma tecnológica debe ser documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el

cumplimiento de los procedimientos definidos. Los cambios en recursos tecnológicos que sean implementados deberán desarrollar la estrategia de uso y apropiación que se tenga definida, aplicada según la necesidad, para garantizar que los usuarios procedan con conocimiento en el manejo de las nuevas herramientas o funcionalidades derivadas de las ya existentes

Punto de control: *Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.*

13.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Responsable del control: Grupo de Tecnologías de la Información (TI)

Una vez se ha producido el cambio tecnológico, el Grupo de TI debe:

- Revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones.
- Asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación;
- Asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.

Punto de control: *Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas de la entidad y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad del ICC.*

13.2.4 Restricciones en los cambios a los paquetes de software

Responsable del control: Grupo de Tecnologías de la Información (TI).

Todo software desarrollado o contratado en el ICC, en el momento que requiera una actualización o cambio debe contemplar:

- Definir el riesgo de pérdida de integridad de los datos del sistema.
- Obtener el consentimiento del fabricante.
- Obtener del fabricante los cambios requeridos.
- Evaluar el impacto.
- Contemplar si el ICC será responsable del mantenimiento futuro del software.
- Definir la compatibilidad con otro software en uso.

Punto de control: *Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.*

13.2.5 Principios de construcción de los sistemas seguros

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe documentar, aplicar y exigir que la construcción de sistemas de información cumpla con requerimientos de diseño de arquitectura segura. Los sistemas de información deben actualizarse con regularidad para combatir nuevas amenazas potenciales. Los nuevos desarrollos deben pasar por un proceso de análisis de gestión de riesgos de seguridad, y el diseño se deberá revisar contra patrones de ataque conocidos. Se debe contar con los tres ambientes diferenciados claramente en cuanto a servidores de aplicaciones y bases de datos.

Se debe proteger cada uno de los computadores, dispositivos de red y de comunicaciones que se consideren críticos del acceso físico de personal no autorizado, para garantizar la confidencialidad, disponibilidad e integridad de la información. Los accesos al ambiente de producción deben ser restringidos por segregación de funciones y permisos de administrador de cada ambiente.

Punto de control: *Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.*

13.2.6 Ambiente de desarrollo seguro

Responsable del control: Grupo de Tecnologías de la Información (TI).

El Grupo de TI con el objeto de asegurar la información en el desarrollo de sistemas de información debe:

- Aplicar los controles tales como: control de acceso, copias de respaldo, registro de eventos y separación de ambientes de desarrollo y de producción.
- Asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas, de acuerdo con el procedimiento de gestión de cambios tecnológicos.
- Contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de propios del ICC y contratados.
- Preservar el carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
- Definir los requisitos externos e internos aplicables (reglamentaciones o políticas).
- Definir los controles de seguridad ya implementados por el ICC, que brindan soportar al desarrollo del sistema.
- Establecer la confiabilidad del personal que trabaja en el ambiente.
- Definir el grado de contratación externa asociado con el desarrollo del sistema.
- Definir la necesidad de separación entre diferentes ambientes de desarrollo.
- Definir el control de acceso al ambiente de desarrollo.
- Establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí.
- Definir las copias de respaldo se almacenan en lugares seguros fuera del sitio.

- Definir el control sobre el movimiento de datos desde y hacia el ambiente.

Punto de control: *Las entidades deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas*

13.2.7 Desarrollo contratado externamente

Responsable del control: Grupo de Tecnologías de la Información (TI).

- El desarrollo de software contratado deberá contemplar todos los requisitos en cuanto a seguridad de la información fijados en este documento.
- Solo se darán por recibidos desarrollos realizados sobre los estándares del ICC, en cuanto a la herramienta de desarrollo, pruebas técnicas y funcionales.
- Los contratos de desarrollo de software con terceros deberán tener claramente definidos los alcances de las licencias, los derechos de propiedad del código desarrollado y los derechos de propiedad intelectual, junto con los requerimientos contractuales relacionados con la calidad y seguridad del código desarrollado.
- Se debe realizar un análisis de vulnerabilidades técnicas a los sistemas de información desarrollados y que estén en proceso de paso a producción, para garantizar que los nuevos desarrollos no exponen la seguridad de la información. No deben tener vulnerabilidades críticas ni altas.
- Se debe acordar la entrega de manuales técnicos que describan la estructura interna del sistema, así como el diccionario de datos, librerías ejecutables, modelo entidad relación de la base de datos, manuales funcionales, manual del usuario y manual de instalación
- El Grupo de TI deben exigir el suministro de evidencia sobre la realización de pruebas de seguridad al software desarrollado por terceros.

Punto de control: *La entidad debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.*

13.2.8 Pruebas de seguridad de sistemas

Responsable del control: Grupo de Tecnologías de la Información (TI)

- Se deberá estandarizar el ciclo de vida, criterios de seguridad y de calidad en el desarrollo de software.
- Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.

- Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post instalación y criterios de aceptación del cambio.
- Para propósitos de desarrollo y pruebas de software, se deberán generar datos de prueba distintos a los que se encuentran en el ambiente de producción.
- Los desarrolladores y terceros no deberán tener acceso a información de producción que contenga datos sensibles.
- Si el desarrollador incluye comentarios en el programa fuente, estos no deben divulgar información de configuración innecesaria.
- La documentación de los desarrollos deberá:
    - Generarse durante el ciclo de vida de desarrollo y no postergarla hasta el final.
    - Ser revisada por los usuarios finales del sistema en desarrollo.
    - Actualizarse si el programa cambia alguna de sus funcionalidades.
    - Almacenarse en un sitio centralizado (servidor) administrado por el funcionario encargado de desarrollo.
- No está permitido modificar programas sin que quede registrado o documentado.
- En lo posible, las pruebas del sistema deberán incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación de errores.
- Se deberán tener las siguientes consideraciones con relación a los datos de entrada y salida de los sistemas de información:
    - Realizar las validaciones de datos de entrada y salida en un sistema confiable.
    - Utilizar rutinas de validación centralizadas y estandarizadas.
    - Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos y longitud entre otros.
    - Limpiar las salidas de datos no confiables hacia consultas SQL, XML o hacia comandos de sistemas operativo.

Punto de control: *Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.*

13.2.9 Prueba de aceptación de sistemas

Responsable del control: Grupo de Tecnologías de la Información (TI).

Las aplicaciones deberán contar con un sistema de autenticación de usuario, que mínimo exija nombre de usuario y contraseña. Además, en los casos que la aplicación esté expuesta a internet, debe implementarse un segundo factor de autenticación. Las aplicaciones deberán contar con manejo de diferentes roles con permisos de acceso y operaciones asociados a estos.

Con la finalidad de garantizar la disponibilidad de la información se deben realizar las siguientes pruebas:

- Pruebas de compatibilidad: se debe garantizar el funcionamiento adecuado y continuo del software desarrollado en diferentes plataformas: hardware, sistemas operativos y redes.

- Pruebas de integración: se debe comprobar las conexiones y comunicaciones entre los diferentes módulos del software desarrollado y los demás sistemas de información de la entidad que tengan relación con el desarrollo.
- Pruebas de función: asegurar que el sistema cumple con la funcionalidad para el cual fue hecho, con las especificaciones técnicas esperadas y es útil para los funcionarios del ICC.
- Pruebas de desempeño: establecer la eficiencia del sistema de información cuando es utilizado por parte de los funcionarios de la entidad, estableciendo posibles fallas antes de su puesta en marcha.
- Pruebas de instalación: instalar el sistema de información en el servidor que alojará la base de datos o los archivos fuente del sistema de información.

Se deben realizar pruebas de aceptación del software por parte de una persona diferente de quien lo ha desarrollado; estas pruebas deben reposar en un documento. La ejecución de pruebas funcionales debe incluir la evaluación de los requisitos de seguridad de la información y la evaluación de los requisitos funcionales.

Punto de control: *Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.*

13.3 Datos de prueba

Objetivo: Asegurar la protección de los datos usados para ensayos

13.3.1 Protección de datos de prueba

Responsable del control: Grupo de Tecnologías de la Información (TI)

Los datos de prueba no deben contener información clasificada o reservada, de ser necesario este contenido se deben utilizar mecanismos de enmascaramiento o sustitución de datos. Una vez terminadas las pruebas, deben ser eliminados con el fin de no revelar información confidencial de los ambientes de producción, dando cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales), Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública) y la Ley 1437 de 2011.

Los entornos de pruebas para nuevos desarrollos o para sistemas de información críticos que se encuentren habilitados deben ser autorizados por el Grupo de TI, y en caso de ser necesario el acceso desde fuera de la red LAN del ICC, se asignará una dirección IP diferente a las direcciones públicas de producción.

Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

- Prohibir el uso de bases de datos operativas o en producción. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
- Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
- Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

Punto de control: *Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.*

14 RELACIONES CON LOS PROVEEDORES

14.1 Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar la protección de los activos de la entidad que sean accesibles a los proveedores.

14.1.1 Política de seguridad de la información para la relación con proveedores.

Responsable del control: Proveedores externos, Grupo de Gestión Contractual y Grupo de Tecnologías de la Información (TI).

Todo proveedor debe cumplir con los lineamientos establecidos en la contratación pública y las políticas de seguridad de la información del ICC. El Grupo de Gestión Contractual a través de las cláusulas contractuales debe establecer los lineamientos para el cumplimiento de la política de seguridad y privacidad de la información, requisitos legales y regulatorios en todos los contratos con proveedores o terceros, incluyendo el reporte de fallas o incidentes que se presenten o evidencien en la ejecución de las actividades; las políticas relacionadas con la protección de datos personales, derechos de autor y propiedad intelectual.

Con el fin de proteger la información y teniendo en cuenta la información a la que tendrá acceso el tercero, se debe preparar y legalizar un acuerdo de confidencialidad entre la entidad y el tercero, conforme al objetivo y al alcance del contrato, el cual debe quedar firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información y con los objetivos de la entidad.

El Grupo de TI establecerá los requerimientos mínimos de seguridad, infraestructura y calidad de servicio, para la adquisición de servicios con terceros. Estos requisitos son fundamentales para llevar a cabo los procesos contractuales que se deriven de la necesidad de contratar servicios con terceros o desarrollos.

Punto de control: *Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad se deben acordar con estos y se deben documentar.*

14.1.2 Tratamiento de la seguridad dentro de los acuerdos con los proveedores

Responsable del control: Grupo de Gestión Contractual, Grupo de Tecnologías de la Información (TI) y Supervisores de contratos.

Los supervisores de contratos deben asegurar que se comuniquen las políticas y procedimientos de seguridad de la información a los proveedores y contratistas.

El Grupo de Gestión Contractual debe incluir en los acuerdos con proveedores y contratistas, los siguientes requisitos de seguridad de la información:

- Cláusula de confidencialidad incluyendo cláusulas que definan las responsabilidades que continúan después de terminado el contrato.
- Cumplimiento de las políticas de seguridad de la información del ICC.
- Reporte de eventos de seguridad de la información a través de los canales definidos en el procedimiento de gestión de incidentes de seguridad de la información.

Los supervisores de contratos deben administrar los cambios en el suministro de servicios contratados, manteniendo los niveles de cumplimiento de servicio, seguridad de la información establecidos con ellos y monitoreando la aparición de nuevos riesgos.

Punto de control: *Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la entidad.*

14.1.3 Cadena de suministro de tecnología de información y comunicación

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI realizará revisión de seguridad digital a la cadena de suministro de los proveedores que participan en la operación misional del Instituto, también deberá definir los requisitos de seguridad digital de la operación realizadas con terceras partes en lo referente a la adquisición de productos y servicios. Se debe garantizar la revisión periódica de los requisitos de seguridad de la cadena de suministro. Dentro de la revisión se contempla los componentes de hardware y software crítico para el desarrollo del servicio.

Para la contratación de servicios o componentes de la infraestructura de TI y/o áreas seguras, se debe exigir a los proveedores la presentación de los planes de continuidad de negocio que aseguren la disponibilidad de la información, suministrada y procesada entre las partes.

Punto de control: *Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.*

14.2 Gestión de la prestación de servicios de proveedores

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

14.2.1 Seguimiento y revisión de los servicios de los proveedores

Responsable del control: Supervisores de contratos.

Los proveedores deben dar cumplimiento a los Acuerdos de Nivel de Servicio (ANS) establecidos en el proceso de contratación. Se debe hacer un seguimiento al servicio y desempeño de los proveedores con base en los acuerdos de nivel de servicios establecido para validar los niveles de seguridad de la información acordados. La responsabilidad de la gestión y el seguimiento de la relación con los proveedores debe ser asignado a un funcionario o grupo de funcionarios que actuarán como supervisión de contrato.

Se debe tener control suficiente sobre todos los aspectos de seguridad de la información para las instalaciones de procesamiento de información a las que se tiene acceso, procesa o gestiona un proveedor.

Punto de control:
Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

14.2.2 Gestión de cambios en los servicios de los proveedores

Responsable del control: Grupo de gestión contractual
En los servicios establecidos con los proveedores se deben gestionar todos los cambios siguiendo el procedimiento definido por el ICC teniendo en cuenta los cambios en los acuerdos con el proveedor, los cambios requeridos por la Entidad y los cambios en los servicios del proveedor a implementar.
Los supervisores de contratos deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos y monitoreando la aparición de nuevos riesgos

Punto de control: *Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.*

15 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

15.1 Gestión de incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.

15.1.1 Responsabilidades y procedimientos

Responsable del control: Todos, Grupo de Tecnologías de la Información (TI) y Rol Oficial de Seguridad de la información.

Es deber de todos los servidores (as) públicos (as), contratistas o terceros, reportar cualquier posible evento o incidente que afecte la confidencialidad, privacidad, integridad o disponibilidad de los servicios tecnológicos, violaciones de acceso, acceso no autorizado y mal funcionamiento en el software o hardware del que se tenga conocimiento o experiencia directa, a través del correo: seguridaddigital@caroycuervo.gov.co. El funcionario o contratista que aproveche deficiencias de seguridad y haga mal uso de la información, será investigado por la instancia disciplinaria para establecer las sanciones que haya lugar.

La gestión del tratamiento de incidentes de seguridad de la información está a cargo del rol de oficial de seguridad de la información, para asegurar respuestas eficientes, documentar y mantener actualizada una gestión de conocimiento por los incidentes o eventos presentados. Así mismo tendrá la responsabilidad de proponer, solucionar e implementar controles necesarios para evitar su repetición. El Grupo de TI deberá estar a cargo de la atención de incidentes en la infraestructura tecnológica. Si es requerido, tanto el oficial de seguridad de la información, el CSIRT (Computer Security Incident Response) y el equipo de Respuesta a Incidentes de Seguridad de la Información de MINTIC realizarán acompañamiento a la solución de dicho incidente.

El Grupo de TI debe reportar a las autoridades competentes los incidentes de seguridad de información graves o los que afecten a la infraestructura de la Entidad, a través de los canales de gestión apropiados y debe documentar y comunicar, por los medios que considere necesario, las lecciones aprendidas de incidentes de seguridad de la información, con el fin de evitar recurrencias.

El Grupo de TI y el rol Oficial de seguridad de la información son los encargados para la recolección de evidencias de los incidentes de seguridad de información con el fin de presentar a las autoridades competentes en las investigaciones que sean necesarias.

El rol Oficial de seguridad de la información, deberá registrar y dar cierre formal a los incidentes de seguridad una vez gestionados por el mismo medio en que fue reportado.

El Grupo de TI establecerá un plan de continuidad de los servicios críticos de TI, para gestionar los incidentes durante o después de la materialización de un incidente de seguridad de la información.

El procedimiento de respuesta a incidentes de seguridad de la información debe:

- Establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollen y comuniquen adecuadamente dentro de la entidad; la planificación y preparación de respuesta a incidentes con las siguientes actividades:
    - Seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información.
    - Registro de las actividades de gestión de incidentes.
    - Manejo de evidencia forense.
    - Valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información.
    - Respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas.
- Establecer los procedimientos para asegurar que:
    - El personal maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la entidad.
    - Se implemente un punto de contacto para la detección y reporte de incidentes de seguridad mantener contactos apropiados con las autoridades.
    - Se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información.
- Definir el reporte de procedimientos debería incluir:
    - La preparación de formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información.
    - El procedimiento que se va a seguir en el caso de un evento de seguridad de la información (tomar nota inmediatamente de todos los detalles, tales como el tipo de no conformidad o violación, mal funcionamiento, mensajes en la pantalla y reporte inmediato al punto de contacto y realizar solamente acciones coordinadas).
    - Referencia a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad.
    - Los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.

Punto de control: *Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.*

15.1.2 Reporte de eventos de seguridad de la información

Responsable del control: Todos

El reporte de eventos que comprometan la gestión de datos personales, seguridad de la información es una actividad obligatoria para todos los funcionarios y contratistas asociados a los activos y servicios del ICC. Al presentarse un evento se debe notificar inmediatamente a través del correo: seguridaddigital@caroycuervo.gov.co.

El oficial de seguridad de la información debe velar por que los funcionarios y contratistas reciban capacitación para registro y/o reporte de eventos y debilidades de seguridad que comprometan la disponibilidad y/o integridad y/o confidencialidad de la información.

Punto de control: *Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.*

15.1.3 Reporte de debilidades de seguridad de la información

Responsable del control: Todos

Todos los funcionarios, contratistas o terceros deberán reportar a través del canal definido cualquier situación que se pueda considerar como una debilidad en la seguridad de la información. La debilidad en seguridad de la información puede describirse como la condición de un componente o sistema de software (sistema de información, aplicativo) que aumenta su susceptibilidad a las vulnerabilidades.

Punto de control: *Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la entidad, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.*

15.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

Responsable del control: Oficial de Seguridad de la Información.

Con base en la información reportada por funcionarios y contratistas del ICC, el oficial de Seguridad de la Información debe realizar el respectivo análisis para establecer la ocurrencia de un evento e incidente de seguridad de la información y la respectiva gestión de este. Cuando se detecte un evento o incidente en la seguridad de la información que puede culminar en una acción legal, se debe iniciar el tratamiento del incidente acorde al procedimiento Gestión de Incidentes del ICC.

Punto de control: *Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.*

15.1.5 Respuesta a incidentes de seguridad de la información

Responsable del control: Oficial de Seguridad de la Información.

Las respuestas de los incidentes de seguridad de la información deben contener por los menos:

a) Contar con un plan de recuperación de incidentes durante o después del mismo.
b) Recolectar evidencia lo más pronto posible después de que ocurra el incidente.
c) Llevar el asunto a una instancia superior, según se requiera.
d) Llevar a cabo análisis forense de seguridad de la información, según se requiera.
e) Registrar todas las actividades de respuesta involucradas para análisis posterior.
f) Comunicar la existencia del incidente a quien necesite saberlo (personal interno y externo).
g) Tratar las debilidades de seguridad de la información que se encontraron que causen o contribuyan al incidente.
h) Una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.
i) Para los incidentes cibernéticos, investigar las notificaciones de los sistemas de detección.

Punto de control: *Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.*

15.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

Responsable del control: Todos

Se debe documentar todo el manejo y gestión de incidentes con el fin de gestionar las lecciones aprendidas y así fortalecer los controles y lineamientos asociados.

Punto de control: *El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.*

15.1.7 Recolección de evidencia

Responsable del control: Rol Oficial de Seguridad de la Información.

Se debe mantener un repositorio centralizado sobre el manejo de los incidentes para poder analizarlos, prevenirlos y divulgar los conocimientos obtenidos, de modo que se esté preparado a futuro y de una mejor forma ante recurrencia de incidentes. Las evidencias de los incidentes de seguridad deben demostrar la calidad e integridad de los controles utilizados demostrando protección y consistencia durante todo el período de almacenamiento y procesamiento de la información. Para recolección de evidencia se debe:

- definir la cadena de custodia;

- establecer la seguridad de la evidencia;
- definir la seguridad del personal;
- definir los roles y responsabilidades del personal involucrado;
- establecer la competencia del personal;
- realizar la documentación;
- definir las sesiones informativas.

Punto de control: *La entidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.*

16 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

16.1 Continuidad de seguridad de la información

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la entidad.

16.1.1 Planificación de la continuidad de la seguridad de la información.

Responsable del control: Líderes de proceso y rol Oficial de Seguridad de la Información.

Se debe realizar la identificación de actividades críticas para el ICC, sobre los cuales se debe realizar un análisis de impacto al Negocio que servirá para la construcción y/o actualización del plan de continuidad.

El plan de continuidad debe ser documentado, probado y actualizado de forma periódica o cuando ocurra un evento que afecte la prestación u operación de los servicios del ICC, este documento debe ser conocido por el Grupo de TI y los responsables de los activos de información. Se debe generar documentación de las pruebas realizadas al plan de continuidad que incluya lecciones aprendidas y acciones de mejora, esta información debe ser acceso a los colaboradores interesados o participantes de las pruebas.

Punto de control: *La entidad debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.*

16.1.2 Implementación de la continuidad de la seguridad de la información.

Responsable del control: Rol Oficial de Seguridad de la Información.

Se requieren las siguientes directrices para la implementación de la continuidad de la seguridad de la información:

- Implementar una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.
- Implementar un comité formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.
- Tener planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como el ICC gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección.

Los supervisores de contratos deben solicitar a los proveedores de servicios críticos contar con planes de continuidad que permitan desarrollar pruebas periódicas de los mismos para conocer si son efectivos en caso de necesitarlos. El Grupo de TI deberá diseñar estrategias de recuperación de los servicios críticos de tecnología.

Punto de control: *La entidad debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.*

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

Responsable del control: Rol Oficial de Seguridad de la Información y Grupo de Tecnologías de la Información (TI).

Se deben realizar pruebas periódicas a los controles y procedimientos de continuidad de negocio y de continuidad de la Seguridad de la Información implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. El ICC debe establecer e implementar un Plan de Recuperación de Desastres (DRP) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.

El plan de recuperación tecnológica y el plan de continuidad del negocio deberán ser probados como mínimo una vez al año. Se debe establecer un programa de pruebas, teniendo en cuenta los requerimientos técnicos necesarios. Las pruebas deberán ejecutarse de manera que simule las condiciones de un evento y no se afecte la operación. Se debe definir un equipo para la planeación de pruebas, los procesos que estarán involucrados, la infraestructura tecnológica y/u operativa requerida, el plan de rollback y las actividades a realizar. Los participantes de los equipos deberán recibir sensibilización con respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.

El Grupo de TI deberá identificar los escenarios y las estrategias del plan de recuperación tecnológica (DRP) de los servicios esenciales de tecnología identificados.

Se deben realizar pruebas periódicas del DRP con el fin de asegurar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas. Las pruebas se deben documentar, generar reportes o informes después de cada prueba y/o ejercicio que incluya recomendaciones, lecciones aprendidas y acciones para mejorar el plan de recuperación tecnológica.

Punto de control: *La entidad debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.*

16.2 Redundancias

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información

16.2.1 Disponibilidad de las instalaciones de procesamiento de información.

Responsable del control: Grupo de Tecnologías de la Información (TI)

El Grupo de TI debe realizar las configuraciones de los servicios tecnológicos procurando asegurar la disponibilidad de servicio, implementar la infraestructura necesaria para contar con redundancia en los sistemas de información y servicios críticos del ICC y probar periódicamente las arquitecturas o servicios redundantes asegurando su operación luego de presentarse un evento.

La información que manejan los funcionarios y que hace parte de la misión funcional de la entidad, será respaldada en los servidores de archivos dispuestos para esto en cada una de las sedes, y así mismo cada uno de estos servidores realizará una réplica de los datos en la sede alterna, para mantener de esta manera un respaldo adicional fuera de las instalaciones donde se encuentran ubicados estos servidores.

Punto de control: *Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.*

17 CUMPLIMIENTO

17.1 Cumplimiento de requisitos legales y contractuales

Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

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

Responsable del control: Grupo de Gestión Contractual y Rol Jurídico.

El ICC debe contar con el documento de requisitos legales el cual debe estar documentado, actualizado y publicado.

Punto de control: *Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la entidad para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.*

17.1.2 Derechos de propiedad intelectual

Responsable del control: Grupo de Gestión Contractual, Rol Jurídico y Grupo de Tecnologías de la Información (TI).

El ICC es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por funcionarios y contratistas, derivadas del objeto del cumplimiento de funciones y obligaciones asignadas, como las necesarias para el cumplimiento del objeto del contrato en cumplimiento del Artículo 91 de la Ley No 23 de 1982 (28 de enero de 1982) “Sobre derechos de autor”.

El software es considerado una obra intelectual que goza de la protección de la ley. La ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción. El Grupo de TI, junto al Grupo de Gestión Contractual y el Rol Jurídico, analizarán los términos y condiciones de la licencia, e implementarán los siguientes controles:

a. Definir normas para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
b. Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las violen.
c. Mantener un adecuado registro de activos.
d. Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
e. Implementar controles para evitar el exceso del número máximo permitido de usuarios.
f. Verificar que solo se instalen productos con licencia y software autorizado.
g. Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
h. Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
i. Cumplir con los términos y condiciones establecidos para obtener software libre.

Los funcionarios y contratistas únicamente podrán utilizar sistemas de información autorizado por el Grupo de TI, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

No se permite el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal. Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de estos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas. La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar demandas penales.

El Grupo de Gestión Contractual debe incluir cláusulas de propiedad intelectual y derechos de autor en contratos de prestación de servicios y con terceros que protejan el software, documentos, derechos de diseño, marcas registradas, patentes y códigos fuente.

Punto de control: *Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.*

17.1.3 Protección de registros

Responsable del control: Grupo de Gestión documental y Grupo de Tecnologías de la Información (TI).

Los registros de la entidad se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del ICC. Es por ello, que se deben mantener actualizadas las tablas de retención documental TRD para la información física y digital por parte del Grupo de Gestión Documental.

El ICC se obliga a proteger todos los registros evitando la pérdida de confidencialidad, integridad y disponibilidad de la información.

Punto de control: *Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.*

17.1.4 Privacidad y protección de información de datos personales

Responsable del control: Rol Jurídico, Rol Oficial de Seguridad de la Información, Rol Oficial de Datos, Líderes de Procesos, Grupo de Recursos físicos y Grupo de Tecnologías de la Información (TI).

El ICC debe documentar una política de tratamiento de datos personales, la cual debe ser publicada en el portal WEB institucional indicando a los titulares las finalidades específicas por las cuales se hace la recolección de sus datos.

Toda dependencia o grupo que por su naturaleza genere información impresa y física de los ciudadanos, funcionarios y contratistas catalogada como sensible de acuerdo con la Ley 1581 de 2012, debe abstenerse de reutilizar este papel como reciclable y a su vez debe garantizar la destrucción de estos documentos cuando ya no sean requeridos para ningún proceso y trámite.

Toda dependencia, servicio tecnológico o sistema de información que recolecte información personal de ciudadanos, funcionarios y terceros, debe solicitar al titular de los datos de forma previa la autorización de tratamiento de sus datos personales. Estas autorizaciones se deben guardar y estar disponibles para cuando sean requeridas en un repositorio con acceso al personal autorizado. El Grupo de TI debe adoptar las medidas técnicas necesarias para proteger las bases de datos donde reposan los datos personales recolectados.

Las zonas de videovigilancia deben contar con un aviso de privacidad que indique a los usuarios que ingresen a las instalaciones del ICC, que están siendo grabados y monitoreados por razones de seguridad. Para este caso se entiende que el usuario que ingrese a las instalaciones del ICC acepta el registro de su imagen de acuerdo con lo indicado en la política de tratamiento de datos personales.

Punto de control: *Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.*

17.1.5 Reglamentación de controles criptográficos.

Responsable del control: Grupo de Tecnologías de la Información (TI).

El ICC se regirá por la Ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y otras disposiciones” y sus decretos reglamentarios, según aplique.

Punto de control: *Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.*

17.2 Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.

17.2.1 Revisión independiente de la seguridad de la información

Responsable del control: Unidad de Control Interno, Rol Oficial de Seguridad de la Información y Grupo de Tecnologías de la Información (TI).

La Unidad de Control Interno debe realizar auditorías internas verificando la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), así como el cumplimiento de políticas, procedimientos y controles generados. El Rol oficial de seguridad de la información se encuentra facultado para hacer las respectivas revisiones e inspecciones al cumplimiento de los lineamientos establecidos por el sistema de gestión de seguridad de la información.

La revisión independiente de la seguridad de la información deberá realizarse al menos una vez al año. El desarrollo de estas revisiones debe ser comunicado a funcionarios, contratistas y demás partes interesadas utilizando los medios que se considere pertinentes para garantizar su divulgación.

Punto de control: *El enfoque de la entidad para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.*

17.2.2 Cumplimiento con las políticas y normas de seguridad

Responsable del control: Todos, Lideres de Procesos y Rol Oficial de Seguridad de la Información.

Los líderes de los procesos deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas de seguridad de la información y comunicación a la instancia disciplinaria.

El Rol oficial de Seguridad de la Información debe realizar revisiones mínimo una vez al año del cumplimiento de las políticas de Seguridad y Privacidad de la Información a través del cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).

Es un deber de los servidores púbicos contratistas y terceros del ICC, conocer esta Política y realizar todos los actos conducentes para su cumplimiento, implementación y mantenimiento.

Punto de control: *Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.*

17.2.3 Revisión del cumplimiento técnico

Responsable del control: Grupo de Tecnologías de la Información (TI).

El Grupo de TI debe coordinar la revisión de los sistemas de información, los servicios y la infraestructura tecnológica. Las pruebas técnicas que se deberán incluir pueden ser: pruebas de penetración, análisis de vulnerabilidades, ethical hacking; para determinar el cumplimiento de los controles técnicos de seguridad de la información. Se deben listar los sistemas de información a los que se les hará revisión técnica y conservar los registros resultantes de la revisión realizada.

Punto de control: *Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.*

18 ACTUALIZACION

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, el Grupo de Planeación y Relacionamiento con el Ciudadano se reserva el derecho a modificar esta política cuando sea necesario.

En todo caso, los cambios realizados en esta política serán publicados a funcionarios, contratistas y terceros del ICC.

Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de las Políticas de Seguridad contempladas en este documento.

19 DISPOSICIONES

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su aprobación y difusión.

Las normas y políticas, objeto de este documento, podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando. Una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

La falta de conocimiento de las normas aquí descritas por parte de los funcionarios, contratistas o terceros no los libera de la aplicación de sanciones por el incumplimiento de estas.

20 REQUISITOS LEGALES Y NORMATIVIDAD

Los requisitos legales que soportan el presente manual son los siguientes:

- **Gobierno Digital:** El objetivo de la política de Gobierno Digital es: "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital" a través de los habilitadores transversales entre ellos seguridad y privacidad que busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.
- **ISO/IEC 27001:2013:** Esta norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización.
- **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 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 1499 de 2017:** Actualiza el Modelo Integrado de Planeación y Gestión (MIPG).
- **Decreto 1008 de 2018:** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1078 de 2015:** Decreta la estructura del sector de tecnologías de la información y las comunicaciones.
- **CONPES 3854 de 2016** Política Nacional de Seguridad digital. Se crean las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital.
- **CONPES 3701 de 2015** Lineamientos de políticas para ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.