MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESO

Gestión Estratégica de Tecnologías de la Información

Versión 1

03/02/2023

MADSIG
Sistema Integrado de Gestión

TABLA DE CONTENIDO

INTRODUCCION

El propósito de un sistema de gestión de seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la Entidad de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno, las tecnologías y que la continuidad del servicio sea asegurada; de igual forma, permite reducir costos, entre otras razones, por la racionalización de recursos, la reducción de riesgos de seguridad de la información, la reducción de la probabilidad y el impacto de los incidentes de seguridad, el cual permite focalizar el gasto descartando inversiones innecesarias, proporcionando aumento de la seguridad con base en la gestión de procesos en lugar de la compra sistemática de productos y tecnologías, además de asegurar la continuidad de la misionalidad de la Entidad.

En este contexto el Ministerio de Ambiente y Desarrollo Sostenible, en adelante Ministerio, debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, a través de un proceso integrado que permita asegurar su cumplimiento e interiorización entre los procesos de la Entidad, asociados a la seguridad de la información, continuidad del negocio, adquisición, desarrollo e implantación de sistemas de información, acceso a la tecnología y uso de las facilidades hacia los usuarios, alineado al Modelo Integrado de Planeación y Gestión conforme a lo relacionado en el Decreto 1499 de 2017 que establece el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión Institucional a través de las políticas de gestión y desempeño, como habilitador transversal de los componentes de la política de gobierno digital, que busca que las Entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos, por medio de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) y alcanzar sus objetivos estratégicos, basados en un enfoque de gestión y de mejora continua, donde se establezcan un conjunto de políticas específicas, que son el soporte de la Política General de Seguridad y Privacidad de la Información adoptada al interior de la Entidad.

Ahora bien, teniendo en cuenta lo antes expuesto, el presente manual se encuentra enmarcado por un conjunto de políticas específicas, las cuales soportan la política general de seguridad y privacidad de la información adoptada al interior de la Entidad. Para esto todas las partes interesadas que tienen responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del Ministerio deben adoptar las políticas y directrices contenidas en el presente manual, así como los

documentos que se encuentren relacionados con él, buscando así asegurar la confidencialidad, integridad y disponibilidad de la información.

1. OBJETIVO DE LA SEGURIDAD DE LA INFORMACION

Establecer los lineamientos correspondientes a las políticas específicas de seguridad y privacidad de la información del Ministerio, que permita proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad, las cuales se deberán conocer y acoger por las partes interesadas de la Entidad conforme a los requisitos legales vigentes.

1.1 Objetivos Específicos

- Establecer políticas específicas para proteger la confidencialidad, integridad y disponibilidad de la información de la Ministerio.
- Socializar a través de este documento las políticas específicas y lineamientos de seguridad de la Información aplicables al Ministerio.
- Crear una cultura de aseguramiento de los activos de información en el Ministerio a través de ejercicios de socialización y capacitación de las políticas y lineamientos definidos en este manual.
- Definir lineamientos de Seguridad de la Información por medio de su implementación promoviendo la mejora continua.
- Orientar a los funcionarios y dependencias sobre las definiciones de política, lineamientos y demás controles de seguridad establecidos en el Ministerio.

2. ALCANCE DEL MANUAL

Las presentes políticas de seguridad de la información son aplicables a la protección de los activos de información del Ministerio ubicados en la sede de Bogotá Calle 37 No. 8 – 40 e incluye todos los procesos de la Entidad, así como todas las partes interesadas que tienen responsabilidad sobre los mismos.

Adicionalmente se incluyen lineamientos de Seguridad de la información para los activos que se encuentran alojados en la nube y también para las actividades de desarrollo de software ejecutadas por terceros.

Este documento se deberá revisar y ajustar en periodos no superiores a un año o cuando en la Entidad surjan cambios que ameriten ajustes puntuales a las definiciones contenidas en este.

3. MARCO LEGAL

- **Resolución 500 de 2021**, *"por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".*
  https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf.

- **Directiva Presidencial 02 Del 24 De febrero De 2022,** "Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)"
  https://www.asocapitales.co/nueva/2022/02/25/directiva-presidencial-02-del-24-de-febrero-de-2022/
- **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.
  https://www.suin- juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699
- **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 se dictan otras disposiciones.
  https://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013
- **CONPES 3854 de 2016 Política** Nacional de Seguridad Nacional busca fortalecer, identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.
  https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.
- **CONPES 3995 de 2020** - Política Nacional De Confianza y Seguridad Digital "Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías"
  https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf
- **Norma técnica colombiana 27001 de 2013** Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).
  https://serviciocivil.gov.co/sites/default/files/marco-legal/2006_03_22_NTC-ISO-IEC%2027001.pdf
- **El Modelo de Seguridad y Privacidad de la Información** – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la **privacidad** de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas.
  https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- **Ley 1581 de 2012**, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
  https://www.sic.gov.co/preguntas-frecuentes-pdp
- **Decreto 338 de 2022,** establece los lineamientos generales para la gobernanza de seguridad digital, con el cual busca aunar y dinamizar el desarrollo legal, los avances técnicos, así como los conocimientos estatales y privados para fortalecer la ciberseguridad del país.
  https://www.leyex.info/documents/leyes/601be1dc32bb1a2ee789f230cc6048df.htm
- **Resolución 1519 del 2020, "**Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
  https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Resolucion/30044657
- **Lineamientos de Mintic,** Modelo de Seguridad y Privacidad de la Información 3.0.2 29/07/2016
  https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
- **DAFP,** Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020
- file:///C:/Users/USER/Downloads/Guía%20para%20la%20administración%20del%20riesgo%20y%20el%20diseño%20de%20controles%20en%20entidades

4. MARCO CONCEPTUAL

4.1 Términos y Definiciones

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la Entidad. (ISO/IEC 27000).
- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada Entidad, órgano u organismo. (CONPES 3854 de 20116).
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y

que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos 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 o 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. (Decreto 1377 de 2013, art 3)
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **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. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella 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. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** Es aquella 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. (Ley 1712 de 2014, art 6)

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **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. (Ley 1581 de 2012, art. 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de datos personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **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. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- **Partes interesadas (Stakeholder):** Persona o Entidad que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

OBJETIVO DE ESTE MANUAL

Definir, por parte del Comité Institucional de Gestión y Desempeño, lineamientos basados en buenas prácticas de seguridad de la información y seguridad digital de acuerdo con los requisitos del Ministerio y con las leyes y reglamentos vigentes.

5. POLITICAS DE SEGURIDAD

5.1. Directrices Establecidas Por la Dirección Para la Seguridad de la Información

Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información, de acuerdo con los requisitos del negocio, los reglamentos y las leyes pertinentes.

5.1.1 Políticas para la seguridad de la información

Control: Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

- En cumplimiento de su objeto misional, el cual es definir la política Nacional Ambiental y promover la recuperación, conservación, protección, ordenamiento, manejo, uso y aprovechamiento de los recursos naturales renovables, al fin de asegurar el desarrollo sostenible y garantizar el derecho de todos los ciudadanos a gozar y heredar de un ambiente sano; el Ministerio se compromete a definir y establecer un Sistema de Gestión de la Seguridad de la Información para garantizar los requerimientos de las partes interesadas, haciendo un uso eficiente de sus recursos y preservar la confidencialidad, integridad y disponibilidad de la información, bajo un enfoque de prevención de riesgos, mejora continua y autocontrol en los procesos y en la prestación de los servicios, con el apoyo de un equipo humano competente y comprometido.

5.1.2 Revisión de las políticas para seguridad de la información

Control: La verificación y revisión de las políticas específicas de seguridad de la información que se encuentran en este documento se deben revisar por lo menos una vez al año o cuando ocurran cambios en la Entidad o en el entorno legal de la misma.

- El Ministerio debe revisar el manual de políticas de seguridad de la información al menos una vez al año o cuando surjan cambios relevantes, de mejora y de cumplimiento al Sistema de Gestión de Seguridad de la Información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION

6.1 Organización Interna de la Entidad interna

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la Entidad.

6.1.1 Roles y responsabilidades para la seguridad de información

Control: Definir y asignar todas las responsabilidades de la seguridad de la información

- Se deben y asignar roles y responsabilidades de acuerdo con la matriz Roles y Responsabilidades. (Consultar anexo).
- Los funcionarios, contratistas, colaboradores y terceros que tenga acceso a la información del Ministerio, son responsables de cumplir las políticas de seguridad de la información descritas en este manual.
- El Oficial de Seguridad de la Información o quien haga sus veces, debe asumir la responsabilidad en el desarrollo e implementación del SGSI, de acuerdo con las responsabilidades definidas.
- El comité Institucional de Gestión y Desempeño asumirá las responsabilidades respecto a la seguridad de la información definidas en la Resolución 2140 de 2017.
- La OTIC es líder de la implementación y gestión de los Controles tecnológicos que afecten sistemas de información, aplicaciones, plataformas de apoyo o infraestructura de comunicaciones y seguridad del Ministerio.
- Los Propietarios de los Activos de Información, son responsables de establecer la identificación, valoración de los activos, clasificación y respectivo etiquetado teniendo en cuenta la metodología de clasificación de la información, igualmente definir el nivel de protección requerido ante accesos no autorizados, pérdida de la confidencialidad, integridad o disponibilidad. Mantener actualizado el inventario de activos de información, validando los controles de acceso asignados a los activos; identificando riesgos asociados con la Seguridad de la Información en los procesos de los cuales son responsables o tienen participación y reportar oportunamente eventos o incidentes de Seguridad de la Información.

6.1.2 Separación de deberes

Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la Entidad.

- El Ministerio debe garantizar que en todos los sistemas de información se implementen controles de acceso, de tal forma que haya segregación de funciones entre quien administre, utilice, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información.

6.1.3 Contacto con las autoridades

Control: Establecer contacto con las siguientes autoridades:

- El Ministerio debe mantener contacto actualizado con las autoridades competentes para el cumplimiento de la Ley; como los organismos de control

ENTIDAD	CONTACTO
Fiscalía General de la Nación	https://sicecon.fiscalia.gov.co/denuncia/ingresoPrincipal
Policía Nacional	https://caivirtual.policia.gov.co/
CSIRT de Gobierno	Csirtgob@mintic.gov.co • 01 8000 910742 Opción 3

6.1.4 Contacto con grupos de interés especial

Control: Mantener contactos con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

- El Ministerio a través de la OTIC debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información, con el fin de mantenerse actualizado en relación con la información de seguridad.

6.1.5 Seguridad de la información en la gestión de proyectos

Control: Aplicar lineamientos de seguridad de la información de proyectos del Ministerio.

- El Ministerio debe establecer los lineamientos de seguridad de la información para el desarrollo de proyectos de acuerdo con el documento **DS-E-GET-26 V1 – POLITICA PARA EL DESARROLLO DE PROYECTOS.**

6.2 Dispositivos móviles y teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

6.2.1 Política para dispositivos móviles

Control: El Ministerio adopta una política para uso de dispositivos móviles.

- Todos los funcionarios y colaboradores del Ministerio que accedan a información la esta Entidad con dispositivos móviles, deben implementar controles de acceso, técnicas criptográficas para cifrar la información crítica o sensible almacenada en estos dispositivos, y los demás controles que se consideren necesarios para permitirles garantizar la confidencialidad, integridad y disponibilidad de la información.
- El funcionario o colaborador es responsable de su dispositivo móvil y no debe descuidar en ningún momento su equipo, al igual que por seguridad deberá activar las opciones de desbloqueo por código de acceso o huella.

- El funcionario o colaborador debe navegar responsablemente por Internet de acuerdo con las políticas y lineamientos de seguridad de la información y de TI.
- Los dispositivos móviles no se deben conectar a puertos USB o estaciones de carga desconocidas.
- No mantener activas las opciones de conexión inalámbricas que no vayan a ser utilizadas.
- No conectarse a redes Wi-Fi públicas.
- Usar las contraseñas de acceso asignadas para los sistemas de información aplicando los lineamientos para generación de contraseñas.
- No se debe descargar ni almacenar información de tipo reservada o clasificada en el dispositivo móvil.
- Los funcionarios y colaboradores deben participar en las campañas de concientización sobre temas de riesgos, seguridad de la información, adelantadas por la Entidad.
- No compartir sus contraseñas con otras personas, ni dejarlas en lugares visibles de fácil acceso.
- Permitir los procesos de actualización de aplicaciones y sistema operativo de acuerdo con los lineamientos estipulados.

6.2.2 Teletrabajo

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

- El Ministerio establece a continuación lineamientos de seguridad de la información para ser aplicados en la modalidad de trabajo adoptada por la Entidad según la **Resolución de Teletrabajo 404 de marzo 8 de 2016 Adopción del Teletrabajo en Ministerio de Ambiente y Desarrollo Sostenible.**
- El Ministerio debe proveer a los funcionarios que estén en modalidad de teletrabajo los mecanismos de seguridad de la información, y lineamientos con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.
- Informar y dar una copia al Teletrabajador de los lineamientos de seguridad de la información establecidos por el Ministerio.
- El funcionario que esté ejecutando sus funciones a través de teletrabajo se compromete a cumplir con las medidas de seguridad que el Ministerio ha adoptado para asegurar la confidencialidad, disponibilidad e integridad de los activos de información.
- El teletrabajador no debe ceder en ningún caso a terceras personas la información a la que tenga acceso, ni verbal, ni escrito o digital.
- Monitorear las actividades de los teletrabajadore para proteger la confidencialidad, integridad y disponibilidad de la información del Ministerio.

- La Entidad debe proveer enlaces de comunicación seguros (VPN) para el acceso de los teletrabajadores.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

7.1 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.

7.1.1 Selección

Control: El Ministerio adelanta la verificación de los antecedentes de todos los candidatos que se van a vincular de acuerdo con las leyes, reglamentos y definiciones establecidos en el proceso de vinculación.

- El Ministerio establece medidas y lineamientos para asegurar que a todos los servidores públicos se les aplique los controles de seguridad de la información definidos en el proceso de ingreso y se les presente las responsabilidades en seguridad de la información durante el proceso de inducción.
- Los servidores públicos que se vinculen al Ministerio son seleccionados de acuerdo con los requisitos del manual específico de funciones de la Entidad y según los requerimientos específicos para la seguridad de la información definidos.
- Al momento de la vinculación, el proceso de talento humano también realizará la inducción a los empleados y contratistas en los siguientes temas:
    - Políticas de seguridad de la información
    - Objetivos de seguridad de la información
    - Lineamientos de seguridad de la información.

7.1.2 Términos y condiciones del empleo

Control: Acuerdos de confidencialidad para funcionarios y contratistas.

- El Ministerio debe establecer acuerdos de confidencialidad para funcionarios y contratistas que se vinculan a la Entidad.

7.2 Durante la ejecución del empleo

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

7.2.1 Responsabilidades de la dirección

Control: El Ministerio exigirá a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y lineamientos establecidos.

- El Ministerio debe establecer los mecanismos para verificar el cumplimiento de las políticas de seguridad de la información por parte de funcionarios y contratistas.

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

Control: Todos los funcionarios del Ministerio y contratistas deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo

- Se debe definir y ejecutar un plan de capacitación y sensibilización en relación con la seguridad de la información, articulado con el plan institucional de capacitación PIC.
- El proceso de talento humano, con el apoyo del responsable de seguridad de la Información y en coordinación con el Grupo del sistema Integrado de Gestión, debe incluir lo pertinente del tema de seguridad de la información en el plan de capacitación anual y será divulgado a los empleados y contratistas de la Entidad.
- Los servidores públicos deben conocer la normativa relacionada con la seguridad de la información del Ministerio ya que el desconocimiento de la misma no los exonerará de los procesos disciplinarios definidos ante violaciones de las políticas de seguridad.
- Se debe evaluar la efectividad de la capacitación y sensibilización en seguridad de la información desarrollada.
- Los incidentes de seguridad deben ser reportados al oficial o líder de seguridad de la información o quien haga sus veces. Cuando en un incidente de seguridad de la información se determine un grado de culpabilidad o responsabilidad por parte de los empleados y contratistas, la Entidad tomará las acciones pertinentes.

7.2.3 Proceso disciplinario

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

- El Ministerio a través de la oficina de Control Interno Disciplinario emprenderá acciones contra empleados que hayan cometido una violación a la seguridad de la información.
- Cuando exista una violación de seguridad de la información que involucre a un funcionario del Ministerio se abrirá un proceso disciplinario como consecuencia del análisis y tratamiento de seguridad de la información.

7.3 Terminación o cambio de empleo

Objetivo: Proteger los intereses de la Entidad como parte del proceso de cambio o terminación del contrato.

7.3.1 Terminación o cambio de responsabilidades de empleo

Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

- Para la terminación del empleo se debe establecer dentro del paz y salvo firmado por las áreas correspondientes, evidencia de que se retiraron accesos lógicos sobre la infraestructura tecnológica y físicos de acuerdo con los procedimientos de control de acceso.
- Tener registro o acta firmada por el jefe inmediato donde se asegura de la transferencia apropiada de información al sucesor del cargo e informe de gestión que indica el estado de las actividades realizadas.
- Los cambios de funciones en los servidores públicos deben estar guiados por procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, y la posterior entrega de estos (activos) de acuerdo con su nuevo rol.
- El grupo de talento humano y grupo de contratos del Ministerio informarán a la OTIC la aplicación de gestión de servicios, los retiros del personal y las novedades administrativas, para el bloqueo o eliminación de datos de acceso y cuentas de correo.
- En casos de desvinculación de un funcionario o contratista, el aviso de retiro por parte del grupo de talento humano o grupo de contratos debe ser inmediato.

8. GESTIÓN DE ACTIVOS

8.1 Responsabilidad por los activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

8.1.1 Inventario de activos

Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos

- El Ministerio debe diseñar e implementar una guía metodológica para la identificación y clasificación de activos de información.

- Se debe realizar el inventario con personal idóneo y competente de todos los activos asociados con la información en los diferentes procesos.
- Es responsabilidad del dueño de los activos de información, clasificarlos debidamente y propender por la aplicación de los lineamientos definidos en la **GUÍA METODOLÓGICA PARA LA IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN G-A-GTI-03**.
- Una vez aprobados los activos de información se deben oficializar ante la oficina TIC.

8.1.2 Propiedad de los activos

Control: Los activos mantenidos en el inventario deben tener un propietario.

- Los lideres de los procesos serán los propietarios de los activos de información.
- Cada proceso debe ser responsables de mantener actualizado el inventario de activos de información y el líder del proceso aprobará y reportará su actualización.

8.1.3 Uso aceptable de los activos

Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

- La información, archivos físicos, sistemas, servicios y los equipos son activos de la Entidad y se proporcionan a los funcionarios, contratistas y terceros autorizados para cumplir los propósitos del negocio.
- Todos los funcionarios y contratistas deben etiquetar la información y darle el uso adecuado según su clasificación, siguiendo las directrices de la ley 1712 del 2014 “Estatuto por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional “.
- Los funcionarios, Contratistas, Proveedores y terceros que tengan información del Ministerio deben reportar eventos de seguridad de la información de acuerdo con el procedimiento de incidentes **PROCEDIMIENTO GESTIÓN DE INCIDENTES DE LA INFORMACIÓN P-A-GTI-09**
- Está prohibido que funcionarios, contratistas, proveedores o terceros ajenos a la oficina TIC destapen o retiren partes de los equipos de cómputo del Ministerio.
- La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad de la OTIC por lo tanto se debe solicitar a soporte de tecnología, la realización de estas actividades.
- Los equipos de cómputo no deben ser traslados del sitio asignado inicialmente, ni cambiar el funcionario al que le fue asignado sin su respectiva autorización y gestión por parte de la OTIC.

- No se puede realizar ningún tipo de configuración, ni modificación de hardware ni software respetando lo establecido por la OTIC.
- No se autoriza el uso de medios extraíbles para almacenamiento de información institucional (USB, Celulares, Memory Card, discos de almacenamiento etc.) en las estaciones de trabajo de la Entidad, con excepción para aquellos funcionarios que, por sus funciones y actividades propias institucionales, sean autorizados.
- Toda actividad informática como, escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc., no autorizada que afecte tanto las redes corporativas como los sistemas de información del Ministerio, están prohibidas dando lugar a los procesos disciplinarios y legales correspondientes.
- Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados (tomas naranjas que son de uso exclusivo para equipos de cómputo), con el fin de evitar picos de voltaje que puedan dañar el componente tecnológico.
- La seguridad física de equipos de cómputo que ingresen a las instalaciones del ministerio que no son propiedad del Ministerio son responsabilidad exclusiva de su propietario.

8.1.4 Devolución de activos

Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la Entidad que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

- Todo funcionario, contratista debe gestionar la devolución de sus activos físicos que tiene a su cargo al terminar su empleo o contrato, gestionando el **Formato Legalización retiro del servicio código F-A-ATH-06**
- Es deber de todo funcionario, contratista que labore con el Ministerio, al dejar de prestar sus servicios, entregar toda información producto del trabajo realizado, gestionando **Formato Legalización retiro del servicio código F-A-ATH-06.**

8.2 Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.

8.2.1 Clasificación de la información

Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

- El dueño de los activos de información debe clasificar estos activos teniendo en cuenta la **GUIA METODOLÓGICA PARA LA IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN G-A-GTI-03 y el formato F-A- GTI-04.**
- El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que el activo está inventariado en la Matriz de Activos de Información o informar al Oficial de Seguridad de la Información para su debido registro.
- El funcionario, contratista, proveedor o tercero responsable del activo de información debe asegurarse de que los activos están clasificados y protegidos apropiadamente.

8.2.2 Etiquetado de la información

Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la Entidad.

- El dueño de los activos de información debe etiquetar los activos teniendo en cuenta el Procedimiento de **CLASIFICACIÓN, MANEJO Y ETIQUETEADO DE LA INFORMACIÓN Código: P-A-GTI-07**

8.2.3 Manejo de activos

Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la Entidad.

Aplicar el procedimiento **CLASIFICACIÓN, MANEJO Y ETIQUETEADO DE LA INFORMACIÓN Código: P-A-GTI-07**, y teniendo en cuenta la **GUÍA METODOLÓGICA PARA LA IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN G-A-GTI-03.** Considerando:

- 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 temporales o permanentes de información 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.
- Identificación de las copias de medios para el cuidado del receptor autorizado.

8.3 Manejo de Medios

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

8.3.1 Gestión de medios removibles

Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la Entidad.

- El uso de medios removibles solamente es autorizado por el dueño del activo de Información; el cual deberá realizar un análisis de riesgos. Dicha autorización debe tener una justificación de la necesidad por parte de la persona que hace la solicitud.
- El manejo de la información del Ministerio en medios removibles está expuesta a riesgos, como pérdida, fuga o modificación, los cuales comprometen no solamente la información sino también la infraestructura tecnológica de la Entidad, por lo tanto, el dueño del activo que autorice su uso y el autorizado será quien asuma las sanciones de ley aplicables en esta materia, siendo responsable de la seguridad de uso de la información en estos medios.
- No está permitido el almacenamiento de información clasificada como reservada o clasificada en medios removibles, en caso de requerirse por necesidad la información contenida en este medio deberá cifrase y protegerse por medio de claves de acceso.
- Las personas autorizadas para el uso de medios removibles son responsables de no utilizar los mismos en dispositivos externos a la Entidad que puedan configurar un riesgo para la misma.
- Se debe borrar o eliminar toda información que no se requiera o no sea útil en los medios removibles, de tal forma que no pueda ser restaurada o reconstruida teniendo en cuenta lo establecido en el documento **G-A-GTI-04 BORRADO SEGURO** del Ministerio.
- Todos los medios deben ser almacenados en un ambiente seguro de acuerdo con las especificaciones de los fabricantes.
- Todos los datos almacenados en medios removibles deben ser evaluados con base en los lineamientos y políticas definidas en el inventario de activos de información, de acuerdo con su clasificación.
- El control de medios removibles estará a cargo del dueño del activo de información quien solicitará la OTIC los accesos y uso de puertos y mecanismos necesarios para el uso de estos.

8.3.2 Disposición de los medios

Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.

- Se debe borrar o eliminar toda información que no se requiera o no sea útil en los medios removibles, de tal forma que no pueda ser restaurada o reconstruida teniendo en cuenta lo establecido en el documento **G-A-GTI-04_V3 Borrado Seguro** de la Entidad.
- Todo funcionario, contratista o cualquier tercero que tenga acceso a la información deberá seguir el debido proceso de solicitud de borrado por medio de la plataforma de gestión de servicios, donde deberá realizar una solicitud formal especificando el objeto de la misma.

- El proceso de borrado seguro o baja de equipos se aplicará a todo tipo de activos destinados al almacenamiento de la información; para realizar este procedimiento se puede validar la guía **G-A-GTI-04_V3 Borrado Seguro.**
- En caso de que estos activos vayan a ser reutilizados o liberados a otra área o Entidad deben ser objeto de borrado seguro. En caso que este activo no se le pueda ejecutar este tipo de proceso será el área encargada o generadora de la información quien definirá si debe ser destruido.
- El dueño del activo de la información deberá evaluar si es viable la destrucción de la información tomando como guía los decretos, leyes y otra normativa vigente.
- La persona encargada de realizar dicho proceso deberá generar un reporte donde se evidencie quién estuvo a cargo del procedimiento.
- El área encargada de realizar el proceso de borrado seguro de equipos deberá enviar un informe donde se evidencie si se han realizado o no los procedimientos de borrado seguro en los activos a su cargo.

8.3.3 Transferencia de medios físicos

Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

- Se debe definir un procedimiento de intercambio seguro de información física o digital.
- Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se debe especificar la clasificación de la información y las consideraciones de seguridad sobre la misma.
- Verificar que el proveedor del transporte o de los servicios de mensajería realice un adecuado embalaje para proteger el contenido del medio de información física.
- Validar la idoneidad de los funcionarios del servicio de mensajería, como acuerdos de confidencialidad y estudios de seguridad.
- Los prestadores de servicio de mensajería deben garantizar el cumplimiento en los lineamientos definidos en el procedimiento de intercambio de información seguro

9. CONTROL DE ACCESO

9.1 Requisitos del negocio para control de acceso

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

9.1.1 Política de control de acceso

Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

- El Ministerio debe definir una política que determina los criterios para establecer quien accede a la información de la Entidad, así como la implementación de los controles necesarios para el acceso a la infraestructura tecnológica como son: redes, correo, internet, sistemas de información, información digital o física y de esta manera proteger la confidencialidad, integridad y disponibilidad de la información.
- Se debe establecer revisar y documentar la política de control de acceso periódicamente.

9.1.2 Acceso a redes y a servicios en red

Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

- Se debe establecer un procedimiento de entrega de usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red de la Entidad, a los recursos de la plataforma tecnológica o a los sistemas de información.
- Todos los usuarios con acceso a un sistema de información o a la red informática de la Entidad dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña, serán responsables de las acciones realizadas por el usuario que les ha sido asignado.
- Todo equipo conectado a la red tendrá acceso a través de la dirección MAC definida.
- Se deben establecer mecanismos de auditoria al personal encargado de la administración del acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información.

9.2 Gestión de acceso de usuarios

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

9.2.1 Registro y cancelación del registro de usuarios

Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

- Se deben realizar revisiones periódicas en los diferentes sistemas de información, aplicaciones y demás herramientas tecnológicas de la Entidad, para garantizar que los usuarios que ya no están vinculados y se encuentren en estado inactivo o deshabilitados, en relación con las novedades del personal de acuerdo con lo reportado por el grupo de talento humano y grupo de contratos.

- Se deben bloquear de manera inmediata los privilegios de acceso físico a las instalaciones de Ministerio inmediatamente el colaborador que ya no tenga ningún tipo de vinculación con la Entidad.
- Se debe realizar la devolución del carné institucional y todos aquellos elementos asignados una vez que se termine su vinculación con la Entidad para poder entregar el respectivo paz y salvo.
- Los administradores de cada uno de los sistemas de información, aplicaciones y demás herramientas tecnológicas serán responsables de crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos y demás recursos tecnológicos cuando esto sea solicitado por el jefe de área o dependencia mediante la herramienta de gestión de servicios de TI.
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos de propiedad del Ministerio asignados al funcionario o contratista cuando las actividades finalicen.

9.2.2 Suministro de acceso de usuarios

Control: Se debería 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.

- Se debe controlar el uso de la información para garantizar y prevenir los accesos no autorizados; así como la asignación mínima de privilegios. El acceso a la información del Ministerio deberá ser otorgado sólo a usuarios autorizados, los permisos y niveles de acceso deben estar basados en concordancia a lo que sea requerido de acuerdo con la necesidad expresa para la realización de las tareas relacionadas bajo su responsabilidad.
- La asignación de privilegios a las soluciones tecnológicas presentes en el Ministerio debe ser solicitada por el líder de proceso o jefe inmediato del área solicitante a OTIC para que se realicen las asignaciones de privilegios necesarias.
- Para generar acceso tanto físico como lógico a contratistas o proveedores, el supervisor del contrato o quien haga sus veces debe realizar la solicitud al área respectiva.
- Se debe verificar, controlar y restringir los accesos físicos y lógicos de los servidores públicos, contratistas o terceros que de alguna manera terminan la vinculación laboral con la Entidad; y deberán diligenciar en su totalidad el formato **F-A-ATH-06 Control de Legalización Retiro del Servicio.**

9.2.3 Gestión de derechos de acceso privilegiado

Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.

- Se debe realizar la revisión de los privilegios de acceso a los sistemas de información, aplicaciones entre otras al menos una vez al año.
- Funcionarios, contratistas y proveedores que tengan algún vínculo con la Entidad deberán hacerse responsables de los usuarios y contraseñas asignados para el acceso a los servicios que están en la red, los recursos de la plataforma tecnológica y los sistemas de información.
- Funcionarios, contratistas y colaboradores no podrán compartir sus cuentas de usuario y contraseñas con otros usuarios o con personas ajenas a la Entidad. Si esto llegara a pasar esto es causal de sanción por parte del Ministerio.
- Se debe identificar al personal que requiere acceso a las instalaciones del Ministerio, autorizar su ingreso y conceder los privilegios necesarios para el acceso físico de acuerdo con Protocolo **de seguridad Ministerio de Ambiente y Desarrollo Sostenible MA-A-GAC-01, y el formato (F-A-GAC-02).**
- Se deben adoptar protocolos de gestión de contraseñas de sobre cerrado y mantenerlos bajo custodia.

9.2.4 Gestión de información de autenticación secreta de usuarios.

Control: La asignación de información de autenticación secreta se debería controlar por medio de un proceso de gestión formal.

- Los funcionarios y contratistas deben mantener estricto control y confidencialidad de la información secreta de sus credenciales (contraseñas de las cuentas de usuario y accesos a sistemas de información).

9.2.5 Revisión de los derechos de acceso de usuarios

Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.

- La administración de los perfiles de usuario es responsabilidad de los administradores de cada aplicación o sistema.
- El jefe de área o dependencia deberá definir los permisos que correspondan a cada perfil y será responsable por el otorgamiento de los permisos de acceso a los recursos de la plataforma tecnológica, servicios de red, los sistemas de información y áreas seguras.
- Se deberán establecer controles de acceso a los ambientes de desarrollo, pruebas y producción de los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios necesarios para el acceso tanto a los ambientes como a la información.

9.2.6 Retiro o ajuste de los derechos de acceso

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 deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.

- La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar, tales como: "root", "adm" "administrador" y "system", entre otros, debe ser controlado por la OTIC, dejando registro de la trazabilidad de uso de estos accesos.
- Los derechos de acceso de un usuario se deben revisar y reasignar, ya sea por cambio de cargo o traslado de área.

9.3 Responsabilidades de los usuarios

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

9.3.1 Uso de información secreta para la autenticación.

Control Se debería exigir a los usuarios que cumplan las prácticas de la Entidad para el uso de información secreta para la autenticación.

- La OTIC deberá controlar que los colaboradores y contratistas no puedan utilizar ninguna estructura o característica de contraseña que pueda dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.
- Los servidores de la Entidad son responsables por el uso apropiado de las credenciales de acceso asignadas.
- No deben compartir sus credenciales o contraseñas con ninguna persona o hacerla pública por cualquier medio.
- Las acciones que se realicen con una cuenta usuario en los sistemas de información serán total responsabilidad del usuario.
- Después de (3) tres intentos fallidos al ingresar los datos de acceso, la cuenta debe quedar bloqueada, y sólo podrá ser desbloqueada por los responsables de soporte tecnológico de la OTIC.
- Se deberá implementar mecanismos de múltiple factor de autenticación para acceso a los servicios de TI.

9.4 Control de acceso a sistemas y aplicaciones

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

9.4.1 Restricción de acceso a la información

Control: El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.

- Se debe contar con mecanismos de control de acceso para las áreas seguras (centro de cómputo, centro de cableado, y oficinas que almacenen información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que la Entidad considere pertinentes.
- Las puertas de acceso al centro de cómputo, centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.
- Se debe aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo, administración de infraestructura, centros de cableado; además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.
- Se debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Se debe monitorear los ingresos al centro de cómputo permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.
- Para generar acceso tanto físico como lógico para los funcionarios del Ministerio, el jefe del área o dependencia correspondiente o quien haga sus veces debe realizar la solicitud al área respectiva.
- Se deben implementar mecanismos de múltiple factor de autenticación para acceso a los sistemas de información de la Entidad.

9.4.2 Procedimiento de ingreso (Log-On) seguro

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

- Toda solicitud de acceso a sistemas y aplicaciones debe hacerse mediante el procedimiento a través de la plataforma GEMA.
- Validar en el directorio activo los registros de intentos exitosos y fallidos por parte de los usuarios para medir la eficacia del control.

9.4.3 Sistema de gestión de contraseñas

Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.

- La longitud mínima de las contraseñas debe ser igual o superior a ocho (8) caracteres y estarán constituidas por combinación de caracteres numéricos, especiales y alfabéticos (letras mayúsculas y minúsculas).
- Las contraseñas deben ser creadas de acuerdo con las normas y políticas fijadas por el Ministerio se aplicarán controles y herramientas como generadores de contraseñas que permitan asegurar el cumplimiento mínimo de seguridad.
- Las contraseñas deben ser cambiadas mínimo cada 45 días, estas contarán con un nivel de confiabilidad lo que significa que al usuario a quien se le asigne una cuenta de usuario único de autenticación.
- Los aplicativos deben sugerir el cambio obligatorio a los usuarios a cambiar las contraseñas temporales en su primer ingreso o registro.
- Mantener un registro de claves de usuario previas y evitar el re-uso.
- No mostrar las contraseñas en la pantalla en el momento de ingresarlas.
- Almacenar las contraseñas cifradas con algoritmos fuertes, mediante uso de funciones hash.
- Validar el nivel de seguridad de las contraseñas de acceso creadas por los colaboradores, permitiendo solamente el uso de contraseñas fuertes.
- Solicitar la modificación en un periodo definido de las contraseñas de ingreso a los aplicativos del Ministerio.

9.4.4 Uso de programas utilitarios privilegiados

Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

- Está estrictamente prohibido el uso de programas utilitarios, software o aplicaciones no autorizadas por parte de funcionarios y contratistas sin la debida autorización de la OTIC.
- El uso de herramientas o utilitarios propios de los sistemas operativos debe ser limitado a personal autorizado y su uso está restringido en casos específicos y debe disponerse de la trazabilidad de las operaciones realizadas en los casos que son autorizados. (GEMA y Consola Antivirus).

9.4.5 Control de acceso a códigos fuente de programas

Control: Se debería restringir el acceso a los códigos fuente de los programas.

- Para acceder a los códigos fuente de programas y elementos asociados se debe contar con autorización de la OTIC, lo anterior con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual.

10. CRIPTOGRAFÍA

10.1 Controles Criptográficos

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

10.1.1 Política sobre el uso de controles criptográficos

Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

- El área encargada deberá buscar mecanismos y herramientas para la trasmisión de la información considerada como reservada o de acceso restringido mediante técnicas de cifrado con el propósito de proteger su confidencialidad e integridad para esto implementará sistemas de cifrado como aplicativos que permitan llevar a cabo el procedimiento para el manejo de la información al igual que establecer estándares y normas de controles criptográficos.
- Los desarrolladores ya sean directos o contratistas deberán cifrar la información reservada o restringida y garantizar que ésta cuente con la confiabilidad que se requiere con el objetivo de garantizar su integridad y disponibilidad al momento de necesitarla.
- Establecer roles y responsabilidades para la implementación de la política y la gestión de los mecanismos criptográficos.
- La OTIC debe establecer una estrategia para cifrar las bases de datos críticas del Ministerio o campos que contengan datos personales, velando por no afectar el desempeño de los sistemas de información.
- La OTIC debe dar a conocer y capacitar a los funcionarios, contratistas, proveedores o terceros en el uso de las herramientas de uso criptográfico, cuando así se requiera su uso.
- Comunicar al Comité Institucional de Gestión y Desempeño, los eventos o incidentes que conlleven al no cumplimiento de los objetivos institucionales por el no uso de controles criptográficos para la información clasificada y reservada.

10.1.2 Gestión de llaves

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

- Las llaves públicas de encriptación deben considerar la políticas de gestión de contraseñas para su generación; esta se hará aplicando procesos de expiración acorde a los criterios establecidos para cada herramienta de encriptación y desencriptación , en los cuales se debe configurar tiempo para la expiración de la llave no superior a los 90 días y esta deberá ser reemplazada cada vez que las personas dueñas del proceso sean sustituidos del cargo o al momento de efectuar controles de cambios en las configuraciones de las herramientas.

- Los certificados digitales para Entidad certificadora, herramientas sistemas de cifrado simétrico de documentos y demás recursos asociados para manejo de llaves o esquemas criptográficos; se deben custodiar de forma cifrada en cuanto a sus claves confidenciales dentro del Módulo de seguridad de hardware (HSM) como medio empleado por la Entidad para resguardar de forma segura, protegida e identificables las claves criptográficas. Ejemplos de estos son las tarjetas con PIN o dispositivos físicos para firma electrónica.
- Realizar revisiones periódicas a las herramientas de uso criptográfico (Tokens, Firma Digital, etc.), con el fin de detectar fallas o vulnerabilidades.
- Notificar con anterioridad a los dueños de la información, aplicaciones, software que requieran de certificados digitales, la fecha de caducidad de éstos para su renovación.
- Realizar la entrega de los certificados digitales generados con el debido procedimiento para su aplicación y uso.
- Prestar soporte técnico para la configuración de los usuarios y soluciones adoptadas para controles criptográficos.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

11.1 Áreas Seguras

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

11.1.1 Perímetro de seguridad física

Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.

- Se debe contar con mecanismos de control de acceso para las áreas seguras (centro de cómputo, centro de cableado, y oficinas que almacenen información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que la Entidad considere pertinentes.
- Las puertas de acceso al centro de cómputo, centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.
- El centro de cómputo debe tener mecanismos de vigilancia tanto en el ingreso como en su interior.
- El centro de cómputo, los centros de cableado y las áreas determinadas como seguras, deben tener control y registro de ingreso y salida del personal autorizado, así como de los elementos almacenados.

11.1.2 Controles de acceso físicos

Control: Las áreas seguras se deberían proteger mediante controles de acceso apropiados para asegurar que solo se permite el ingreso a personal autorizado.

- Se debe aprobar de manera previa las solicitudes de acceso al centro de cómputo y áreas consideradas como seguras, administración de infraestructura, centros de cableado; además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.
- Se debe implementar mecanismos de autenticación para el acceso al centro de cómputo y centros de cableado.
- Se debe implementar registros de ingreso y salida física en las áreas seguras.
- Todos funcionarios, contratistas, colaboradores y visitantes deben portar algún tipo de identificación visible durante su permanencia en las instalaciones del Ministerio.
- Se debe realizar acompañamiento al personal de servicio de soporte de una parte de un funcionario o colaborador del Ministerio.

11.1.3 Seguridad de oficinas, recintos e instalaciones

Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.

- Se debe proteger las áreas de centro de cómputo y centros de cableado con instalaciones de seguridad físicas robustas.
- Se debe mantener de forma anónima la confidencialidad de las áreas físicas en donde se procesa información sensible.

11.1.4 Protección contra amenazas externas y ambientales

Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

- Se debe contar con soluciones de control de incendios, sistemas de precisión ambiental.
- Se debe contar con un plan de emergencias definido por el Grupo de Servicios Administrativos, que debe ser probado anualmente, con el fin de brindar protección contra amenazas externas.

11.1.5 Trabajo en áreas seguras

Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.

- Funcionarios, contratistas y colaboradores solo deben conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en las necesidades de sus responsabilidades.
- El trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas.
- Las áreas seguras vacías deben estar cerradas con llave y se deberían revisar periódicamente.
- No se debe permitir equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, en áreas consideradas como seguras; salvo que se cuente con su debida autorización.

11.1.6 Áreas de despacho y carga

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

- La recepción y despacho de carga debe ser controlada por el grupo de servicios administrativos y la empresa de vigilancia del Ministerio en los horarios definidos para la realización de estas actividades, y en ningún caso cerca de las instalaciones de las áreas consideradas como seguras.

11.2 Equipos

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

11.2.1 Ubicación y protección de los equipos

Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.

- Se debe ubicar los equipos de procesamiento de información (servidores, equipos de comunicaciones) en áreas seguras.
- Está prohibido el consumo de alimentos o bebidas y fumar dentro o en cercanías de las instalaciones de procesamiento de información.
- Se debe evaluar regularmente la efectividad del funcionamiento de los sistemas de puesta a tierra.

11.2.2 Servicios de suministro

Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

- Se debe cumplir con las especificaciones de los fabricantes de equipos de soporte ambiental y eléctrico con los requisitos legales locales.
- 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.

11.2.3 Seguridad del cableado

Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debería estar protegido contra interceptación, interferencia o daño.

- Se debe implementar una instalación de cableado estructurado que esté debidamente certificado en todos sus puntos de conexión.
- Se debe tener instalada y configurada un sistema eléctrico regulado para la conexión de todos los activos de tecnología.

11.2.4 Mantenimiento de equipos

Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.

- El Ministerio debe contar con planes de mantenimiento (que incluyan las condiciones definidas por las aseguradoras, requisitos técnicos de los equipos, las definiciones de ventana de tiempo, etc.) para todos los equipos que soporten los procesos de la Entidad.
- Se debe ejecutar los planes de mantenimiento establecidos de manera satisfactoria.
- Se debe hacer una revisión de la efectividad de los mantenimientos ejecutados.

11.2.5 Retiro de activos

Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.

- Todos los funcionarios, contratistas, colaboradores y partes externas deben estar debidamente autorizados para el retiro o traslado de activos del sitio donde se encuentran.

- Se debe llevar registro de todos los activos que se retiran del sitio donde están ubicados dejando observaciones respecto de su devolución.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Control: Se deberían 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.

Los funcionarios y contratistas o colaboradores que retiren equipos o medios removibles de las instalaciones de la Ministerio deben seguir las siguientes directrices:

- 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 Ministerio, se debe poner la denuncia ante la autoridad competente e informar inmediatamente a la OTIC y coordinador del grupo servicios administrativos para el trámite interno correspondiente.

11.2.7 Disposición segura o reutilización de equipos

Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.

- Cuando una estación de trabajo o equipo portátil vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la información.
- El equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobre escritura de los medios que contienen información) con el fin de evitar pérdida de la información o recuperación no autorizada de la misma. Ver indicaciones adicionales en el **G-A-GTI-04-BORRADO SEGURO.**

11.2.8 Equipos de usuario desatendidos

Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les da protección apropiada.

- Cuando el colaborador se ausente de su sitio de trabajo, este deberá verificar que la pantalla de su computador este bloqueada, así como las aplicaciones a las que accede no queden abiertas y habilitadas para que personas ajenas puedan tener acceso a la información de la

Entidad, también deberá guardar los documentos físicos, medio magnético que contenga información de uso interno, clasificada o reservada.

- Al imprimir documentos de carácter confidencial (información pública clasificada e información pública reservada), estos deben ser enviados con pin de seguridad y retirados de la impresora inmediatamente.

11.2.9 Política de escritorio limpio y pantalla limpia

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

- Todos los funcionarios y contratistas del Ministerio 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; se deben contemplar los siguientes lineamientos cuando se retiren de sus puestos de trabajo.
- Los computadores deben cargar por defecto el fondo de pantalla del Ministerio, éste no debe ser modificado y debe permanecer activo.
- Las pantallas de los computadores, así como de los portátiles asignados a funcionarios deben estar libre de archivos o enlaces de acceso a cualquier tipo de archivos.
- Se prohíbe el almacenamiento de información personal en los computadores del Ministerio, el escritorio lógico (del computador) debe estar libre de información pública clasificada e información pública reservada.

12. SEGURIDAD DE LAS OPERACIONES

12.1 Procedimientos Operacionales y Responsabilidades

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

12.1.1 Procedimientos de operación documentados

Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesitan.

- Se debe definir un procedimiento de operación que contemple operación y administración del centro de cómputo y centros de cableado en donde se documenten las configuraciones e instalaciones de equipos, el manejo de la información manual y automática, y otras

condiciones de cumplimiento para la operación adecuada de estos sitios, como la recuperación de sistemas, equipos y aplicaciones.

12.1.2 Gestión de cambios

Control: Se deberían 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.

- El Ministerio debe implementar procedimientos para la gestión de los cambios en donde los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información se deban realizar de acuerdo con los lineamientos en este procedimiento **P-A-GTI-04, y** formato **F-A-GTI-01.**

12.1.3 Gestión de capacidad

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.

- Se debe monitorear la capacidad de los sistemas y su infraestructura para garantizar la disponibilidad y proyectar nuevos requisitos del negocio.
- Se debe implementar un procedimiento de Gestión de Capacidad **P-A-GTI-06 GESTION DE LA CAPACIDAD.**
- Definir un plan de capacidad especialmente para sistemas críticos en donde se deben tener en cuenta aspectos tales como:
    - Responsables
    - Actividades
    - Fechas de inicio y fin.
    - Recursos, riesgos, costos, tiempo y proyecciones.

12.1.4 Separación de los ambientes de desarrollo, pruebas y producción

Control: Se deberían separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.

- El Ministerio debe contar con ambientes de desarrollo, prueba y producción con separación lógica que contengan las reglas de transferencia del software entre los ambientes de desarrollo, prueba y paso a ambiente de producción.
- Se debe contar con datos de prueba debidamente almacenados y protegidos, y en ningún caso estos datos deben contener datos sensibles o datos reales.

- Los accesos a los diferentes ambientes deben cumplir con los requerimientos de la política de control de acceso definida en el numeral **9 Control de Acceso,** y los usuarios deben utilizar diferentes perfiles entre el ambiente de pruebas y el ambiente de producción.

12.2 Protección Contra Códigos Maliciosos

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

12.2.1 Controles contra códigos maliciosos

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

- Se deben proteger los servidores, estaciones de trabajo, equipos portátiles, y dispositivos móviles contra código malicioso.
- Los contratistas y colaboradores que hagan uso de computadores y portátiles que no pertenezcan al Ministerio y hagan uso de la infraestructura e información de la Entidad deben tener instalado software antivirus licenciado.
- La instalación del antivirus debe ser realizada únicamente por personal autorizado de la OTIC en los servidores, estaciones de trabajo y portátiles de la Entidad.
- Como parte esencial de la arquitectura de TI del Ministerio, se debe contar con soluciones de análisis y control de código malicioso que contemple la descarga de software, filtrados de URLs por categoría potencialmente dañinas o improductivas, la protección de la mayoría de los medios posibles, como internet, correo electrónico, software ejecutable, scripts, entre otros; y restringir la ejecución automática de aplicaciones que no estén debidamente autorizadas.
- Mecanismos de administración que permitan el control y despliegue de las políticas y reglas de control establecidas, así como sus actualizaciones y sincronización automática, en el menor tiempo posible.
- Monitoreo permanente de la red de datos frente a la detección y búsqueda de código malicioso.
- Se debe evitar que los usuarios (funcionaros, colaboradores y terceros) puedan desactivar o eliminar las herramientas o sistemas de protección de la seguridad de la información como la solución de antivirus, antimalware y de prevención de ataques avanzados, entre otros.

12.3 Copias de Respaldo

Objetivo: Proteger contra la pérdida de datos.

12.3.1 Respaldo de la información

Control: Se deberían 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.

- El propósito de la presente política es garantizar que la Entidad cuente con un de plan de generación de copias de respaldo, estableciendo e implementado diferentes actividades para crear, recuperar y mantener las copias de la información generada por la Entidad, a fin de cumplir con su misionalidad y funcionamiento. En el caso de un desastre, es vital que la información esté disponible en una ubicación alternativa para ser utilizado con fines de recuperación.
- La OTIC debe establecer las políticas de copias de seguridad desde la herramienta de backups para: los sistemas de información y bases de datos, servidor de archivos, código fuente, activos de información, configuración de infraestructura, configuración de redes, directorio activo, correo electrónico, etc.
- Todas las copias de respaldo deben contar con un procedimiento de restauración y contemplar un sitio secundario para su almacenamiento y preservación.
- Todos los administradores de base de datos, aplicaciones y servicios deben cumplir con las políticas de backup establecidas por la OTIC.
- Se debe garantizar la disponibilidad de infraestructura asignada para los procesos de respaldo y asegurar su disponibilidad cuando sea requerida la copia, incluso después de un desastre o falla de un dispositivo.
- Cada proceso de respaldo que se realice de forma automática debe dejar registro en los logs de los servidores, o sistemas de información. Todo respaldo realizado de forma manual debe dejar constancia o evidencia documentada.
- Realizar copias de respaldo de los servidores virtuales actualmente en producción, de una manera óptima y práctica, para su posterior almacenamiento por fechas y disposición para restauraciones programadas y de emergencia.
- Es necesario realizar una copia de seguridad de las máquinas virtuales en producción, que contenga la estructura en hardware virtual, tales como memoria, procesamiento, dispositivos de red, discos duros virtuales, entre otros, compatible con la estructura de virtualización actualmente en producción en el Ministerio.
- La ejecución de las pruebas de restauración de las copias de respaldo debe asegurar la recuperación de los datos y garantizar la integridad de estos.

12.4 Registro (Logging) y Seguimiento

Objetivo: Registrar eventos y generar evidencia.

12.4.1 Registro de eventos

Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

- El Ministerio debe monitorear en forma continua todos los eventos de los sistemas operativos, bases de datos y servicios, incluyendo en sus Logs; fechas, hora y detalles del evento.
- Se deben registrar los eventos de intentos de accesos exitosos y fallidos a los sistemas de información y servicios de TI.
- Se deben registrar y monitorear todos los eventos utilizando herramientas de correlación.

12.4.2 Protección de la información de registro.

Control: Los sistemas de gestión de registros y la información de registro se deben proteger contra alteración y acceso no autorizado.

- Se deben copiar en tiempo real los Logs de registro para evitar perdida o adulteración de estos.
- Se debe asignar credenciales solo a la persona debidamente autorizada por la OTIC para realizar le monitoreo y gestión de riesgos.
- La solución de correlación de eventos debe estar separada en una red segmentada y asegurada.

12.4.3 Registros (Logs) del administrador y del operador

Control: Las actividades del administrador y del operador del sistema se deberían registrar (Logged), y los registros (Logs) se deberían proteger y revisar con regularidad.

- 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.

12.4.4 Sincronización de relojes

Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una Entidad o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.

- 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 Ministerio 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.

12.5 Control de Software Operacional

Objetivo: Asegurar la integridad de los sistemas operativos.

12.5.1 Instalación de software en sistemas operativos.

Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.

- La instalación y desinstalación de software está a cargo exclusivamente de funcionarios de Mesa de Ayuda y ningún funcionario contratista o colaborador puede adelantar estas labores.
- El Software debe contar con su respectiva documentación (Licencia) y en el caso del software libre debe estar permitido el uso comercial y su instalación debe ser descargada de la página oficial del fabricante.
- Toda instalación de software debe ser debidamente documentada.
    - Documento de Licencia del Software (representa el permiso que le da el fabricante para la instalación y uso de su producto)
    - Manual de Instalación del Software (Para determinar que el software ha sido instalado apropiadamente)
    - Manual del Usuario para uso del Software (Para guiar al usuario en su uso y apropiación)
    - Restricciones de uso según los acuerdos de licenciamiento, términos y condiciones descritos en el documento de licencia y la página oficial del fabricante.
- La OTIC debe hacer revisiones periódicas del uso del software instalado en los servidores, estaciones de trabajo y portátiles del Ministerio, para mantener un registro de auditoría de las librerías de programas.
- Todo software que viole los acuerdos de licenciamiento, las políticas y controles de este manual debe ser desinstalado inmediatamente y debe ser reportado el hecho como incidente de seguridad por incumplimiento de la política.
- Se deben definir procedimientos para el manejo de propiedad intelectual y dada de baja de software.

12.6 Gestión de la Vulnerabilidad Técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas

12.6.1 Gestión de las vulnerabilidades técnicas

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

- Se debe generar y ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y Hacking Ético.
- Se deben definir planes de cierre de brechas en las vulnerabilidades identificadas en donde se identifiquen los responsables de remediación y los tiempos de ejecución de estas remediaciones.
- Todos los ajustes resultantes del plan de cierre de brechas se deben realizar con base en el procedimiento y controles de la Gestión de Cambios establecida en la Entidad.
- La aplicación de parches se debe evaluar y aprobar previamente a su instalación para evitar efectos no deseados en la ejecución del cambio.
- El Ministerio debe definir y establecer roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.

12.6.2 Restricciones sobre la instalación de software

Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.

- Toda instalación de software debe ser realizada y aprobada por la OTIC.
- Los usuarios que utilicen el software instalado deben cumplir el principio de menor privilegio.
- Se deben implementar mecanismos técnicos para restringir la instalación de software.

12.7 Consideraciones Sobre Auditorías de Sistemas de Información

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

12.7.1 Controles sobre auditorías de sistemas de información

Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

- Los requisitos de auditoría para acceso a sistemas de información y a datos se deben acordar con los líderes de procesos y propietario de sistemas de información.
- El alcance de las pruebas técnicas de auditoría debe ser acordado y controlado.
- Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y hacking ético) que puedan afectar la disponibilidad del sistema se deben ejecutar en ventanas de tiempo previamente definido en un ambiente controlado.
- Se debe hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.
- Las pruebas de auditoría deben tener acceso de solo lectura al software y a los datos.
- 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.

13. SEGURIDAD EN LAS TELECOMUNICACIONES

13.1 Gestión de la Seguridad de las Redes

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

13.1.1 Controles de redes

Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.

- Se debe implementar controles para asegurar la seguridad de la información en las redes, y la protección de servicios relacionados, contra acceso no autorizado.
- Se debe establecer las responsabilidades y procedimientos para la gestión de equipos de redes.
- Se debe separar el acceso operacional con base en un esquema de segmentación que contemple:
    - Segmentaciones por servicios TI
    - Segmentación de la red inalámbrica (Institucional e invitados)
    - Segmentación por áreas
    - Segmentación de la zona “WIFI gratis para mi gente”.
- Se debe promover la confidencialidad, integridad y disponibilidad a través de las redes y sus segmentos tanto en las redes públicas como en las inalámbricas.
- Se deben activar los mecanismos de registro (Logging) y seguimiento para traza de auditorías.
- Se deben restringir la conexión de los sistemas, servicios y dispositivos a través de mecanismos de control de acceso.

13.1.2 Seguridad de los servicios de red

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

- 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.

13.1.3 Separación en las redes

Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.

- El Ministerio debe separar a través de mecanismos de VLANs (redes lógicas) los accesos a los diferentes servicios de TI.
- Las redes se deben controlar a través de seguridad de perímetro, portales cautivos, dispositivos de valoración de requisitos y políticas de control de acceso.
- Se deben definir mecanismos de autenticación y protocolos de seguridad para el acceso a redes.

13.2 Transferencia de Información

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

13.2.1 Políticas y procedimientos de transferencia de información

Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.

- El Ministerio debe firmar acuerdos o compromisos de confidencialidad con los servidores públicos, contratistas y terceros, los cuales deben incluir una cláusula de confidencialidad para el acceso a la información y que requieran conocer o intercambia y este etiquetada como restringida o confidencial.
- Para intercambios periódicos se debe privilegiar la transmisión de datos a través de vías seguras. Cuando el intercambio se establezca con entes gubernamentales, se hace necesario establecer convenios o nexos de diferente naturaleza.

- Se deben establecer repositorios de información dedicados y asegurados para los activos de información que requieran ser compartidos y definir repositorios de información para trabajos en forma colaborativa.
- El uso de estos repositorios debe ser considerados como temporales y no deben ser considerados como un repositorio documental, para la cual se deben seguir las políticas y procedimientos de publicación oficial con base en las definiciones de gestión documental del Ministerio.
- Para acceso a sitios web se debe implementar herramientas de seguridad perimetral seguros (firewalls) y el uso de protocolos seguros

13.2.2 Acuerdos sobre transferencia de información

Control: Los acuerdos deberían tratar la transferencia segura de información del negocio entre la Entidad y las partes externas.

- El Ministerio debe implementar acuerdos de transferencia de información donde se especifiquen aspectos tales como: responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo, los procedimientos para asegurar trazabilidad y no repudio; los estándares técnicos mínimos para empaquetado y transmisión; certificados de depósito de títulos en garantía; estándares de identificación de mensajería; las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos; el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente; las normas técnicas para registro y lectura de información y software; cualquier control especial que se requiera para proteger elementos sensibles, tales como criptografía; mantener una cadena de custodia para la información mientras está en tránsito; los niveles aceptables de control de acceso.

13.2.3 Mensajería electrónica

Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.

- El Ministerio debe asignar una cuenta de correo electrónico a cada uno de sus funcionarios y colaboradores que lo requieran para el cumplimiento de sus funciones.
- Los mensajes y la información contenida en los buzones de correo son de propiedad del Ministerio y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- La información enviada por correo electrónico, clasificada como "Reservada" o "Clasificada", debe ser protegida con contraseña de acceso o cifrado según corresponda. La Oficina de Tecnologías de la información deberá definir controles para la transferencia de información a través de redes públicas para las aplicaciones del Ministerio.

- La OTIC deberá disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones del Ministerio, teniendo en cuenta los siguientes criterios:
  - Contar con información secreta de autenticación.
  - Utilizar F2A (Doble factor de autenticación) como elemento de mejora en la seguridad de las credenciales de los usuarios.
  - Mantener la privacidad de las partes involucradas.
  - Cifrar los mensajes cuando sea requerido.
  - Uso de protocolos de comunicación seguro.
- El Ministerio debe definir e implementar un descargo de responsabilidades (Disclaimer) configurado e implementado en la plataforma de correo electrónico institucional.

13.2.4 Acuerdos de confidencialidad o de no divulgación

Control: Se deberían 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.

- Los funcionarios, contratistas y terceros, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un acuerdo de confidencialidad o de no divulgación, si este no está incluido como una cláusula dentro del contrato individual de trabajo para trabajadores oficiales o contrato de prestación de servicios.
- Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la Entidad, en los términos de la Ley 1581 de 2012, 1712 de 2014 y las demás normas que la adicionen, modifiquen, reglamenten o complementen. Este documento debe ser archivado de forma segura por el área de Talento Humano y Contractual, según sea el caso.
- Dentro del mismo acuerdo el colaborador o tercero deben declarar conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1 Requisitos de Seguridad de los Sistemas de Información

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

14.1.1 Análisis y especificación de requisitos de seguridad de la información

Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

- La OTIC debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados.
- Las dependencias o procesos que contraten el desarrollo de software o adquieran software de terceros, deben apoyarse en la OTIC para definir los requisitos de seguridad de la información necesarios.
- A nivel de los requisitos de los sistemas de información se debe definir:
    - El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario
    - Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos
    - Las necesidades de protección de activos de información involucrados, respecto de su disponibilidad, confidencialidad e integridad
    - Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación mediante HTTPS, cifrado de contraseñas almacenadas, uso de firmas digitales
    - Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.
    - La necesidad de exigir la implementación de metodologías de desarrollo seguro.

14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

- Se debe definir el nivel y rol de aprobación de contenidos o documentos para publicación en el portal del Ministerio y en las diferentes redes públicas
- Las aplicaciones que están usando redes públicas deben contar con mecanismos de protección de información sensible.
- Se deben definir e implementar mecanismos técnicos que minimicen las amenazas de fraude y manipulación de la información publicada en las redes.

14.1.3 Protección de transacciones de los servicios de las aplicaciones.

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.

- Se debe implementar autenticación secreta de usuario en todos los servicios de transacciones con los bancos.
- Se debe cumplir con los lineamientos establecidos para seguridad lógica, seguridad física, de red, seguimiento y control en las terminales de áreas financieras de las Entidades públicas de acuerdo con el documento **"Guía 18 Lineamientos: Terminales de áreas financieras Entidades públicas "del MSPI.**

14.2 Seguridad en los Procesos de Desarrollo y de 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.

14.2.1 Política de desarrollo seguro

Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la Entidad.

- El Ministerio velará por que el desarrollo interno o externo de aplicaciones o sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para el desarrollo seguro, así como la metodología para la realización de pruebas de aceptación y seguridad del software desarrollado.
- Se debe verificar que los desarrollos estén debidamente documentados, así como todas las versiones del desarrollo se deben preservar adecuadamente en varios medios y guardar una copia de respaldo en sitio externo.

14.2.2 Procedimientos de control de cambios en sistemas

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

- La OTIC, es la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con los desarrollos, actualizaciones e instalaciones de software. Además, debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.
- Se debe ejecutar el control de cambios teniendo en cuenta los lineamientos y requerimientos de seguridad definidos, los cuales deberán contar con la aprobación de las partes interesadas.

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

Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la Entidad.

- Se debe hacer una verificación de los cambios en las plataformas de operación y en las aplicaciones respecto al impacto y cumplimiento de los lineamientos de seguridad de la información.

14.2.4 Restricciones en los cambios a los paquetes de software

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

- Solo se deben utilizar paquetes de software licenciados y adquiridos a través de un proveedor autorizado, así como las actualizaciones de aplicaciones y parches que se deban realizar.
- Cualquier tipo de modificación que se realice, debe ser puesta a prueba y ser validada antes de su implementación.

14.2.5 Principios de construcción de sistemas seguros

Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

- El Ministerio debe documentar, aplicar y exigir que la construcción de sistemas de información cumpla con requerimientos de diseño de arquitectura segura, que incluya capas de negocio, datos, aplicaciones y tecnología; y deben actualizarse con regularidad para combatir nuevas amenazas potenciales.
- Los nuevos desarrollos deben realizar análisis de gestión de riesgos para la seguridad, y el diseño se debería revisar contra patrones de ataque conocidos.

14.2.6 Ambiente de desarrollo seguro

Control: Las organizaciones deberían 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.

- Se debe diseñar, implementar, documentar, mantener y auditar un ambiente de desarrollo seguro que incluya el personal confiable, procesos y tecnología asociados con el desarrollo e integración de sistemas. En caso de ser necesario, se deben establecer ambientes de desarrollo seguros para las labores de desarrollo de sistemas específicos.
- Adicionalmente se debe realizar la valoración de riesgos asociados con las labores de desarrollo de sistemas individuales, considerando: datos sensibles que el sistema va a procesar, almacenar y transmitir; requisitos externos e internos aplicables, controles de seguridad ya implementados por el Ministerio, que se relacionen con el desarrollo del sistema;

el objetivo y alcance del contrato asociado con el desarrollo del sistema; la necesidad de separación entre diferentes ambientes de desarrollo; el control de acceso al ambiente de desarrollo; el seguimiento de los cambios en el ambiente y en los códigos almacenados en los repositorios oficiales; las copias de respaldo se almacenen en lugares seguros fuera del Ministerio; el control sobre el movimiento de datos desde y hacia el ambiente.

14.2.7 Desarrollo contratado externamente

Control: La Entidad debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

- Para los desarrollos de aplicaciones por parte de un proveedor externo, se deben aplicar las políticas y lineamientos de seguridad de la información, así como buenas prácticas en los procesos de desarrollo, que incluyan compromisos de confidencialidad, derechos de propiedad intelectual, desarrollo de auditorías, las condiciones de soporte y mantenimiento.

14.2.8 Pruebas de seguridad de sistemas

Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.

- Para la realización de las pruebas de software, los proveedores de desarrollo deben proveer datos ficticios o anonimizados, evitando la utilización de datos reales.
- Las pruebas de seguridad deben garantizar los requisitos de seguridad de la información establecidos para el desarrollo.
- Las partes interesadas en el desarrollo deben exigir las evidencias de que se efectuaron pruebas de seguridad al software desarrollado por terceros.

14.2.9 Prueba de aceptación de sistemas

Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.

- Se deben realizar pruebas de aceptación del software por parte de una persona diferente de quien ha desarrollado el software, además estas pruebas deben ser evidenciadas a través de un documento firmado por quienes las realizaron, en donde se acepte que el software desarrollado cumple con los lineamientos y funcionalidades para su uso.
- Se deben realizar las pruebas en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente productivo del Ministerio, y que las pruebas son confiables.

14.3 Datos de Prueba

Objetivo: Asegurar la protección de los datos usados para pruebas.

14.3.1 Protección de datos de prueba

Control: Los datos de prueba se deberían seleccionar, proteger y controlar cuidadosamente.

- Se debe aplicar los procedimientos de control de acceso de los ambientes de producción en las mismas condiciones en las mismas condiciones para los ambientes de prueba.
- No se deben usar datos de prueba que contengan información de datos personales o confidenciales.
- Se deben borrar del ambiente de pruebas todos los datos inmediatamente después de finalizar las pruebas.
- Se debe llevar un registro de copiado de los datos para suministrar rastros de auditoría.

15. RELACIONES CON LOS PROVEEDORES

15.1 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.

15.1.1 Política de seguridad de la información para las relaciones con proveedores

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 deberían acordar con estos y se deberían documentar.

- El Ministerio debe establecer mecanismos de verificación de lineamientos de seguridad en sus relaciones con todos los proveedores, especialmente en aquellos considerados como críticos.

15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

Control: Se deberían 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.

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

- Se deben hacer visitas a los proveedores con el fin de identificar situaciones que puedan comprometer la información del Ministerio en el no cumplimiento de los lineamientos de seguridad establecidos.
- El grupo de contratos debe incluir en los acuerdos con proveedores y contratistas, los siguientes requisitos de seguridad de la información:
    - Cláusula de confidencialidad
    - Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 3 años después de terminado el contrato)
    - Cumplimiento de las políticas de seguridad de la información del Ministerio
    - 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
    - Etiquetado y manejo de la información de acuerdo con las directrices del **procedimiento Clasificación, Manejo y Etiquetado de la información gestión de activos P-A-GTI-07**
    - Cláusula de seguimiento y revisión de los servicios de los proveedores o terceros para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, en los acuerdos contractuales correspondientes.
- 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.
- Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la OTIC.

15.1.3 Cadena de suministro de tecnología de información y comunicación

Control: Los acuerdos con proveedores deberían 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.

- Se deben establecer en los acuerdos de servicios con los proveedores de comunicaciones los requisitos de seguridad de la información a lo largo de la cadena de suministros, así como las prácticas de seguridad adecuadas si se incluyen otros productos comprados a otros proveedores
- Se deben monitorear los servicios de comunicaciones para validar el cumplimiento de los productos y servicios estén de acuerdo con los requisitos de seguridad definidos.

15.2 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.

15.2.1 Seguimiento y revisión de los servicios de los proveedores

Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

- 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.
- Se debe asignar la responsabilidad de la gestión de la relación con los proveedores, a un funcionario o grupo de funcionarios del Ministerio y asegurar que los proveedores asignen la responsabilidad de revisión de conformidad y el cumplimiento de los requisitos acordados.
- 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.

15.2.2 Gestión de cambios en los servicios de los proveedores

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

- En los servicios establecidos con los proveedores se deben gestionar todos los cambios siguiendo el procedimiento definido por el Ministerio 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.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 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 debilidades.

16.1.1 Responsabilidades y procedimientos

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

- La gestión de incidentes de seguridad debe estar basada en los lineamientos del Procedimiento de Gestión de Incidentes, donde se debe establecer como mínimo: quiénes

deben reportar, los canales de comunicación, tipo de situaciones que se deben reportar, decisiones sobre las situaciones reportadas, respuesta a incidentes, aprendizaje de estos y recolección de evidencias digitales.

- Cualquier incumplimiento identificado debe remitirse a la OTIC - Seguridad de la información, quien debe determinar si el evento se considera como incidente de seguridad de la información, teniendo en cuenta las categorías y criterios de clasificación definidos **P-A-GTI-09 PROCEDIMIENTO GESTIÓN DE INCIDENTES.**
- Se debe asegurar que los responsables de la gestión de incidentes de seguridad de la información comprendan las prioridades de la Entidad para el manejo de incidentes de seguridad de la información.

16.1.2 Reporte de eventos de seguridad de la información

Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.

- Al presentarse un evento asociado con la seguridad de la información se debe notificar inmediatamente a la OTIC – Seguridad de la Información a través de los siguientes canales:
  - A la mesa de ayuda GEMA
  - Correo electrónico segurinfo@minambiente.gov.co
  - Al teléfono 3323400 ext. 6080.
- Se deben identificar las diferentes situaciones que están involucradas en el incidente como la violación a la integridad, disponibilidad o confidencialidad, control de seguridad insuficiente o ineficaz, errores humanos, violaciones a la seguridad física, violaciones de acceso, mal funcionamiento del software, cambios no controlados, etc.

16.1.3 Reporte de debilidades de seguridad de la información

Control: Se debería 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.

- Todos los funcionarios, colaboradores o terceros deberán reportar a través de los canales definidos cualquier situación que se pueda considerar como una debilidad en la seguridad de la información.

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

Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.

- Con base en la información reportada, la OTIC – Seguridad de la Información debe realizar el respectivo análisis para establecer la ocurrencia de un incidente de seguridad de la información y la respectiva gestión de este.

16.1.5 Respuesta a incidentes de seguridad de la información

Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

- Se debe gestionar adecuadamente los incidentes identificados con base en el procedimiento definido.
- La respuesta a los incidentes debe incluir el levantamiento de evidencias teniendo en cuenta el instrumento definido para este efecto.
- Se debe definir un protocolo para dar respuesta adecuada a los incidentes de seguridad de la información.

16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.

- 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.

16.1.7 Recolección de evidencia

Control: La Entidad debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

- Se debe aplicar la metodología para la recolección de evidencia digital en cumplimiento de la **GUÍA PARA EL LEVANTAMIENTO DE EVIDENCIAS G-A-GTI-06.**
- Se deben definir mecanismos para la recolección de evidencias físicas.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

17.1 Continuidad de Seguridad de la Información

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

17.1.1 Planificación de la continuidad de la seguridad de la información

Control: La Entidad debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

- Se debe garantizar la continuación de la seguridad de la información en la gestión de continuidad del negocio del Ministerio.
- En el plan de recuperación de ante desastres se deben tener en cuenta las políticas de seguridad de la información aplicables y se debe suponer que los requisitos de seguridad de la información siguen siendo los mismos que se utilizan en situaciones normales.
- Se debe determinar los requisitos de seguridad de la información cuándo se planifican la continuidad de negocio y la recuperación en caso de desastres.
- Se debe realizar en el análisis de impacto del negocio (BIA) la revisión de los aspectos de seguridad de la información para enfrentar situaciones adversas.

17.1.2 Implementación de la continuidad de la seguridad de la información

Control: la Entidad debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

- El Ministerio debe implementar mecanismos para mantener la seguridad de la información en la gestión y recuperación de situaciones adversas.
- El Ministerio debe definir políticas y controles de seguridad de la información aplicables ante situación adversas.
- Contemplar un sitio alterno, donde los controles implementados en el ambiente de producción deben ser consistentes con el sitio alterno.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Control: La Entidad debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

- 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.

- Los cambios de seguridad en el ambiente de producción deben ser aplicados de la misma forma para el ambiente de contingencia y deberán ser documentados.
- El Ministerio 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.
- Se deben realizar pruebas periódicas del DRP con el fin de asegurar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas.

17.2 Redundancias

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

17.2.1 Disponibilidad de instalaciones de procesamiento de información.

Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

- Se deben establecer e implementar redundancias en el Plan de Recuperación de Desastres (DRP) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.
- Se deben realizar pruebas periódicas del DRP con el fin de garantizar el funcionamiento de las redundancias establecidas.
- Se deben identificar los riesgos asociados a las redundancias establecidas.

18. CUMPLIMIENTO

18.1 Cumplimiento de Requisitos Legales y Contractuales

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

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Control: todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la Entidad para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la Entidad.

- Se debe elaborar el normograma con los requisitos de las partes interesadas aplicables a seguridad de la información.
- Se deben documentar los controles y las responsabilidades individuales específicas para cumplir estos requisitos.

18.1.2 Derechos de propiedad intelectual

Control: se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

- "El Ministerio de Ambiente y Desarrollo Sostenible define que todas las obras creadas (Referencia; Software de aplicaciones y otros documentos de carácter científico) serán propiedad del Ministerio, en cumplimiento del Artículo 91 de la LEY No 23 DE 1982 (28 DE ENERO DE 1982) SOBRE DERECHOS DE AUTOR."
- La OTIC debe realizar revisiones periódicas del uso del software instalado en las estaciones de trabajo y servidores de la Entidad, con el fin de validar el cumplimiento de la Ley 603 de 2000 de Derechos de Autor, conjuntamente debe identificar los activos de información que se encuentran afectados por derechos de propiedad intelectual.
- La OTIC debe asegurarse de que todo el software que se ejecute en el Ministerio esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de Ley.
- El Grupo de Contratos debe incluir cláusulas de propiedad intelectual y derechos de autor en contratos, que protejan el software, documentos, derechos de diseño, marcas registradas, patentes y códigos fuente.
- Es ilegal realizar procesos de ingeniería inversa.

18.1.3 Protección de registros

Control: los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

- El Ministerio se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de Confidencialidad, Integridad y Disponibilidad, siguiendo las directrices de inventario de Activos. **(G-A-GTI-03 Metodología para la clasificación e identificación de activos de la información).**
- El Ministerio debe implementar mecanismos de protección de registros tales como bases de datos, transacciones de auditoría, llaves criptográficas y registros de operación definiendo el periodo de retención y medios de almacenamiento (físico o digital), considerando las recomendaciones de los fabricantes para evitar la posibilidad de deterioro.

18.1.4 Privacidad y protección de información de datos personales.

Control: Se deberían 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.

- El Ministerio debe definir una política de protección de datos personales.

18.1.5 Reglamentación de controles criptográficos

Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.

- El Ministerio, se regirá por la Ley 527 de 1999 (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.

18.2 Revisiones de Seguridad de la Información

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

18.2.1 Revisión independiente de la seguridad de la información

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 deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

- El proceso de evaluación, control y mejora debe realizar auditorías internas de revisión independiente al menos anualmente. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque del Ministerio para gestionar la seguridad de la información. Esta revisión que es responsabilidad de la oficina de Control Interno del Ministerio debe incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios en el enfoque hacia la seguridad, incluyendo la política y los objetivos de control.

18.2.2 Cumplimiento con las políticas y normas de seguridad

Control: Los gerentes deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

- La OTIC debe liderar la revisión periódica (al menos anualmente) de los sistemas de información para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información.
- Se debe identificar en los resultados de evaluación las políticas y normas de seguridad las causas de las no conformidades para implementar acciones correctivas.

18.2.3 Revisión del cumplimiento técnico

Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

- Se deben realizar pruebas técnicas (pruebas de penetración, análisis de vulnerabilidades, ethical hacking, entre otros) para validar el cumplimiento de las políticas y controles de seguridad de información.

REFERENCIAS

Incibe_. (s.f.). *CONTRASEÑAS*. Obtenido de Instituto Nacional De Ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

Incibe_. (s.f.). *Copias De Seguridad*. Obtenido de Instituto Nacional De CiberSeguridad: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

Incibe_. (s.f.). *Guía sobre borrado seguro de la información*. Obtenido de Instituto Nacional De Ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

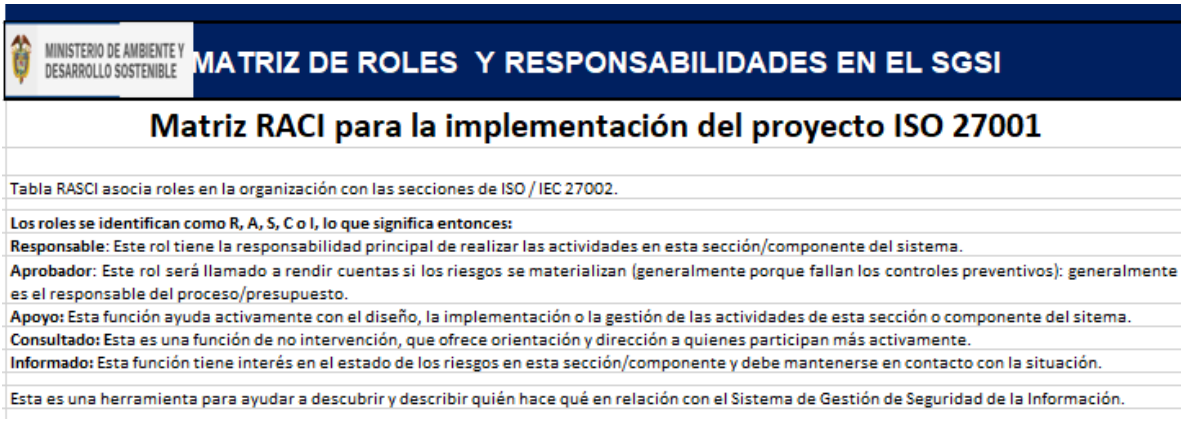
Incibe_. (s.f.). *PROTECCIÓN DEL PUESTO DE TRABAJO*. Obtenido de Instituto Nacional De Ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-puesto-trabajo.pdf

MinTic. (29 de Julio de 2016). *Modelo de Seguridad y Privacidad de la Información*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Pinzón Serrano, L. C. (s.f.). *Política de escritorio limpio y pantalla limpia*. Obtenido de MinTIC: https://www.mineducacion.gov.co/1780/articles-407695_galeria_02.pdf

Serrano, P. C. (s.f.). *Política sobre el uso de controles criptográficos*. Obtenido de MinTIC: https://www.mineducacion.gov.co/1759/articles-407695_galeria_07.pdf

ANEXO MATRIZ DE ROLES Y RESPONSABILIDADES DEL MINISTERIO



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

MATRIZ DE ROLES Y RESPONSABILIDADES EN EL SGSI

Matriz RACI para la implementación del proyecto ISO 27001

Tabla RASCI asocia roles en la organización con las secciones de ISO / IEC 27002.

Los roles se identifican como R, A, S, C o I, lo que significa entonces:

Responsable: Este rol tiene la responsabilidad principal de realizar las actividades en esta sección/componente del sistema.

Aprobador: Este rol será llamado a rendir cuentas si los riesgos se materializan (generalmente porque fallan los controles preventivos): generalmente es el responsable del proceso/presupuesto.

Apoyo: Esta función ayuda activamente con el diseño, la implementación o la gestión de las actividades de esta sección o componente del sitema.

Consultado: Esta es una función de no intervención, que ofrece orientación y dirección a quienes participan más activamente.

Informado: Esta función tiene interés en el estado de los riesgos en esta sección/componente y debe mantenerse en contacto con la situación.

Esta es una herramienta para ayudar a descubrir y describir quién hace qué en relación con el Sistema de Gestión de Seguridad de la Información.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Norma ISO/IEC 27002

R = Responsible A = Accountable S = Supportive C = Consulted I = Informed
R = Responsable A = Aprobador S = Apoyo C = Consultao I = Informado

		Propietarios de Activos de Información	Funcionarios de a Entidad	Dirección de la Entidad – Despacho del Ministro	Director de TIC	Comité Sectorial de gestión y desempeño	Oficial de Seguridad de la Información – OSI	Equipo de seguridad de operaciones de SI	Director de Talento Humano	Secretaría General – Presupuesto	Director Jurídico área legal y de Cumplimiento	Director de Finanzas	Responsable de Gestión de Instalaciones/Facilities	Responsable de Infraestructura de TI	Responsable de I+ D +I	Otros jefes de áreas o grupos de trabajo	Otras Direcciones o Áreas de la Organización	Proveedores
5	**Políticas de seguridad e la Información**																	
5.1.1	Políticas para la seguridad de la información	C	I	C	R	A	R	S	C	S	C	C	C	S	C	C	C	R
5.1.2	Revisión de las políticas para la seguridad de la información	C	I	S	A	R	S	C	S	S	S	S	C	S	S	I	I	I
6	**Organización de la Seguridad de la Información**																	
6.1.1	Roles y Responsabilidades de la Seguridad de la Información	A		C	R	S	C		C		C				C	C		
6.1.2	Segregación de tareas	A	I		C	R	C	S							C			
6.1.3	Contacto con autoridades	A			C	S	S	S			R							
6.1.4	Contacto con grupos especiales de interés	A			C	C	R	S			S				S			
6.1.5	Seguridad de la información en gestión de proyectos	A			C	R	S	S							S			
6.2.1	Política para dispositivos móviles	A	I		C	R	S	C							C			I
6.2.2	Teletrabajo	A	I		R	S	C	C							C			I
7	**Seguridad de los Recursos Humanos**																	
7.1.1	Verificación de antecedentes	A				S	S		R									
7.1.2	Términos y condiciones para el empleo	A	I			S			S		R							
7.2.1	Responsabilidades de la dirección	A	I	C	R	S			S									
7.2.2	Toma de conciencia, educación y entrenamiento en seguridad de la información	A	I		S	R	S	S	S		C							
7.2.3	Procesos disciplinarios	A	I		S				R									
7.3.1	Terminación o cambio en las responsabilidades del empleo	A	I			S			S		R				S			
8	**Gestión de activos**																	
8.1.1	Inventario de activos	A				S	S	S		R					C			
8.1.2	Propiedad de los activos	R			R	S	A					S	S		C			
8.1.3	Uso aceptable de los activos	A	I			R	S	C	S	C			S					I
8.1.4	Devolución de activos	A	I		R	C	A	S	S	S		C	S	S				I
8.2.1	Clasificación de la información	A	I		S	R	C	S										
8.2.2	Etiquetado de la información	A	I			S	R	S	C	C	C	C	S	S				
8.2.3	Manejo de activos	A	I			C	S					C	S	R				
8.3.1	Gestión de medios removibles	A	I			S	S	C					S	R				
8.3.2	Eliminación de medios	A	I			S	A	S				C		R				
8.3.3	Transferencia de medios físicos	A	I			S	C	C						R				I

Control de acceso																		
9.1.1	Política de control de acceso	A			S	R	S	S	C	C				S				I
9.1.2	Acceso a redes y servicios de red	A	I			S	C	S						R				I
9.2.1	Registro y de-registro de usuarios	A				S	C		R					S				
9.2.2	Suministro de acceso a usuarios	A				S	C		S					S				
9.2.3	Gestión de derechos de acceso removibles	A				S								R				I
9.2.4	Gestión de información secreta de autenticación de usuarios	A				S	C	C						R				
9.2.5	Revisión de derechos de acceso de los usuarios	A			C	S	R	S	C					S				
9.2.6	Remoción o ajuste de derechos de acceso	A				S	S	C						R				
9.3.1	Uso de información secreta de autenticación	A	I			S		S						R				
9.4.1	Restricción de acceso a la información	A	I			S	C							R				
9.4.2	Procedimientos seguros de inicio de sesión	A				S	C							R				I
9.4.3	Gestión de contraseñas	A				S	C	S						R				
9.4.4	Uso de privilegios de programas utilitarios	A	I			S	C	S						R				I
9.4.5	Control de acceso al código fuente de las aplicaciones	A	I			S	C	S						R				I
10 Criptografía																		
10.1.1	Política de uso de controles Criptográficos	A	I			S	R	S						S				
10.1.2	Gestión de claves	A				S	R							S				
11 Seguridad Física y Ambiental																		
11.1.1	Perímetro de seguridad física	A	I			S	C	S					R	C				
11.1.2	Controles físicos de entrada	A	I			S	C	S					R	C				
11.1.3	Aseguramiento de oficinas, áreas e instalaciones	A	I			S	C	S					R	C				
11.1.4	Protección contra amenazas externas y ambientales	A	I			S	C	S					R	C				
11.1.5	Trabajo en áreas seguras	A	I			S	C	S					R					I
11.1.6	Áreas de entrada y carga	A	I			S	C	S					R					
11.2.1	Emplazamiento y protección de equipos	A	I			S	C	S					R					I
11.2.2	Servicios de soporte	A				S	C	S					R	C				
11.2.3	Seguridad en cableado	A				S	C	S					S	R				
11.2.4	mantenimiento de equipos	A				S	C	S					R					
11.2.5	Remoción de activos	A	I			S	C	S					R					
11.2.6	Seguridad de equipos y activos fuera de sitio	A	I			S	C	S					C	R				
11.2.7	Eliminación segura o reúso de equipos	A	I			S	C	S					S	R				
11.2.8	Equipo de usuario desatendido	A	I			S	C	S					S	R				
11.2.9	Política de escritorio y pantalla limpia	A	I			S	C	S					S	R				I
12 Seguridad en las Operaciones																		
12.1.1	Procedimientos operativos de Operación	A					C	S						R				I
12.1.2	Manejo del cambio	A	I		S	R	S			S				S	C			
12.1.3	Gestión de la capacidad	A			S	R				S			C	S	C			
12.1.4	Separación de ambientes de prueba y producción.	A			S	R	C	S						S				
12.2.1	Controles antimalware	A			S		C	S		C				R	C			I
12.3.1	Copia de respaldo de la Información. Backup	A			R	S	C			S				S				
12.4.1	Registro de eventos	A			S	S	C	S		S				R				
12.4.2	Protección de la información de registros (Logs)	A			S	S	R	C		S				S				
12.4.3	Registro (Logs) del Administrador y el operador	A				S	R	S						S				
12.4.4	Sincronización de relojes	A					C	S						R				
12.5.1	Instalación de software en sistemas en producción.	A	I			S	C			C				R				
12.6.1	Gestión de las vulnerabilidades técnicas	A				S	S	S						R				
12.6.2	Restricciones en la instalación de software	A	I			S	S	S						R				
12.7.1	Controles de auditoria en sistemas de información	A			S	S	R	S						S	C			

13 Seguridad en comunicaciones																			
13.1.1	Controles de red	A				S	C	S						R				I	
13.1.2	Seguridad en servicios de red.	A				S	C							R				I	
13.1.3	Segregación en las redes.	A				S	C							R	S				
13.2.1	Políticas y procedimientos para transferencia de información.	A	I			S	R							S				I	
13.2.2	Acuerdos de transferencia de información.	A			S	R	S							S					
13.2.3	Mensajería electrónica	A	I		S	S	C				C			R				I	
13.2.4	Acuerdos de confidencialidad y no divulgación.	A			S	S	S		S		R	S		S				R	
14 Adquisición, desarrollo y mantenimiento de sistemas.																			
14.1.1	Análisis y especificación de requisitos en seguridad de la información.	A			C	S	R			C				C	C	I	I		
14.1.2	Aseguramiento de servicios de aplicaciones en redes públicas.	A			C	R	S	S						S	C				
14.1.3	Protección de transacciones en servicios y aplicaciones.	A				S	C	S						R					
14.2.1	Política de desarrollo seguro.	A			C	S	S							S	R	I	I	I	
14.2.2	Procedimiento de control de cambio en sistemas	A			C	S	R			C				S	C				
14.2.3	Revisión técnica de aplicaciones luego de cambios en plataformas de producción.	A				S	R							S					
14.2.4	Restricciones en cambios los paquetes de software.	A				S	S	S						R	C			I	
14.2.5	Principios de la ingeniería en sistemas seguros	A				R	S							S	S				
14.2.6	Ambiente de desarrollo seguro	A				S	S							S	R			R	
14.2.7	Desarrollo tercerizado.	A				S	S	C						S	R				
14.2.8	Prueba de seguridad en los sistemas	A				S	R	S						S	S				
14.2.9	Pruebas de aceptación de los sistemas	A	C			S	S							S	R				
14.3.1	Protección de datos de prueba	A				R	S	S						S	S			I	
15 Relación con los proveedores																			
15.1.1	Política de seguridad de la información para relaciones con los proveedores	A			C	R	S	S								I	I	I	
15.1.2	Incorporación de la seguridad en los acuerdos con los proveedores.				A	S	R				S			S				R	
15.1.3	Cadena de suministro para las tecnologías de la información y las comunicaciones				A	S	R							S					
15.2.1	Supervisión y revisión en los servicios con proveedores	A					S	C						R					
15.2.2	Gestión de cambios a servicios de proveedores	A				S	S							R					
16 Gestión de incidentes de seguridad de la información.																			
16.1.1	Responsabilidades y procedimientos	A				R	S		S		C			S	S				
16.1.2	Reporte de eventos de seguridad de la información	A	I			S	R	S						S	S		I	I	
16.1.3	Reporte de debilidades en la seguridad de la información	A	I			S	R	S						S	S		I	I	
16.1.4	Evaluación y decisiones en eventos de seguridad de la información	A				R	S	S			C			S	S				
16.1.5	Respuesta a incidentes de seguridad de la información	A		C		S	R	S			C			S	S				
16.1.6	Aprendizaje de los incidentes en seguridad de la información	A				R	S	C	C			C	C	C	C	C			
16.1.7	Recolección de evidencia	A					R	S			C			S	S			S	
17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.																			
17.1.1	Planeación de la continuidad de la seguridad de la información	A				S	R							S	S		R	R	I
17.1.2	Implementar la continuidad de la seguridad de la información.				S	S	R							S	S		R	R	R
17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información.						A	R						S	S				R
17.2.1	Disponibilidad en las instalaciones de procesamiento de información.				S	S	A							R	S				R
18 Cumplimiento																			
18.1.1	Identificar requisitos legales y contractuales aplicables.	A	I	C	S	S	S				S			S	S			I	
18.1.2	Derechos de propiedad intelectual	A	I	C	R	S	S				C				S			I	
18.1.3	Protección de registros	A	I	C	R	S	S								S			I	
18.1.4	Privacidad y protección de la información identificable como personal.	A	I	C	S	S	S				R				S			I	
18.1.5	Regulación de controles criptográficos.	A				R					C				S				
18.2.1	Revisión independiente de la seguridad de la información	A			R	S									C				
18.2.2	Cumplimiento con políticas de seguridad y estándares	A	I	C	S	R					C				S		I	I	I
18.2.3	Revisión de cumplimiento técnico	A			S	R					C				S				
	Número de responsabilidades	1	0	0	10	22	22	1	3	1	5	0	11	34	4	2	2	7	125 RESPONSABLE
	Número de responsabilidades	106	0	0	3	1	5	0	0	0	0	0	0	0	0	0	0	0	115 APTOBADOR
	Número de controles soportados	0	0	1	20	81	35	55	10	8	4	3	20	52	5	0	0	1	295 APOYO
	Número de controles sobre los que se consultó	2	1	9	11	3	41	12	6	7	13	6	5	14	11	1	1	0	143 COSULTADO
	Número de controles de los que se informó	0	48	0	0	0	0	0	0	0	0	0	0	0	0	7	7	33	95 INFORMADO