MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ADMINISTRADORA DE LOS RECURSOS DEL SISTEMA GENERAL DE SEGURIDAD SOCIAL EN SALUD

BOGOTÁ, 18 DE MAYO DE 2020

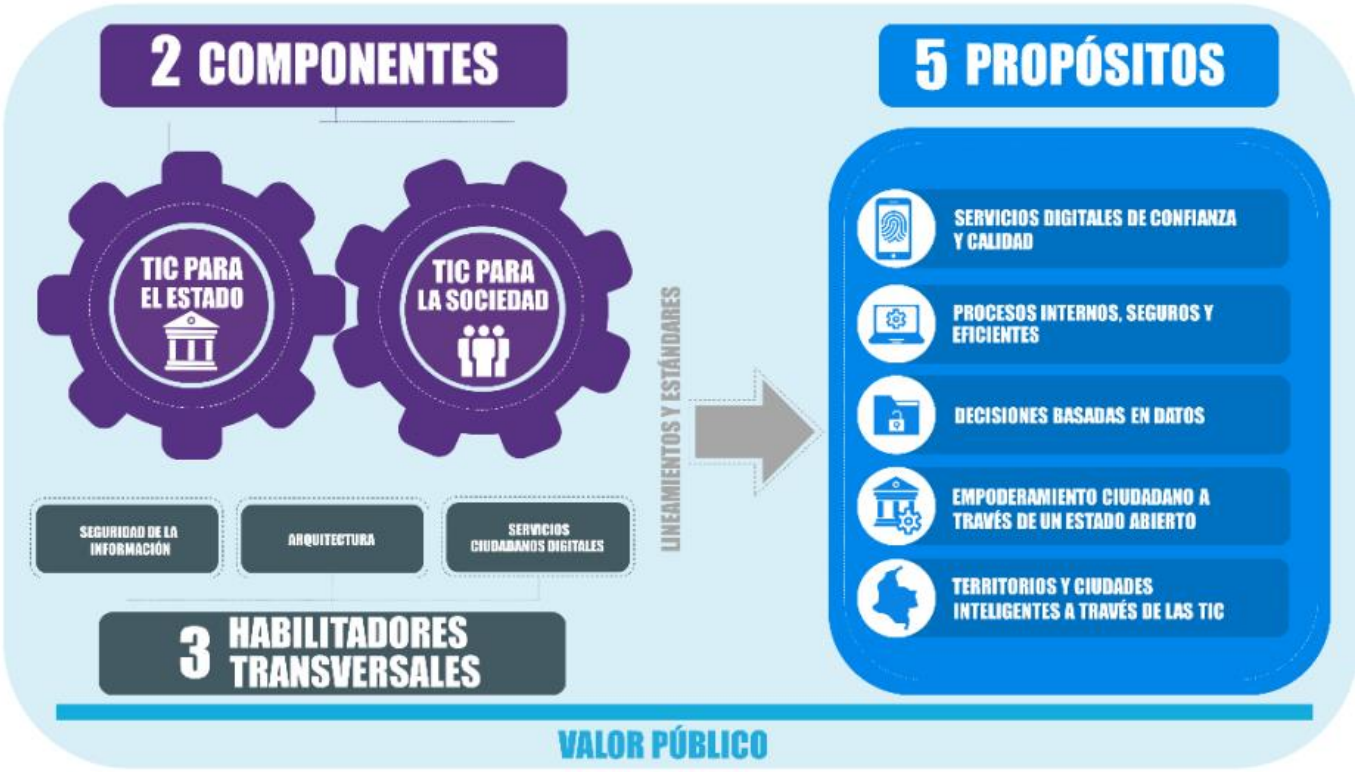
TABLA DE CONTENIDO

MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

En la Administradora de Recursos del Sistema General de Seguridad Social en Salud de ahora en adelante la ADRES o la Entidad, la información es considerada como un activo fundamental para la prestación de sus servicios y la apropiada toma de decisiones; razón por la cual, existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la Continuidad del negocio, Administración de riesgos y Consolidación de una cultura de seguridad de manera progresiva.

Consciente de las necesidades actuales, la ADRES adapta, implementa, revisa y mejora el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. Dicho modelo dentro de la ADRES, es entendido como eje fundamental para el desarrollo del Sistema de Gestión de Seguridad de la Información, el cual es parte integral del conjunto de Sistemas de Gestión desarrollados al interior de la ADRES; cumpliendo adicionalmente como habilitador transversal "Seguridad de la Información" de la Política de Gobierno Digital que este Ministerio ha propuesto[1].



Con esto permite (i) Identificar y minimizar los riesgos a los cuales se expone la información Entendiendo el contexto tanto a nivel interno y externo conforme con el manual operativo de administración de riesgos de la Entidad. (ii) Ayudar a la reducción de costos operativos y financieros,

[1] Manual de Gobierno Digital. (2018). Versión 6. [eBook] Bogotá D.C.: MinTIC, p.17. Disponible en: https://www.mintic.gov.co/portal/604/articles-81473_recurso_1.pdf [Accedido el 26 dic. 2018].

(iii) Establecer una cultura de seguridad y (iv) Promover el cumplimiento de los requerimientos vigentes a nivel legales, contractuales y del negocio.

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 los Directivos, Servidores Públicos, Contratistas y Terceros que tienen responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la ADRES, 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, la Integridad y la Disponibilidad de la información.

2. OBJETIVO

Definir las Políticas Específicas de Seguridad y Privacidad de la Información de la Administradora de Recursos del Sistema General de Seguridad Social en Salud – ADRES; la cuales deben conocer, acoger y poner en práctica todos los Directivos, Servidores públicos, Contratistas y demás partes interesadas que presten sus servicios o tengan algún tipo de relación con la Entidad. Esto con el propósito de fomentar e incentivar de manera progresiva la cultura de Seguridad y Privacidad dentro de la Entidad, la cual permee la cultura organizacional actual.

3. ALCANCE

El presente Manual de Políticas Específicas de Seguridad y Privacidad de la Información abarca todos los procesos de la Entidad e incluye a los Directivos, Servidores públicos, Contratistas y demás partes interesadas[2] del Sistema de Gestión de Seguridad de la Información. De igual manera cabe precisar que las políticas de Seguridad de la Información aquí mencionadas están alineadas con la norma ISO 27001 Versión 2013.

4. TERMINOS Y DEFINICIONES

Activo de Información. Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (Datos, aplicaciones, personas, servicios, tecnología, instalaciones, equipo auxiliar) que tenga valor para la Entidad. Se clasifica de la siguiente manera: (i) Datos: Elementos básicos de información que cumplen con el ciclo de generación (recolección), almacenamiento, trasmisión y eliminación. (ii) Aplicaciones: Es todo el Software que se utiliza para la gestión de la información. (iii) Personas: Todo tipo de persona involucrada con las actividades de la ADRES y que tengan acceso de una u otra manera a los activos de Información de la Entidad. (iv) Servicios: Actividades que se suministran tanto a nivel interno como externo con el propósito de cumplir una necesidad explicita para el usuario. (v) Tecnología: Hace referencia a todos los equipos que son utilizados para la gestión de la información y las comunicaciones dentro de la ADRES. (vi) Instalaciones: Ubicaciones en donde se alojan los sistemas de información. (vii) Equipamiento auxiliar: Son todos aquellos activos que dan soporte a los sistemas de información y que no se han referenciado en alguna otra categoría.

Amenaza. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

[2] Ver Anexo 1. Análisis de las Partes Interesadas

Análisis de riesgos cualitativo. Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo. Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Ciberdefensa: Según CONPES 3701 de 2011 es la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

Ciberseguridad: Según CONPES 3701 de 2011 es la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Confidencialidad. Según la norma ISO/IEC 27002:2013 es la propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Credencial de grupo. Conjunto de identificadores de usuarios y contraseñas que son asignados a un grupo de Servidores públicos o Contratistas, con un propósito particular, para el acceso de a un Sistema de Información o Servicio dentro de la Entidad.

Credencial de usuario. Conjunto de identificadores de usuarios y contraseñas que son asignados a una persona de manera única e intransferible con el propósito de acceder a un Sistema de Información o Servicio dentro de la Entidad.

Criptografía. Es la ciencia que resguarda documentos y datos que actúa a través del uso de las cifras o códigos para escribir algo secreto en documentos y datos que se aplica a la información que circulan en las redes locales o en internet.

Desastre. Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva o directriz. Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según la norma ISO/IEC 27002:2013 Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo, y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo.

Evaluación de riesgos. Proceso global de identificación, análisis y estimación de riesgos.

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.

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Incidente de Seguridad: Según la norma ISO/IEC 27002:2013 es evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: De acuerdo con la Ley 1712 de 2014 "por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones", es un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Infraestructura crítica: De acuerdo con el CONPES 3701 de 2011 es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación.

Integridad: En consideración a la norma ISO/IEC 27002:2013 es la propiedad de la información relativa a su exactitud y completitud.

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

Llaves criptográficas. Es una pieza que contiene información que controla la operación de un algoritmo de criptografía.

Logs: Dentro del CONPES 3701 de 2011 se define como un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SSI a nivel mundial.

Medio extraíble. Se entiende como aquellos soportes de almacenamiento diseñados para ser extraídos de un computador sin tener que apagarlo. Algunos de estos están diseñados para ser leídos por lectoras y unidades también extraíbles. Como: (i) Discos ópticos (Disco compacto, DVD, Blu-ray). (ii) Disquetes, discos Zip. (iii) Cintas magnéticas. De igual manera, también puede hacer referencia a algunos dispositivos (y no medios) de almacenamiento extraíbles, cuando éstos son usados para transportar o almacenar algún tipo de información, tales como: (i) Memorias USB. (ii) Discos duros externos. (iii) Tarjeta de memoria.

No repudio: Según CCN-STIC-405:2006 el no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según OSI ISO-7498-2 servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Parte interesada. Es una persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad relevantes a los Sistemas de Gestión de la Entidad.

Plan de continuidad del negocio. Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

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.

Privacidad[3]: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Riesgo: Según la norma ISO/IEC 27002:2013, es la 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.

Seguridad de la información. Es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información

Seguridad informática. Se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

Teletrabajo. Todas las formas de trabajo fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se les denomina "trabajo a distancia", "Lugar de trabajo flexible", "Trabajo remoto" y ambientes de "Trabajo Virtual".

Trazabilidad. Según CESID:1997 es la cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad: De acuerdo con la ISO/IEC 27002:2013, es la debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5. MARCO NORMATIVO

- Constitución Política de Colombia de 1991. Artículo 15, mediante el cual se reconoce el Habeas Data como Derecho Fundamental. Artículo 20, Derecho a la Libertad de Expresión y de Prensa.
- Ley 23 de 1982 "Sobre derechos de autor".
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

[3] Modelo de Seguridad y Privacidad de la Información. (2017). 3rd ed. [eBook] Bogotá D.C.: MINTIC, p.15. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf [Accedido el 26 dic. 2018].

- Ley 1273 de 2009, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- Ley 1341 de 2009, "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC– se crea la Agencia Nacional de Espectro y se dictan otras disposiciones".
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1474 de 2011, Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital.
- Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- Ley 1952 de 2019 "Por medio de la cual se expide el código general disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario".

6. RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

En relación con la seguridad de la información, Se han definido los siguientes 10 roles:

- Director(a) General Comité Institucional de Gestión y Desempeño
- Director Gestión de Tecnología de Información y Comunicaciones
- Líder de Seguridad
- Líderes de proceso
- Enlaces de proceso
- Jefe Oficina Asesora de Planeación y Control de Riesgos
- Jefe Oficina Control Interno
- Jefe Oficina Asesora Jurídica
- Director(a) Administrativo y Financiero

A continuación, se presenta la siguiente Matriz RACI[4], en la cual se realiza un mapeo de los roles y su relación con las responsabilidades asociadas al Sistema de Gestión de Seguridad y Privacidad de la Información.

Responsabilidad	Director(a) General	Comité Institucional de Gestión y Desempeño	Director Gestión de Tecnología de Información y Comunicaciones	Líder de Seguridad	Líderes de proceso	Enlaces de proceso	Jefe Oficina Asesora de Planeación y Control de Riesgos	Jefe Oficina Control Interno	Jefe Oficina Asesora Jurídica	Director(a) Administrativo y Financiero
Establecer Políticas Generales y Específicas de Seguridad de la Información	I	A	C	R	I	I				
Establecer roles y responsabilidades de seguridad de la información	A	C	C	R	I					
Establecer y documentar procedimientos de seguridad de la información en componente tecnológico		I	A	R	I					
Establecer y documentar procedimientos de seguridad de la información en componente administrativo		I	I	C		R				A
Identificar legislación aplicable y de los requisitos contractuales	I	A	C	R	I				R	R
Asignar el presupuesto adecuado y suficiente para destinar y proporcionar los recursos necesarios	A	I	C	R						I
Realizar levantamiento y clasificación de activos de información de los procesos		A		R	C	R			C	
Realizar análisis de Riesgos de Seguridad de la Información	I	A	I	R	R	R	C	I		
Implementar plan de tratamiento de riesgos de Seguridad de la Información		A	C	R	R	R	I	I		

[4] Matriz RACI: Conocida como matriz de responsabilidades porque sirve para establecer las responsabilidades de cada actor que participa en una tarea. En los roles de: Responsable (R), Aprobador (A), Consultado (C) e Informado (i).

La matriz se construye con una tabla donde por filas tenemos tareas y por columnas actores.

Definir e implementar planes de mejora frente a hallazgos en Seguridad de la Información catalogados con criticidad Bajo y Medio			A	R	C			I	I	I
Definir e implementar planes de mejora frente a hallazgos en Seguridad de la Información catalogados con criticidad Alto		A	R	R	C			I	I	I
Implementar controles de Seguridad de la Información		A	C	R	I	I				
Diseñar y ejecutar plan de sensibilización y capacitación en Seguridad de la Información		A	C	R	I	I				
Realizar análisis de impacto del negocio	I	A	I	C	R	R				
Establecer el plan de Continuidad de Negocio para la Entidad	I	R		I	C	I				
Establecer el plan de Continuidad de Recuperación de Servicios de TI		A	R	R	I				C	C
Establecer planes de contingencia a nivel de procesos		A	C	I	R				C	C
Realizar evaluaciones independientes del nivel de madurez del modelo de Seguridad de la Información en la Entidad	I	I	C	C	C	C		R/A		
Definir e implementar planes de mejora frente a hallazgos en Seguridad de la Información		I	C	R	C	R		A		

7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Política General

La Política General de Seguridad y Privacidad de la Información con el código de formato GPDI- P01, se encuentran aprobada por la Dirección General y está disponible en el portal Web de la Entidad (www.adres.gov.co) en la sección de Transparencia.

7.1 Obligaciones y Deberes del Recurso Humano

- Los grupos internos de Gestión de Talento Humano y Gestión de Contratación de la Dirección Administrativa y Financiera de la ADRES son los encargados de realizar las verificaciones frente a estudios de seguridad que vean pertinentes, con el propósito de confirmar la veracidad de la información suministrada por el candidato a ocupar un cargo, ya sea como Servidor Público o como Contratista.
- En el momento de posesión del cargo por parte de un Servidor Público, éste debe firmar y posteriormente cumplir el Compromiso de confidencialidad y no divulgación de información que la Dirección Administrativa y Financiera tenga definido. Dicho compromiso refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administrada por los mismos. De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada, entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. Adicionalmente, dentro de dicho compromiso se debe establecer, asimismo, la vigencia de este acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

- En el caso de vinculación contractual la Dirección Administrativa y Financiera debe validar que el Compromiso de Administración y manejo integro de la información interna y externa haga parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información. Adicionalmente, dentro de dicho contrato se debe establecer asimismo la vigencia de este acorde al tipo de vinculación del personal al cual aplica el cumplimiento.
- Para los cargos donde se realicen labores sensibles o sean identificados como susceptibles a corrupción, se debe realizar la segregación de funciones entre diferentes Servidores Públicos o contratistas con el fin de mitigar el mal uso de la información ya sea por acciones deliberadas o por negligencia.
- Es responsabilidad de cada líder de proceso junto con la colaboración de la Dirección Administrativa y Financiera verificar periódicamente las funciones, medidas aplicadas y controles de los cargos sensibles o sean identificados como susceptibles a corrupción y de ser necesario reevaluar el nivel de riesgo asociado al proceso; esto de acuerdo con el Sistema de Administración de Riesgos Integrados de la Entidad que la Oficina Asesora de Planeación y Control de Riesgos lidera.
- Las cuentas de usuario de los Contratistas de la ADRES una vez cumplan su vínculo contractual serán inactivadas por parte de la Dirección de Gestión de Tecnologías de Información y Comunicaciones, para lo cual el grupo interno de Gestión de Contratación deberá informar oportunamente las vigencias de los diferentes contratos y sus prorrogas que se tengan en las dependencias de la Entidad.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones definirá anualmente el plan de capacitación y sensibilización frente a Seguridad de la Información, el cual debe estar articulado con el Plan Institucional de Capacitación que la Dirección Administrativa y Financiera defina.
- La Dirección Administrativa y Financiera en cabeza del Grupo Interno de Talento Humano realizará revisión periódica de los resultados de capacitaciones para mejoramiento de los procesos entorno a la Seguridad de la Información.
- Los Servidores Públicos, contratistas y terceros de la ADRES sin excepción deben:
  - Cumplir a cabalidad la política General de Seguridad y Privacidad de la Información, así como las directrices definidas en las políticas específicas del presente Manual de acuerdo con su rol y funciones que desempeña dentro de la Entidad.
  - Dar adecuada gestión a las diferentes credenciales de usuario o llaves criptográficas que les sean asignadas, teniendo en cuenta que estas son de uso personal e intransferibles; El usuario debe cambiar periódicamente las claves de acceso de estas (cuando aplique) de acuerdo con las condiciones de complejidad que sean definidas para cada una de ellas.
  - Dar adecuada gestión a las diferentes credenciales de grupo que les sean asignadas y usarlas de manera única para las finalidades que se le hayan asignado.
  - Evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado por parte de la Dirección de Gestión de Tecnologías de Información y Comunicaciones.
  - No usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.
  - Conservar tanto los escritorios físicos como digitales libres de información clasificada y reservada propia de la Entidad – Política de escritorios limpios. Con el propósito de lograr niveles óptimos de confidencialidad de esta al no poder ser consultada, copiada o utilizada por todo tipo de personal que no tenga autorización para su uso o conocimiento.
  - Hacer uso adecuado y eficiente de los recursos tales como estaciones de trabajo y periféricos asignados por la Dirección Administrativa y Financiera, con el único fin de llevar a cabo las labores y funciones que se le han definido dentro de la Entidad.

- Bloquear su estación de trabajo en el momento que no se encuentre utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Permitir tomar el control remoto de sus equipos para el soporte técnico, previo cierre por parte del usuario de los archivos con información sensible. Adicionalmente, el usuario no debe desatender el equipo mientras tenga el control de la máquina un tercero. Para esto, el acceso remoto se debe realizar mediante herramientas autorizadas por la Dirección de Gestión de Tecnologías de Información y Comunicaciones.
- Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.
- En el momento de desvinculación o cambio de labores se debe realizar la entrega formal del puesto de trabajo al jefe inmediato o quien este delegue de acuerdo con los procedimientos que desde los grupos internos de Gestión de Talento Humano y Gestión de Contratación de la Dirección Administrativa y Financiera -DAF se tengan definidos. Así mismo, deben encontrarse a paz y salvo con la entrega de los Equipos Tecnológicos, Periféricos y otros Activos de Información suministrados por las instancias respectivas desde el momento de su vinculación o producto de su actividad laboral.
- De igual manera, al momento de una desvinculación laboral con la entidad, todo funcionario y/o contratista debe dejar consignado por escrito, su compromiso de confidencialidad e integridad con el cual garantice no divulgar información reservada y que pueda comprometer la seguridad de la entidad, Esto conforme con las directrices que la la Dirección Administrativa y Financiera de la ADRES defina para tal fin.
- Participar de las jornadas de Capacitación en Seguridad de la Información, que sean definidas dentro del Plan Institucional de Capacitación que la Dirección Administrativa y Financiera defina para cada una de las vigencias.

- La ADRES cuentan con los grupos de emergencia, brigadistas y planes de evacuación que la Dirección Administrativa y Financiera ha definido, los cuales deben ser revisados y socializados como mínimo una vez en el año a todo el personal de la Entidad.

7.2 Gestión de Activos de Información

- La ADRES define, publica, revisa y actualiza el Inventario de Activos de Información por lo menos dos veces al año conforme a la ejecución del Procedimiento Gestión de Activos de información que la Dirección de Gestión de Tecnologías de Información y Comunicaciones ha definido para tal fin. Para lo cual, los líderes de procesos o quien haga sus veces deben gestionar con el responsable designado la identificación, valoración y clasificación de sus activos de información dentro del inventario.
- La ADRES es la propietaria de los activos de información a excepción de los que se han clasificado como personas. Por su parte, los responsables de estos son los servidores públicos, contratistas o demás colaboradores que estén autorizados a: (i) Manejo de la Información de acuerdo con los procesos a su cargo. (ii) Uso de los diferentes Sistemas de Información o Aplicaciones Informáticas. (iii) Uso del Hardware o infraestructura de tecnologías de información y comunicaciones.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones es:
  - La responsable de los activos de información correspondientes a la infraestructura tecnológica de la ADRES, exceptuando las estaciones de trabajo, teléfonos u otros dispositivos asignados a los diferentes funcionarios y contratistas por la Dirección Administrativa y Financiera. En consecuencia, debe asegurar su apropiada operación y

administración. La instalación, cambio o eliminación de componentes de la plataforma tecnológica se debe realizar conforme al Procedimiento de Gestión de Cambios que ha adoptado la Entidad.
  - Debe efectuar una revisión periódica de los programas, sistemas de información, servicios tecnológicos que son utilizados en cada dependencia y notificar al Oficial de Seguridad cualquier irregularidad frente a los mismos.
  - Con el fin de asegurar el no repudio, debe definir las acciones pertinentes para poder hacer seguimiento a la creación, origen, recepción, entrega de información u otro activo de información. Así mismo, debe definir el periodo de retención o almacenamiento de los registros de auditoria realizados por los usuarios a través de las aplicaciones, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad, esto conforme a los procedimientos que al interior de esta Dirección se definan.
- Las herramientas de seguridad que se implementen en la Entidad tienen carácter de uso corporativo y por tal razón, es obligatoria su instalación y uso en la infraestructura tecnológica. Por tanto, cualquier equipo que no cuente con los controles establecidos, no podrá ser conectado a la red de datos de la Entidad.
- El almacenamiento de archivos tales como documentos, vídeo, música o fotos, entre otros; que no sean de carácter institucional no está permitido realizarlo en las unidades de almacenamiento colaborativo o histórico que la Dirección de Gestión de Tecnologías de Información y Comunicaciones ha definido.
- El retiro parcial o definitivo de estaciones de trabajo o Activos de Información asignados a los Servidores Públicos o Contratistas se debe hacer de acuerdo con lo definido en la Entidad dentro de la guía de Gestión Administrativa definida por la Dirección Administrativa y Financiera. Para lo cual, la empresa de Servicios de Seguridad Física que este contratada debe hacer efectivo control de acuerdo con los lineamientos definidos.
- Para acceder a los servicios de impresión (impresora, escáner o fotocopiadora) los usuarios deben manejar de manera individual e intransferible una contraseña, la cual es entregada por la Dirección Administrativa y Financiera en el momento en el cual este inicia labores o contrato en la Entidad. Una vez impresos documentos con información pública clasificada o pública reservada estos deben ser retirados de las impresoras inmediatamente.
- El mantenimiento, reparaciones o cambio de consumibles de los servicios de impresión, así como la dispensación de la papelería es responsabilidad exclusivamente del Recurso Humano que la Dirección Administrativa y Financiera destine para tal fin a título propio o tercerizado.
- La información institucional que se genere por parte de los servidores públicos, contratistas y terceros se debe almacenar dentro de los servicios de almacenamiento que la Entidad disponga para tal fin. Por tal razón, el almacenamiento de información que se genere directamente sobre las estaciones de trabajo no es permitido y de hacerse es de responsabilidad única del Servidor Público o Contratista que lo realice.
- En el caso que algún medio vaya a ser destruido o eliminado del inventario, se debe llevar un proceso de borrado seguro de los mismos de acuerdo con lo definido dentro del Procedimiento Gestión de Requerimientos y guías anexas que han sido definido por la Dirección de Gestión de Tecnologías de Información y Comunicaciones. Así mismo, se realizará la respectiva actualización al inventario de Activos.
- Los Activos de información que sean considerados como uso exclusivo de usuarios privilegiados se encuentran destinados exclusivamente para los usuarios administradores que desde la Dirección de Gestión de Tecnologías de Información y Comunicaciones se les haya concedido dicho permiso, para lo cual se debe:
  - Limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados.
  - Limitar la disponibilidad de los programas utilitarios.
  - Registrar el uso de los programas utilitarios.

- Definir y documentar los niveles de autorización para los programas utilitarios.
- Retirar o deshabilitar todos los programas utilitarios innecesarios.

- De acuerdo con lo anterior, la ADRES garantiza el inventario, propiedad, uso aceptable, devolución de los activos de información.

7.3 Clasificación de la Información

- La clasificación, tratamiento y control de la información se realiza para todas las dependencias de la Entidad en concordancia con la legislación colombiana vigente y conforme a la Metodología de Clasificación y Valoración de Activos de Información que la Dirección de Gestión de Tecnologías de Información y Comunicaciones ha definido para tal fin de acuerdo con lo definido dentro de la resolución 3589 de 2018 y las posteriores que se puedan llegar a generar relacionadas a dicha finalidad.
- Dentro de la ADRES todos los documentos físicos estarán etiquetados, de acuerdo con las tablas de retención documental de la Entidad y el Índice de Información Clasificada y Reservada adoptado, el cual se encuentra definido en la Metodología de Clasificación y Valoración de Activos de Información. A su vez, el manejo, custodia y préstamo de dichos documentos se debe realizar de acuerdo con las medidas que defina la Dirección Administrativa y Financiera buscando controlar el acceso no autorizado a contenidos que en ellos resida.
- Tomando como insumo lo definido dentro de la Guía de Identificación y Clasificación de Activos de Información y las tablas de retención Documental, el reúso de papel como reciclaje está totalmente prohibido si en este se encuentra información catalogada como Pública Clasificada o Pública Reservada. Por tal razón, la Dirección Administrativa y Financiera definirá dentro de sus guías como se debe hacer la correcta eliminación de documentos físicos indicando adicionalmente, las características que se deben cumplir cuando estos contengan información catalogada como clasificada o reservada.
- El líder de cada proceso o quien este delegue es el encargado de realizar la solicitud de servicios de almacenamiento para la información que al interior de cada proceso se realice teniendo en cuenta el propósito de esta, el cual se puede definir en: (i) De Gestión y acceso concurrente. (ii) Histórico acceso esporádico y de consulta. Dicha solicitud debe ser dirigida a la Dirección de Gestión de Tecnologías de Información y Comunicaciones, de acuerdo con lo definido dentro del procedimiento de Gestión Requerimientos. Adicionalmente, debe indicar a sus equipos de trabajo que: (i) La información no debe ser redundante. (ii) No debe contener archivos ejecutables o que se detecten con algún tipo de código malicioso. (iii) Deben aplicar la compresión de los archivos que tienen un gran tamaño. (iv) Mantener depurada la información que se encuentra almacenada en los servicios de almacenamiento de archivos red de la Entidad.
- El tipo de archivo a almacenar en los servicios de almacenamiento de la ADRES, debe ser coincidente con los programas licenciados por la ADRES o en su defecto a aquellos programas de licencia libre y que su uso este permitido a nivel Corporativo.
- De acuerdo con lo anterior, la ADRES garantiza la clasificación, etiquetado y manejo de los activos de los activos de información.

7.4 Control de Acceso

- La Dirección de Gestión de Tecnologías de Información y Comunicaciones de acuerdo con las necesidades de las diferentes dependencias es la encargada de establecer las configuraciones de los niveles de acceso lógico a los Activos de Información de los cuales dicha Dirección es responsable de la administración técnica. De igual manera, en el caso que otra dependencia sea la responsable será esta la que a su vez realiza la respectiva gestión.

- Dentro de la ADRES el control de Acceso se encuentra definida dentro del procedimiento Gestión de Control de Acceso en el marco del proceso Soporte y Operación TIC.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones tendrá la potestad de revocar los accesos de los Contratistas al finalizar cada año; para lo cual, informará previamente a los directores y jefes de oficina las condiciones de fecha de bloqueo a aplicar dentro de cada proceso de inactivación de usuarios.
- La Entidad cuenta con un control centralizado e inventario de licencias para la instalación de Software y cambios de configuración del sistema. Por lo tanto, los Servidores Públicos, Contratistas o Terceros que tengan asignada una estación de trabajo no deben tener privilegios de usuario administrador excepto las personas que desde la Dirección de Gestión de Tecnologías de Información y Comunicaciones se les haya concedido dicho permiso. Por consiguiente, es deber de los usuarios finales informar oportunamente cuando sus credenciales de acceso permitan instalar programas o hacer cambios de configuración al equipo asignado.
- El acceso a los Activos de Información que requieran credenciales de usuario debe cumplir como mínimo con las siguientes consideraciones de seguridad:
  - Longitud mínima de la contraseña superior a 8 caracteres.
  - Manejo como mínimo de 3 de los siguientes tipos de caracteres: minúsculas, mayúsculas, números, caracteres especiales (símbolos).
  - Duración máxima de la contraseña.
  - Histórico de contraseñas. Llevar un registro de las contraseñas usadas previamente, e impedir su reusó continuamente.
  - Mecanismos de auditoria.
  - Autogestión de contraseñas. Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada.
  - Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez.
  - Exigir por que se cambien las contraseñas en forma regular, según sea necesario.
  - Almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones.
  - Almacenar y transmitir las contraseñas en forma protegida.
  - Se debe contar con un perfilamiento de usuarios para permitir el acceso solo a los módulos, funcionalidades, reportes acordes al mismo, dicho perfilamiento deberá ser revisado periódicamente por los administradores de los sistemas de información.

  En el caso que por arquitectura de los sistemas de información u otro servicio que cuente con contraseñas de acceso y no puedan cumplir con las características antes relacionadas, la Dirección de Gestión de Tecnologías de Información y Comunicaciones debe definir un plan de mejoramiento frente al cumplimiento de las consideraciones ya descritas.
- Los equipos de uso personal, que no son de propiedad de la ADRES, solo tienen acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser únicamente conectados a los puntos de acceso autorizados y definidos por la Dirección de Gestión de Tecnologías de Información y Comunicaciones de la ADRES.
- La Dirección Administrativa y Financiera es la encargada de la definición de las directrices necesarias para el personal (Altos Directivos, Directivos, servidores públicos, visitantes, contratistas, proveedores) frente Acceso Físico a las instalaciones de la ADRES esto de acuerdo con lo consignado dentro de la Guía Gestión Administrativa que se ha desarrollado para tal fin. De igual manera, es quien debe mantener actualizado el programa de Seguridad Física y mantenimiento de las instalaciones pertenecientes a la Entidad.
- Los Sistemas de Información de la ADRES deben contar con las siguientes consideraciones:
  - Permitir el uso sólo a los usuarios autorizados
  - Evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado a acceder al sistema;

- Validar la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.
- Proteger contra intentos de ingreso mediante fuerza bruta.
- Llevar un registro con los intentos exitosos y fallidos;
- Declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso.
- Visualizar en la pantalla principal del sistema de Información, la siguiente información al terminar un ingreso seguro:
  - Registrar la fecha y la hora del ingreso previo exitoso;
  - Registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso
- No visualizar una contraseña que se esté ingresando
- No transmitir contraseñas en un texto claro en una red;
- Terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles.
- Restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.
- Suministrar menús para controlar el acceso a las funciones de sistemas de aplicaciones.
- Controlar a qué datos puede tener acceso un usuario particular
- Controlar los derechos de acceso de los usuarios tales como: (i)Lectura, (ii) Escritura. (iii) Borrado y (iv) ejecución.
- Controlar los derechos de acceso de otras aplicaciones.
- Limitar la información contenida en los elementos de salida.

- Dentro de la ADRES se han definido áreas de acceso restringido destinadas para la protección de activos de información vitales como unidades de procesamiento (servidores, almacenamiento) o donde se maneje Información Sensible para lo cual se debe considerar:
  - Las áreas restringidas deben contar con sistemas de control de acceso, sistema de video vigilancia o en su defecto deben estar cerradas con llave; dicho control de acceso se debe revisar periódicamente por parte de la Dirección Administrativa y Financiera o el tercero que esta delegue.
  - El acceso a las áreas restringidas se debe hacer llevando un registro de fecha y hora de entrada y salida del personal que ingresa; cuando se requiera de acuerdo con la sensibilidad de la información que se maneja.
  - En los casos que se determine áreas restringidas críticas la Dirección Administrativa y Financiera y la Dirección de Gestión de Tecnologías de Información y Comunicaciones de la ADRES podrá determinar el no uso de dispositivos móviles dentro de la estancia del personal en dichas áreas.
  - El uso de dispositivos para la captura de material fotográfico y/o videos está prohibido dentro de las áreas accesos restringido; salvo cuando se cuente una autorización temporal dada por parte de la Dirección Administrativa y Financiera.

7.5 Adquisición o Desarrollo de Sistemas de Información

- La Dirección de Gestión de Tecnologías de Información y Comunicaciones debe establecer, documentar, ejecutar y actualizar la Metodología de desarrollo de la Entidad, la cual se debe validar por lo menos una vez al año conforme a la situación actual de los Sistemas de Información de la Entidad y la Infraestructura tecnológica que los soporta. Así mismo, dicha metodología definirá las características que deben cumplir los manuales técnicos, de usuario y

diccionario de datos de los diferentes Sistemas de Información, los cuales deben ser revisados y actualizados conforme a los cambios que se generen en estos.

- La Dirección de Gestión de Tecnología de Información y Comunicaciones debe verificar que los desarrollos de la Entidad estén completamente documentados, de acuerdo con la metodología de desarrollo seleccionada al interior de esta, la cual debe cumplir con:
  - Definición de la seguridad del ambiente de desarrollo.
  - Orientar la seguridad en el ciclo de vida de desarrollo del software.
  - Establecer las directrices de codificación seguras para cada lenguaje de programación usado.
  - Definir los requisitos de seguridad en la fase diseño.
  - Definir los puntos de chequeo de seguridad dentro de los hitos del proyecto.
  - Establecer los repositorios de información que cumplan con características de seguridad
  - Definir las condiciones de seguridad en el control de la versión.
  - Definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.
- El paso del ambiente de pruebas a producción de los Sistemas de Información se realiza de acuerdo con lo definido dentro del procedimiento Gestión de Cambios que se ha definido dentro de la Entidad, en donde se debe:
  - Identificar y registrar cambios significativos.
  - Efectuar análisis del riesgo frente al cambio.
  - Planificar el proceso del cambio.
  - Probar el cambio en los ambientes definidos para tal fin.
  - Comunicar a las partes interesadas frente al momento en que se realizará el cambio, para así determinar si se activan o no procedimientos de Contingencia.
  - Indicar los pasos necesarios que se deben tener en cuenta si se requiere revertir el cambio (rollback).
- Los Sistemas de Información deben contar con validaciones que garanticen la consistencia de la información que se registra, de igual manera deben contar con controles que permitan el manejo de errores y la seguridad durante el procesamiento de la información.
- Con el fin de garantizar la segregación de ambientes, para los desarrollos propios de la Dirección de Gestión de Tecnología y Comunicaciones se tienen separados los ambientes de desarrollo, pruebas y producción, en diferentes equipos o servidores y segmentos de red. Esta segregación se debe aplicar de igual manera para los desarrollos de terceros.
- La Dirección de Gestión de Tecnología de Información y Comunicaciones debe desarrollar y/o adquirir el software requerido por la ADRES; de manera coordinada con la Dirección u oficina que manifieste la necesidad del Software.
- La Dirección de Gestión de Tecnología y Comunicaciones debe establecer claramente los requerimientos no funcionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información de acuerdo con lo definido en los procedimientos de Gestión de Proyectos de Información y la metodología de desarrollo definida dentro de la Entidad.
- La Dirección de Gestión de Tecnología de Información y Comunicaciones dentro de su metodología para desarrollo define las estrategias para analizar la seguridad en los sistemas de información; indicando como no usar datos sensibles cuando sea posible en ambientes de desarrollo y prueba.
- La Dirección de Gestión de Tecnología de Información y Comunicaciones frente al código fuente de los sistemas de información debe:
  - Proteger las librerías de código fuente de los diferentes sistemas de información.
  - Establecer que el personal de soporte debe tener acceso restringido a las librerías de las fuentes de los programas.
  - Mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de Control de Cambios.

- Definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los ingenieros encargados sólo se deben hacer una vez que se haya recibido autorización apropiada.
- Conservar un registro de auditoría de todos los accesos a las librerías de fuentes de programas.
- Mantener actualizado el inventario de sistemas de Información, que se deben mantener en un entorno seguro.

7.6 Gestión de Intercambio de información

- Posterior a su generación y consolidación toda información que sea solicitada por un tercero debe ser validada y autorizada la entrega por parte del Líder del proceso responsable de dicho Activo de información, con el propósito de generar el no repudio de la misma. Adicionalmente, en el caso que se defina que esta debe ser entregada en medios extraíbles, se debe comprimir y cifrar usando las herramientas que la Dirección de Gestión de Tecnologías de Información y Comunicaciones ha dispuesto para tal fin.
- Con el propósito de cumplir con la ley Protección de Datos Personales, en lo posible se debe intercambiar información anonimizando los mismos; siempre y cuando el requerimiento de intercambio así lo permita.
- En el caso de requerir una trasferencia o trasmisión de información la Dirección u Oficina propietaria de la misma y la Dirección de Gestión de Tecnologías de Información y Comunicaciones deben definir, documentar y probar los mecanismos, forma y controles automáticos que se deben implementar para el intercambio. Así mismo, se debe determinar si es necesario o no la suscripción o no de algún convenio o acuerdo entre la ADRES y el solicitante de la información, caso para el cual La Oficina Asesora Jurídica o el Grupo interno de Contratación apoyará en la definición jurídica de este.
- En el caso de requerir una trasferencia o trasmisión de información la Dirección de Gestión de Tecnologías de Información y Comunicaciones debe:
  - Definir el uso de firmas, certificados electrónicos o cifrado por cada una de las partes involucradas en el intercambio de información, conforme al objeto y a la arquitectura de los Sistemas de Información y Servicios que soportarán dicha acción.
  - Definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique;
  - Conforme al propósito del intercambio, definir que la información permanezca confidencial.
  - Definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados;
  - Validar que el almacenamiento de los detalles del intercambio esté afuera de cualquier entorno accesible públicamente.
  - Utilizar una autoridad confiable para los propósitos de emitir y mantener firmas o certificados digitales.
- Está restringida la copia de archivos en medios removibles de almacenamiento como dispositivos USB; en caso de ser necesario realizar algún proceso de copia de información en dichos medios, por parte del director, jefe de la dependencia o del coordinador del grupo interno en donde se presenta la necesidad debe realizar la solicitud de acceso temporal a través de la mesa de Servicios de la Dirección de Gestión de Tecnologías de Información y Comunicaciones.
- La mensajería instantánea en la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES, está asociada a los servicios de correo electrónico del dominio @adres.gov.co. Por tanto, no está permitido intercambiar información de la Entidad a través de otras plataformas de mensajería, no obstante, en caso de requerirse otro medio debe

solicitarse concepto al grupo Interno de Soporte de tecnologías de la Dirección de Gestión de Tecnologías de Información y Comunicaciones.

- Los Servidores Públicos, Contratistas y Terceros de la ADRES que se les asigna una cuenta de correo electrónico corporativo la deben usar con carácter Institucional; por tal razón, tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los servidores públicos, contratistas y el personal provisto por terceras partes dentro de la ADRES.
- Los servidores públicos, contratistas y demás colaboradores de la ADRES en ninguna circunstancia tienen permitido el envío vía correo electrónico de archivos que contengan archivos ejecutables o con algún tipo de programa maligno (malware).
- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asume la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reportar inmediatamente a la mesa de servicio (Soporte de primer nivel) de la ADRES, en donde se validará la pertinencia para generar un caso de incidentes de seguridad o gestionarlo como un requerimiento.
- Dentro de la configuración del correo electrónico se deber configurar la siguiente nota (disclaimer):

  El contenido de este mensaje y sus anexos son propiedad la Administradora de Recursos del Sistema General de Seguridad Social en Salud - ADRES, es únicamente para el uso del destinatario ya que puede contener información reservada o clasificada; las cuales no son de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso de este, así como cualquier acción que se tome respecto a la información contenida, por personas o Entidades diferentes al propósito original de la misma, es ilegal. Si usted es el destinatario, le solicitamos dar un manejo adecuado a la información; de presentarse cualquier suceso anómalo, por favor informarlo al correo mesadeservicios@adres.gov.co.
- La información que se publique dentro de las Redes Sociales de la Entidad debe cumplir con los criterios definidos dentro del Plan de Comunicaciones de ADRES, el cual está a cargo de la Dirección General de la Entidad. De igual manera dentro de este plan se encuentra definidos los responsables de la administración de dichas redes dentro de la Entidad.
- No se debe utilizar el nombre de la Entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de las funciones, propósito de la Entidad.
- La información que publique o divulgue cualquier Servidor Público, Contratista o Tercero de la ADRES, que sea creado a nombre personal por alguno de estos en las diferentes Redes Sociales, se considera fuera del alcance del Sistema de Gestión de Seguridad de la Información de la Entidad y del Plan de Comunicaciones y por lo tanto su Confiabilidad e Integridad, así como los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que la haya generado.
- Todos los medios audiovisuales contenidos en las cuentas de Redes Sociales de la Entidad son tomadas en eventos públicos o con el permiso expreso de las personas que están en estas. Por tal razón, la ADRES se reserva el derecho de eliminar cualquier comentario que contenga: (i) Obscenidades. (ii) Ataques personales de cualquier tipo. (iii) Mensajes no deseados. (iv) Nombres de empleados públicos del Gobierno Nacional. (v) Palabras ofensivas sobre grupos étnicos o raciales específicos. (vi) Amenazas (que remitiremos a las agencias del orden público correspondientes). Así como contenido que: (i) Promueva los productos comerciales. (ii) Esté orientado hacia el éxito o fracaso de un partido político, grupo o candidato partidista. (iii) Incite al odio. (iv) Es objeto de una reclamación por violación, que se considera como una violación de la propiedad intelectual, o que de otro modo es censurable.

7.7 Continuidad del Negocio

- La ADRES, liderado por la Dirección General e incluyendo la participación de todas las direcciones y oficinas, debe definir, probar y actualizar el Plan de Continuidad de Negocio, el cual incluye:
  - Procedimiento Gestión de La Continuidad de Negocio.
  - Árboles de comunicación de crisis.
  - Activos de información críticos.
  - Personal crítico por cargo y funciones dentro de la ADRES.
  - Identificar las amenazas, vulnerabilidades y riesgos asociados que pueden ocasionar interrupciones de los procesos o actividades que afecten los servicios de la Entidad.
  - Pruebas del plan.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones define, articula y mejora con las demás direcciones el Plan de Recuperación de Desastres aplicable a las necesidades de la Entidad.
- Es responsabilidad de los líderes de cada proceso llevar a cabo la identificación de los planes de contingencia por proceso aplicables a las necesidades propias de las actividades definidas a nivel procedimental.
- La ADRES debe evaluar como mínimo una vez al año los requerimientos del negocio para establecer:
  - Cambios sensibles en los procesos
  - Actividades en los procesos críticos que requieren redundancia.
  - Cambios sensibles en cuanto al recurso humano.
  - Procesos manuales y semiautomáticos que pueden ser considerados dentro de la operación en un escenario de contingencia.

7.8 Gestión de Incidentes de Seguridad

- Dentro de la Entidad los Sistemas de Información, los Servidores, Dispositivos de Red y demás servicios tecnológicos están susceptibles a guardar los registros de auditoría y logs en donde las finalidades de estos buscan lo siguiente:
  - Identificación de usuarios.
  - Datos consultados, modificados o eliminados.
  - Intentos fallidos de conexión.
  - Tipos de transacción realizada.
  - Fechas, horas y detalles de los eventos clave, (entrada y salida).
  - Intentos de acceso al sistema exitosos y rechazados.
  - Establecer los cambios a la configuración del sistema
  - Uso de privilegios.
  - Acceso a archivos y tipo de acceso
  - Identificación del dispositivo o ubicación, si es posible, e identificador del sistema.
  - Los registros de auditoría se encuentran protegidos de acceso o modificaciones, con el fin de evitar cualquier tipo de alteración en el nivel de integridad, por tal circunstancia como mecanismo de seguridad todos los registros poseen copias de respaldo.
- Todos los Servidores públicos, contratistas y terceros que por su relación con la Entidad tenga acceso a la información de esta, están en capacidad de identificar y reportar sobre cualquier Incidente de Seguridad y Privacidad de la Información. Por consiguiente, el director o jefe de cada proceso es el primer responsable en verificar que los Incidentes de Seguridad y Privacidad de la Información presentados al interior de su grupo de trabajo sean reportados de manera oportuna por medio de los canales de la mesa de servicios que se ha definido para tal fin.

- Para la exactitud de los registros de auditoría generados dentro de los Sistemas de Información, la Entidad, dispone de un protocolo de tiempo de red NTP, por sus siglas en inglés, que está sincronizado a su vez con la hora legal colombiana.
- El único canal definido para reportar Incidentes de Seguridad y/o Privacidad ante las autoridades y el pronunciamiento oficial ante Entidades externas de la Entidad es el (la) director(a) de la Dirección de Gestión de Tecnologías de Información y Comunicaciones o el servidor público que este delegue. Dicho director (a), de acuerdo con la relevancia del evento o incidente de seguridad generado, debe informar a la Dirección General para que, de acuerdo con los protocolos de comunicación definidos se realice una comunicación formal a las instancias que se definan pertinentes.
- Dentro de los procesos de mejora continua, la implementación de lecciones aprendidas frente a incidentes de seguridad y privacidad debe ser utilizada como herramienta para la toma de decisiones y revisiones tanto de la política general como de las políticas específicas de seguridad y privacidad de la información.
- De acuerdo con el análisis realizado al incidente de seguridad y privacidad de la información, debe ser reportado ante el CSIRT - Gobierno (Computer Security Incident Response) Equipo de respuesta a incidentes del Gobierno de Colombia.

7.9 Gestión de Requisitos Legales

- La ADRES respeta y cumple la normatividad colombiana vigente, en especial la relacionada a temas de Seguridad y Privacidad de la Información. Para lo cual el Equipo de gestión del Sistema de Gestión realiza revisiones sobre los requisitos legales y contractuales que deben ser considerados y evaluados por la Entidad.
- La ADRES implementa y revisa periódicamente toda la legislación vigente frente a la protección de datos personales, buscando:
  - Poder asegurar el cumplimiento de los derechos de los titulares de la información.
  - Contar con las autorizaciones para el tratamiento de datos personales (recolectar, almacenar, usar, trasmitir y eliminar) de los titulares cuando la ADRES actué como responsable de las bases de datos personales.
  - Ser garante del buen manejo de la información personal de sus servidores públicos, contratistas y terceros que en el ejercicio de sus actividades suministren información personal de cualquier tipo. Para ha definido la Política de Tratamiento de Datos Personales, la cual se encuentra dentro de la página Web de la Entidad.
- Se da cumplimiento a la normatividad vigente relativo a los derechos de propiedad intelectual tanto propia como de terceros en donde se incluye: (i) Derechos de autor de software o documentos, licencias, código fuente, entre otros. (ii) Derechos de autor de documentos gráficos, libros u otro material en donde se asocie la propiedad individual o grupal Para esto debe implementar controles que permitan la salvaguarda de estos con el propósito de no permitir copias sin la autorización del propietario.

7.10 Mejoramiento Continuo

- La ADRES en cabeza de la Dirección de Gestión de Tecnologías de Información y Comunicaciones a manera de autoevaluación, realizará por lo menos dos veces al año el ejercicio de Autodiagnóstico conforme al Instrumento de medición vigente que el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC ha definido dentro del marco del Modelo de Seguridad y Privacidad de la Información – MSPI.
- El Líder de Seguridad de la Información de la Entidad una vez implementado el Sistema de Gestión debe definir y realizar periódicamente la evaluación de los controles, la eficiencia de los

Sistemas de Información, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar acciones frente a las deficiencias detectadas.

- La ADRES en cabeza de la Dirección General debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de los lineamientos definidos dentro del Sistema de Administración de Riesgos Integrados de la Entidad que la Oficina Asesora de Planeación y Control de Riesgos lidera.
- Dentro del marco del Plan de Acción de la Entidad, la Dirección de Gestión de Tecnologías de Información y Comunicaciones debe definir el Plan de Seguridad y Privacidad de la información y el Plan de Tratamiento de Riesgos de Seguridad de la Información con una vigencia anual, para lo cual se deben realizar cortes de seguimiento y retroalimentación de las actividades definidas conforme a las directrices definidas por la Oficina Asesora de Planeación y Control de Riesgos.
- La Oficina de Control Interno de la ADRES debe realizar seguimientos a la implementación del Sistema de Gestión de Seguridad de la Información -MSPI que al interior de la Entidad se haya definido. Dicho esto, es responsabilidad de la Dirección de Gestión de Tecnologías de Información y Comunicaciones establecer y ejecutar junto con las demás direcciones los planes de mejoramiento que se generen producto de dichas auditorias.

8. POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1 Gestión de la Tecnología

- El mantenimiento a la infraestructura tecnológica dentro de la Entidad posibilita un nivel adecuado dentro de su disponibilidad e integridad, para lo cual:
  - La Dirección de Gestión de Tecnologías de Información y Comunicaciones dentro de su proceso Gestión de soporte a las tecnologías define para los Mantenimientos preventivos las directrices que se deben llevar a cabo frente a intervalos, equipos y responsables tomando en cuenta las especificaciones dadas por el proveedor.
  - La trazabilidad de mantenimientos preventivos y correctivos se realiza por parte de la Dirección de Gestión de Tecnologías de Información y Comunicaciones dentro de los registros que se definan en los procedimientos de Gestión de Requerimientos y Gestión de Incidentes de seguridad. Para lo cual se debe llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo.
  - Se debe realizar procesos de eliminación de manera segura de la información que se encuentre en cualquier equipo que sea necesario retirar por mantenimiento o cambio. Para esto previamente cuando aplique se deben ejecutar las respectivas copias de respaldo. El responsable funcional del equipo certificará que la copia y restauración de la información sea completa.
  - Establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos;
  - Cuando aplique, cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros;
  - Establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones debe establecer, documentar, ejecutar y actualizar el Procedimiento Gestión de Capacidad, el cual se debe validar por lo menos una vez al año conforme a la situación actual de los Sistemas de Información de la Entidad y la Infraestructura tecnológica que los soporta.

- En el caso de retiro de Activos de información por parte de Servidores Públicos o Contratistas, estos deben tener en cuenta las siguientes directrices frente a la seguridad de los activos:
  - Establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos.
  - Seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes).
  - Aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina) cuando los activos de información se encuentren fuera de la Entidad.
  - Establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones debe establecer parámetros para bloquear automáticamente las sesiones de las estaciones de trabajo una vez estas se encuentren desatendidas por el usuario.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones debe establecer la sincronización de todos los sistemas de información con una única fuente de referencia de tiempo.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones y La Dirección Administrativa y Financiera deben propender para que el cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información de la Entidad se encuentre debidamente protegido contra interceptación, interferencia o daño. Para lo cual:
  - Las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada.
  - Los cables de potencia están separados de los cables de comunicaciones para evitar interferencia.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones cumpliendo con los estándares de privacidad se reserva el derecho de monitorear, desinstalar, e informar a las instancias respectivas el uso de software o utilitarios no autorizados o que no cuenten con el debido licenciamiento.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones debe contar con Sistemas de Información, Servicios o Hardware con el propósito de monitorear cualquier archivo recibido por correo electrónico, por los diferentes servicios de red o por cualquier forma de medio de almacenamiento, con el propósito de detectar el software malicioso, antes de su uso. No obstante, es responsabilidad de todos los Servidores Públicos y Contratistas, sin excepción ejecutar las validaciones de la información que a efecto de sus funciones sea enviada o recibida.
- Dentro de la gestión del catálogo de servicios es responsabilidad de la Dirección de Gestión de Tecnologías de Información y Comunicaciones de la ADRES:
  - Velar por la disponibilidad de los recursos y servicios de red.
  - La instalación, activación, gestión de los puntos de red alámbricos e inalámbricos.
  - Contar con los sistemas de protección entre las redes de la ADRES.
  - Cuando aplique identificar y documentar los servicios, protocolos y puertos autorizados en las redes de datos e inhabilitar o eliminar los servicios, protocolos y puertos no utilizados.
  - Segmentar la red, de modo que permita separar los grupos de servicios de información.
  - Velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con las partes interesadas en función de las necesidades de la Entidad,
  - Realizar evaluaciones de los riesgos asociados a los servicios prestados por la Dirección.
- Las redes inalámbricas deben:

- Estar separadas de las redes LAN, con el fin de garantizar que no se tenga acceso a los recursos o información clasificada y reservada de la Entidad.
- Contar con algún sistema de Control de Acceso a usuarios, así como tener opciones de filtrado de contenidos Web.
- Una vez instalados los dispositivos dentro de la Red de la Entidad, las contraseñas de administración por defecto de estos equipos deben ser cambiadas inmediatamente por el Administrador de la Infraestructura o quien este delegue.
  El sistema de protección de la red que se defina debe ser como mínimo WPA2 o superior a, el cual será definido por el Coordinador de Soporte de Tecnologías de Información.

8.2 Uso de los Servicios de Red e Internet

- La infraestructura de Red e Internet de la ADRES debe contar con controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, así como para proteger los Sistemas de Información y Servicios que se encuentren conectados. Adicionalmente, dentro de la infraestructura de red de la Entidad, se debe:
  - Aplicar logging y seguimientos adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información;
  - Tener la posibilidad si así se requiere de restringir la conexión de los sistemas a la red.
  - Establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red.
  - Definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red;
  - Establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.
  - Proteger la integridad de las diferentes redes incorporando segregación en estas cuando se requiera.
- La infraestructura, servicios y tecnologías usados para acceder a Internet son propiedad de la ADRES, por lo tanto, cumpliendo con los estándares de privacidad se reserva el derecho de monitorear el uso de Internet por parte de la Dirección de Gestión de Tecnologías de Información y Comunicaciones.
- El uso de las redes inalámbricas está permitido dentro de la entidad conforme a las necesidades del servicio y las directrices dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- El uso de Internet incluida la descarga de archivos por parte de los Servidores Públicos, Contratistas y Terceros debe realizarse con propósitos laborales. Por tal razón, la navegación a sitios con contenidos como: (i) Pornografía, (ii) Drogas, (iii) Alcohol, (iv) Terrorismo, (v) Hacktivismo, (vi) Segregación racial, (vii) Código malicioso (Malware) o (viii) Cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este manual de políticas y por la ADRES contrarios a la ley o a las políticas de la Entidad o que representen peligro está restringida.
- El uso de Internet incluida la descarga de archivos por parte de los Servidores Públicos, Contratistas y Terceros debe realizarse con propósitos laborales. Por tal razón, la navegación a sitios con contenidos como: (i) Redes sociales. (ii) Comercio electrónico. (iii) Portales de Ocio entre otros; podrán ser bloqueados por parte de la Dirección de Gestión de Tecnologías de Información y Comunicaciones y solo se habilitarán con previa solicitud de los líderes de los procesos en donde se exprese la necesidad de uso de un portal específico, esto conforme con lo definido dentro del procedimiento de Gestión de Requerimientos que se tenga definido al interior de la Entidad.

8.3 Respaldo y Restauración de la Información

- La información por respaldar por parte de la Dirección de Gestión de Tecnologías de Información y Comunicaciones será la que se encuentre dentro de las unidades de almacenamiento colaborativo o histórico, así como la de los buzones de correo electrónico de los Servidores Públicos y Contratistas.
- Es responsabilidad del líder de cada proceso o quien este delegue de realizar la solicitud de servicios respaldo de Información conforme con lo definido dentro del Catálogo de Servicios que la Dirección de Gestión de Tecnologías de Información y Comunicaciones ha definido para tal fin. Dichas copias de respaldo tendrán un periodo de retención de un año, salvo las excepciones que explícitamente el solicitante defina dentro de su requerimiento.
- De acuerdo con lo definido por parte de la Dirección de Gestión de Tecnologías de Información y Comunicaciones dentro del Catálogo de servicios de esta, se ha determinado que el respaldo de información se puede realizar mediante el uso de: (i) Cintas, (ii) CD, (iii) DVD, (iv) Discos Duros externos o (v) Espacios de almacenamiento para información histórica. Esto teniendo en cuenta el tipo, tamaño y frecuencia de respaldo de la información.
- Las oficinas y direcciones que se les sea asignados Espacios de almacenamiento para información histórica tienen la responsabilidad, conforme a sus necesidades, de copiar, organizar y depurar la información que sea sujeto de dicho respaldo. Adicionalmente, deben definir la frecuencia con la cual se realizará el respaldo.
- El custodio de las copias de respaldo será la Dirección de Gestión de Tecnologías de Información y Comunicaciones; en caso de requerir alguna restauración el líder de cada proceso o quien este delegue deberá realizar la solicitud conforme en lo definido en el procedimiento de Gestión de Requerimientos de esta Dirección.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones debe realizar pruebas periódicas de restauración en ambientes de prueba de la información en la cual está sea custodia y que se considere más sensible para la operación de la Entidad, esto con el propósito de evaluar la correcta generación de las copias de seguridad.
- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información, para lo cual debe realizar la respectiva solicitud conforme a lo definido dentro del procedimiento de gestión de requerimientos de la Dirección de Gestión de Tecnologías de Información y Comunicaciones.
- La información carente de valor para la Entidad, conforme al registro de activos de información, índice de información clasificada o tablas de retención documental se eliminará una vez que se haya utilizado, esto con el propósito de evitar que la capacidad de almacenamiento se vea desbordada innecesariamente.

8.4 Acceso remoto

- Está prohibido realizar alguna actividad de tipo remoto sin la debida solicitud por parte del director, jefe de la dependencia o del coordinador del grupo interno en donde se presenta la necesidad y posterior aprobación de la Dirección de Gestión de Tecnologías de Información y Comunicaciones de la ADRES. En caso de requerirse la conexión remota está debe ser hecha a través de una conexión temporal segura VPN, la cual es aprobada, entregada y auditada por la Dirección de Gestión de Tecnologías de Información y Comunicaciones. Por tal razón, el uso de sistemas de información que presenten el servicio de conexión remota que no se encuentren avalados por dicha Dirección, se encuentra restringido.
- Las partes interesadas que requieran conexión con la infraestructura de ADRES para restar el servicio deben hacerlo mediante un canal de comunicación seguro conforme a las guías de

interoperabilidad que la Dirección de Gestión de Tecnologías de Información y Comunicaciones adopte.

- Sin excepción toda conexión a VPN que se autorice por parte de la Dirección de Gestión de Tecnologías de Información y Comunicaciones de la ADRES tendrá un tiempo de vigencia conforme con lo definido dentro del Catálogo de servicios de dicha Dirección.
- Las estaciones de trabajo remotas que se conecten vía VPN a los servicios, sistemas de información e infraestructura de la ADRES deben contar con sistema operativo, sistemas utilitarios y sistema de protección antimalware actualizados y debidamente licenciados.
- la Dirección de Gestión de Tecnologías de Información y Comunicaciones cumpliendo con los estándares de seguridad deberá establecer los controles para restringir el acceso a los servicios de la Entidad y deshabilitar la salida a internet desde la estación de trabajo remota, cuando se use conexiones VPN.
- la Dirección de Gestión de Tecnologías de Información y Comunicaciones cumpliendo con los estándares de privacidad se reserva el derecho de monitorear las conexiones VPN asignadas a las diferentes partes interesadas.

8.5 Dispositivos Móviles

- Teniendo en cuenta que el uso de Dispositivos Móviles personales es frecuente dentro del ámbito laboral y por tal razón, se puede llegar a tener en ellos información relacionada a las funciones relativas al cargo. El Servidor Público o Contratista que decida por nombre propio usar dichos dispositivos con estas finalidades debe:
  - Configurar algún método de bloqueo de pantalla tal como (i) contraseñas, (ii) biométricos, (iii) patrones o (iv) reconocimiento de voz. De igual manera es responsable del uso de este en lugares con algún riesgo de seguridad y debe prevenir el extravío, robo o hurto de este. De igual manera.
  - Mantener actualizados, los Sistemas Operativos y Aplicativos dentro de los dispositivos móviles, en donde adicionalmente estos se deben encontrar debidamente licenciados por los proveedores de servicios.
  - Implementar alguna técnica de cifrado de las unidades de almacenamiento del dispositivo.
  - Controlar y restringir el acceso físico por parte de otras personas diferentes al Servidor Público o Contratista.
- Ante la ocurrencia de un evento de pérdida de un dispositivo móvil de un Servidor Público o Contratista y si en él se encontraba información de la Entidad, el Funcionario Público debe informar oportunamente a su jefe inmediato quien validará la pertinencia de informar a la Dirección de Gestión de Tecnologías de Información y Comunicaciones de acuerdo con lo establecido dentro del procedimiento de gestión de Incidentes de Seguridad.
- El uso de herramientas de mensajería instantánea dentro de dispositivos móviles personales con propósitos laborales, no se encuentra restringido. Sin embargo, no se permite por estas aplicaciones, el envío de fotografías, audios, videos o cualquier otro tipo de archivo clasificados como información Pública Reservada o Información Pública Clasificada conforme con lo definido dentro del Índice de Información Clasificada y Reservada adoptado en la Entidad.
- Es responsabilidad del Servidor Público o Contratista que decida por nombre propio usar dichos dispositivos realizar copias de respaldo periódicas teniendo en cuenta las características del dispositivo y cantidad de información almacenada.

8.6 Cifrado de información y uso de llaves de seguridad (tokens)

- La Dirección de Gestión de Tecnologías de Información y Comunicaciones, es la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de

la ADRES, considerando los criterios de Confidencialidad, Integridad, Autenticidad y no repudio en las comunicaciones o en el tratamiento de la información para los Sistemas o Servicios Propios. En el caso de contar con mecanismos de cifrado de información externos tales como llaves de seguridad suministradas por Bancos, Entes certificadores y demás, la Entidad adoptará los mecanismos de cifrados definidos por estos terceros.

- La Dirección de Gestión de Tecnologías de Información y Comunicaciones definirá dentro de sus guías como se debe hacer la correcta gestión de llaves de cifrado en donde entre otras cosas, se deben definir consideraciones frente a:
  - Generación de llaves para los diferentes sistemas de cifrado y diferentes sistemas de información.
  - Gestión, almacenamiento, custodia, uso, respaldo, revocación o eliminación de llaves públicas y privadas.
  - Registrar y auditar las actividades relacionadas con gestión de llaves.
  - El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los Servidores Públicos y Contratistas de la Entidad.
  - Los Servidores Públicos, contratistas que les sean asignadas llaves de seguridad deben dar avisos a las entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de estos.

8.7 Relaciones con Terceros (Proveedores)

- La Entidad establece los mecanismos de control en sus relaciones con terceros a los que provea o que provean bienes o servicios. Por tal razón, los servidores públicos responsables de la realización y/o firma de contratos, acuerdos o convenios con terceros deben garantizar el cumplimiento del presente manual. En especial para las siguientes directrices:
  - Se debe validar la inclusión de Acuerdos de Niveles de Servicios en los contratos suscritos con terceros, en especial los celebrados con persona jurídica.
  - Es responsabilidad del propietario del activo de información del cual se va a compartir información evaluar los riesgos que se puedan presentar en el momento de entrega de información al tercero.
- Los proveedores, contratistas y demás personal externo de la ADRES garantizan la confidencialidad e integridad de la información a la cual tengan acceso durante la permanencia en las instalaciones de la entidad para tal fin:
  - Los proveedores o contratistas que tengan relaciones contractuales con la Entidad, se les incluirá dentro de su contrato una cláusula de confidencialidad de información. Conforme a las definiciones dadas por el Grupo Interno de Gestión de la Contratación de la Dirección Administrativa y Financiera.
  - Los proveedores deben tener acceso limitado a información sensible de la entidad. Si para fines de su labor fuera necesario tener acceso a dicha información, el responsable de la esta debe proporcionarla con las medidas de seguridad acordes, con el fin de que no pueda ser modificada o alterada por el proveedor.
  - Los proveedores y contratistas no podrán tener acceso a áreas o zonas seguras de la ADRES. Sí fuera necesario su ingreso a determinadas áreas será necesario la autorización de un funcionario de la entidad el cual deberá acompañar al contratista durante el tiempo que este permanezca en dicha área.
  - Es deber de los proveedores anunciarse en la recepción de la ADRES a su ingreso y salida, así como registrar sin falta los equipos necesarios para la realización de su labor en la entidad. Para lo cual, la empresa de Servicios de Seguridad Física que este contratada debe hacer efectivo control de acuerdo con los lineamientos definidos.

8.8 Privacidad y Confidencialidad de la Información

- La Política Protección de Datos Personales se encuentra definida conforme a lo establecido en la normatividad vigente. Adicionalmente, se encuentra aprobada por la Dirección General y está disponible en el portal web institucional (www.adres.gov.co) En el enlace de Transparencia.

9. REVISIÓN

Las políticas de seguridad de la información descritas en el presente documento se deben revisar por lo menos una vez al año o cuando ocurran cambios significativos en la Entidad o en el entorno legal de la misma. Dicha revisión estará a cargo del Comité Institucional de Gestión de Desempeño.

10.CUMPLIMIENTO

El incumplimiento a la presente Política de Seguridad y Privacidad de la Información trae consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional en cuanto a la Seguridad y Privacidad de la Información. En especial a las medidas administrativas, disciplinarias o legales a que haya lugar.

11.VIGENCIA

La presente política entra en vigor el día 18 de mayo de 2020.

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Descripción del cambio**	**Asesor del proceso**
01	*28 de marzo de 2019*	Emisión y Publicación inicial	Marian Helen Batista Pérez Gestor de Operaciones OAPCR
02	*18 de mayo de 2020*	Actualización de responsabilidades de la ADRES frente a la política de Seguridad y Privacidad de la información, las cuales se encuentran detalladas dentro del manual de Políticas de Seguridad de la Información. Cambio de codificación de la política conforme al mapa de procesos actual de la Entidad.	Olga Marcela Vargas Valenzuela Asesora OAPCR

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Juan Carlos Escobar Baquero Gestor de Operaciones - Dirección de Gestión de Tecnologías de la Información y las Comunicaciones **Fecha:** *13 de mayo de 2020*	**Sergio Andrés Soler Rosas** Director de Gestión de Tecnologías de la Información y las Comunicaciones **Fecha:** *15 de mayo de 2020*	**Diana Cárdenas Gamboa.** Directora General de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud- ADRES **Comité Institucional de Gestión y Desempeño** **Fecha:** *18 de mayo de 2020*

ANEXO 1. Análisis de las Partes interesadas

La Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES, identifica las partes interesadas que son pertinentes al Sistema de Gestión de Seguridad de la Información, sus necesidades y expectativas, con el objetivo de comprenderlas, aceptarlas e incluirlas en el alcance, cumpliendo, de esta manera, con lo establecido en el numeral 4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas, de la norma NTC-ISO-IEC 27001:2013.

PARTE INTERESADA	NECESIDADES	EXPECTATIVAS
Servidores públicos y Contratistas	Contar con los sistemas de información y servicios tecnológicos que les permita agilizar su trabajo y que la información registrada a través de estos sea resguardada bajo los criterios de confidencialidad, integridad y disponibilidad. Fortalecer el grado de uso y apropiación efectivo en temas tecnologías de la Información, Cultura en seguridad de la información. Prevenir fuga o perdida de información. Lograr la apropiación de las Políticas en Seguridad y Privacidad de la información.	Comunicación efectiva y asertiva en el marco del desarrollo de las funciones. Fortalecimiento permanentemente frente al Sistema de Seguridad de la Información y las buenas prácticas en el uso de las tecnologías de información. Lograr la adopción de buenas prácticas que permitan garantizar la confidencialidad, disponibilidad e integridad de la información. Mitigar los riesgos por perdida, o uso indebido de la información cumpliendo con la normatividad vigente.
Entidades y Empresas	Implementar Sistemas de Información, herramientas o servicios para el intercambio de información. Articulación interinstitucional mediante el establecimiento de acuerdos de cooperación.	Fomentar alianzas con Entidades y Empresas privadas comprometidas con la misionalidad de la entidad. Lograr la adopción de buenas prácticas que permitan garantizar la confidencialidad, disponibilidad e integridad de la información. Mitigar los riesgos por perdida, o uso indebido de la información cumpliendo con la normatividad vigente.
Ciudadanía, comunidad en general	Fortalecer la seguridad en la información suministrada a la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES Garantizar la protección de los datos personales de la comunidad en general conforme al procesamiento de información dentro de las diferentes líneas misionales.	Cumplir tanto la Política General como Políticas Específicas de Seguridad de la Información reduciendo las probabilidades de afectación a la información.
Gobierno	Generar informes de los incidentes de seguridad presentados al Interior de la Entidad o externos que afecten la operación de esta. Brindar información acerca de la ejecución de la Política de Gobierno Digital. Compartir los Incidentes de Seguridad de la Información detectado por los	Acompañamiento en el análisis de la infraestructura con el fin de identificar vulnerabilidades en la implementación del Sistema de Gestión de Seguridad de la Información. Fortalecer los canales de comunicación con las diferentes Entidades competentes, para el oportuno reporte de ataques cibernéticos y así poder actuar a tiempo para su mitigación.

PARTE INTERESADA	NECESIDADES	EXPECTATIVAS
	diferentes grupos de respuesta a incidentes tanto a nivel Público como privado a los cuales la Entidad tenga acceso. Dar cumplimiento a los lineamientos, directrices que han sido establecidos para la implementación del Sistema de Gestión de Seguridad de la Información.	Robustecer la comunicación entre La Fiscalía General de la Nación y la ADRES para proceder de manera oportuna frente a posibles delitos que atente con la Seguridad de la Información de la Entidad.
Proveedores	Realizar acompañamiento frente al cumplimiento de las cláusulas establecidas en los contratos frente a la administración de información que conforme a su objeto contractual eventualmente lleguen a manejar.	Conocer tanto la Política General como Políticas Específicas de Seguridad y Privacidad de la información de la Entidad.