



**MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD
Y PRIVACIDAD DE LA INFORMACIÓN**

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

BOGOTÁ, DICIEMBRE DE 2022


	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

TABLA DE CONTENIDO

1. INTRODUCCIÓN	4
2. OBJETIVO	5
3. ALCANCE	5
4. TERMINOS Y DEFINICIONES	5
5. MARCO NORMATIVO	10
6. PRINCIPIOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	12
7. MODELO DE GOBIERNO DE LA SEGURIDAD DIGITAL	13
7.1 RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN.....	13
7.2 MODELO DE TRES LÍNEAS DE DEFENSA EN SEGURIDAD DE LA INFORMACIÓN	15
7.2.1 <i>Funcionamiento del Modelo</i>	15
7.2.2 <i>Roles clave del modelo</i>	16
7.2.3 <i>Perspectiva estratégica del modelo de gobierno</i>	17
7.2.3.1 <i>Órgano de Gobierno</i>	17
7.2.4 <i>Perspectiva Táctica del Modelo de Gobierno</i>	18
7.2.4.1 <i>Segunda línea de defensa</i>	18
7.2.4.2 <i>Tercera línea de defensa</i>	18
7.2.5 <i>Perspectiva operacional</i>	18
7.2.5.1 <i>Primera línea de defensa</i>	18
7.2.5.2 <i>Segunda línea de defensa</i>	19
7.3 EQUIPOS DE RESPUESTA A INCIDENTES DE SEGURIDAD DIGITAL.....	20
8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	20
POLÍTICA GENERAL.....	20
8.1 CRITERIOS DE LA SEGURIDAD DE LA INFORMACIÓN	20
8.2 CRITERIOS DE CALIDAD DE LA INFORMACIÓN.....	20
8.3 SANCIONES PREVISTAS POR INCUMPLIMIENTO	21
8.4 UNIDAD DE SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD	21
8.5 OBLIGACIONES Y DEBERES DEL RECURSO HUMANO.....	22
8.6 POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN.	23
8.6.1 IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	24
8.6.2 DISPOSICIÓN DE ACTIVOS DE INFORMACIÓN	24
8.6.3 USO ADECUADO DE ACTIVOS DE INFORMACIÓN	26
8.6.4 ETIQUETADO DE INFORMACIÓN	27
8.6.5 GESTIÓN DE MEDIOS REMOVIBLES.....	27
8.6.6 DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN.....	27
8.7 CONTROL DE ACCESO	28
8.8 ADQUISICIÓN O DESARROLLO DE SISTEMAS DE INFORMACIÓN	30
8.9 GESTIÓN DE INTERCAMBIO DE INFORMACIÓN	31
8.10 CONTINUIDAD DEL NEGOCIO.....	33
8.11 POLÍTICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD	33
8.12 GESTIÓN DE REQUISITOS LEGALES	35
8.13 MEJORAMIENTO CONTINUO	36

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

9. POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	36
9.1 GESTIÓN DE LA TECNOLOGÍA	36
9.2 POLÍTICA DE SEGURIDAD DE CORREO ELECTRÓNICO INSTITUCIONAL.....	38
9.3 USO DE LOS SERVICIOS DE RED E INTERNET.....	39
9.4 POLÍTICA DE ESCRITORIOS Y PANTALLA LIMPIOS.....	40
9.5 RESPALDO Y RESTAURACIÓN DE LA INFORMACIÓN	40
9.5.1 PLAN DE COPIAS Y MÉTODOS APLICABLES	41
9.5.2 CICLOS DE BACK UP.....	41
9.6 ACCESO REMOTO	42
9.7 POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO.....	43
9.7.1 RESPONSABILIDADES DE LOS USUARIOS.....	43
9.7.2 POR PARTE DE LOS USUARIOS:	43
9.7.3 MONITOREO Y CAPACITACIÓN	43
9.8 DISPOSITIVOS MÓVILES.....	44
9.9 CIFRADO DE INFORMACIÓN Y USO DE LLAVES DE SEGURIDAD (TOKENS)	44
9.10 RELACIONES CON TERCEROS (PROVEEDORES)	45
9.11 PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.....	46
10. RIESGOS	46
11. CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN	46
11.1 ENFOQUE PREVENTIVO	46
11.2 ENFOQUE REACTIVO	47
11.3 RESPUESTA Y COMUNICACIÓN	48
11.4 RECUPERACIÓN Y APRENDIZAJE.....	48
12. REVISIÓN.....	48
13. CUMPLIMIENTO.....	48
14. VIGENCIA.....	48
ANEXO 1. ANÁLISIS DE LAS PARTES INTERESADAS.....	50

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

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, la administración de riesgos y la 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 Sistema Integrado de Gestión Institucional, 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 propuesto¹.



Esto permite (i) Identificar y minimizar los riesgos a los cuales se expone la información entendiendo el entorno y el contexto interno, conforme con el manual de administración de riesgos de la Entidad.

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].

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

(ii) Ayudar a la reducción de costos operativos y financieros, (iii) Establecer una cultura de seguridad y (iv) Promover el cumplimiento de los requerimientos vigentes a nivel legal, contractual y de 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; las 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 permea 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 interesadas² 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

Para el entendimiento del presente manual se define un lenguaje común en donde se establecen los principales conceptos y el marco teórico en el que se fundamenta la Seguridad de la Información (SI) y Ciberseguridad de la ADRES.

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, transmisión 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 explícita 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.

² Ver Anexo 1. Análisis de las Partes Interesadas

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

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.

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.

CERT: (Computer Emergency Reponse Team) Equipo de respuesta a emergencias cibernéticas como sus siglas en ingles. Es el equipo que dispone de capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.

Ciberespacio: Red interdependiente de infraestructuras de tecnologías de información que incluye internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias.

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.

CSIRT: (Comuter security Incident & Response Team) Equipo de respuesta a incidentes de seguridad cibernética, por sus siglas en Ingles. Es el equipo que provee las capacidades de gestión de incidentes a una organización o sector en especial.


CSIRT Sectorial: Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de tecnologías de la información y las telecomunicaciones.

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.

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

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.

Firma Digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación (Ley 527 de 1999).

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.


Gobernanza de Seguridad Digital para Colombia: Corresponde al conjunto de interacciones y enfoques entra las múltiples partes interesadas para identificar, enmarcar, proponer y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad y disponibilidad de la información, servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes a información que en conjunto constituyen el entrono digital.

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.

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

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.


Modelo de gobierno de Seguridad digital: Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad y disponibilidad de los servicios tecnológicos, servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes a información que en conjunto constituyen el entrono digital sistemas de información,

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.

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

Privacidad³: 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. Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo. (Ley 1221 de 2008)

Trabajo en Casa: Se entiende como trabajo en casa la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones. Este no se limita al trabajo que puede ser realizado mediante tecnologías de la información y las comunicaciones, medios informáticos o análogos, sino que se extiende a cualquier tipo de trabajo o labor que no requiera la presencia física del trabajador o funcionario en las instalaciones de la empresa o entidad. (Ley 2088 de 2021)

Trabajo remoto: Es una forma de ejecución del contrato de trabajo en la cual toda la relación laboral, desde su inicio hasta su terminación, se debe realizar de manera remota mediante la utilización de tecnologías de la información y las telecomunicaciones u otro medio o mecanismo, donde el empleador y trabajador, no interactúan físicamente a lo largo de la vinculación contractual. En todo caso, esta forma de ejecución no comparte los elementos constitutivos y regulados para el teletrabajo y/o trabajo en casa y las normas que lo modifiquen. (Ley 2121 de 2021)

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/gestioniti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf [Accedido el 26 dic. 2018].

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

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.
- 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".
- Directiva presidencial 02 de 2022 "Reiteración de la política pública en materia de seguridad digital"
- Decreto 338 de 2022 "Por el cual se adiciona el Título 21 a la parte 2 del libro del Decreto único 1078 de 2015, con el fin de establecer lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza en Seguridad Digital y se dictan otras disposiciones"

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

6. PRINCIPIOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta las definiciones del Decreto 338 de 2022, se definen los siguientes principios que rigen este manual:

- **Confianza:** La seguridad digital debe fortalecer la confianza mediante la comunicación, el intercambio de información y la concreción de acuerdos claros sobre la división de tareas y acciones a realizar.
- **Coordinación:** Las actuaciones que se realicen en materia de seguridad digital deberán integrar de manera coordinada las múltiples partes interesadas, para garantizar la armonía en el ejercicio de sus funciones y el logro de este objeto.
- **Colaboración entre las múltiples partes interesadas:** En la aplicación e interpretación de estos lineamientos se deben involucrar activamente las múltiples partes interesadas, y permitir establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital y aumentar la capacidad de resiliencia frente a eventos no deseados en al entorno digital.
- **Cooperación:** Aunar esfuerzos para para el logro de los objetivos institucionales o comunes.
- **Enfoque basado en la gestión de riesgos:** Gestionar el riesgo de forma que el uso de tecnologías de la información y las comunicaciones fomenten la confianza en el entorno digital.
- **Gradualidad:** Desarrollar herramientas operativas y estratégicas, de alcance definido en tiempo, espacio y recursos, que permitan la implementación gradual y sostenida, de estrategias, programas, planes y proyectos que se requieran para garantizar la seguridad y protección del ciberespacio.
- **Inclusión:** La seguridad digital debe incluir a todas las partes interesadas, fomentar su participación y establecer condiciones necesarias para el desarrollo eficiente de alianzas.
- **Proporcionalidad:** Las acciones y operaciones en el ciberespacio serán proporcionales con la gestión dinámica de los riesgos derivados de los avances y usos de la ciencia y la tecnología, ponderando circunstancias de necesidad, oportunidades, capacidades, amenazas y riesgos.
- **Salvaguarda de los derechos humanos y los valores fundamentales de los ciudadanos:** En la aplicación e interpretación de los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la gestión de los riesgos de seguridad digital, la identificación de infraestructuras cibernéticas y servicios esenciales y la respuesta a incidentes de seguridad digital.
- **Uso eficiente de la infraestructura y de los recursos para protección de infraestructura críticas cibernéticas y servicios esenciales:** Velar por la infraestructuras y los recursos tendentes a la protección de las infraestructuras y servicios digitales.

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

7. MODELO DE GOBIERNO DE LA SEGURIDAD DIGITAL

El modelo de gobierno y/o dirección se basa en tres funciones básicas:

- **Dirigir:** asignando responsabilidades y dirigiendo la preparación e implementación de estrategias y políticas, para garantizar el aseguramiento de los activos de información;
- **Evaluar:** examinando y emitiendo juicio sobre la gestión actual y futura de la seguridad de la información en la entidad, incluyendo planes y propuestas de control; y
- **Monitorear:** verificando el desempeño del sistema de gestión de la seguridad de la información en la ADRES.

Estas tareas se enfocan en el desarrollo de las siguientes funciones y responsabilidades

7.1 Responsabilidades en seguridad de la información

Los modelos de Gobierno y/o dirección se basan en tres funciones básicas sobre diferentes dominios definidos para el alcance de la seguridad de la información; los cuales serán descritos a continuación:

- **EVALUAR**

Los órganos rectores deben evaluar las opciones para asignar responsabilidades con respecto al uso actual y futuro de la Seguridad de la Información (SI) y la Ciberseguridad (CBS) en la organización. Al evaluar las opciones, los órganos rectores deben tratar de garantizar el uso eficaz, eficiente y aceptable de los Activos de Información en apoyo de los objetivos de la Entidad.

Los órganos rectores deben evaluar la competencia de quienes tienen la responsabilidad de tomar decisiones con respecto a SI y CBS. En general, estas personas deben ser gerentes que también son responsables de los objetivos y el desempeño del negocio de la organización, con la asistencia de especialistas de SI y CBS que entiendan los valores y procesos de la Entidad.

- **DIRIGIR**

Los órganos rectores deben ordenar que se sigan las estrategias de acuerdo con las responsabilidades de SI asignadas.

Los órganos rectores deben ordenar que reciban la información que necesitan para cumplir con sus responsabilidades.

- **MONITOREAR/ SUPERVISAR**

Los órganos rectores deben supervisar que se establezcan los mecanismos apropiados para la gobernanza de SI.

Los órganos rectores deben vigilar que las personas a las que se les ha dado la responsabilidad reconozcan y entiendan sus responsabilidades.

Los órganos rectores deben supervisar el desempeño de las personas a las que se les da la responsabilidad en el gobierno de SI (por ejemplo, aquellas personas que sirven en comités directivos o presentan propuestas a los órganos rectores).

A continuación, se definen las responsabilidades en Seguridad de la Información (SI) y Ciberseguridad (CBS) que deben adoptar los órganos de gobierno o rectores en relación con los diferentes dominios del Sistema de Gestión de Seguridad de la Información (SGSI).

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:
		Fecha:	12/12/2022

DOMINIO	EVALUAR	DIRIGIR	MONITOREAR/SUPERVISAR
ESTRATEGIA	Al considerar los planes y políticas, el órgano rector debe evaluar el uso de los <i>Activos de Información</i> y el aseguramiento de estos para garantizar que se alinean con los objetivos de la organización y satisfacen los requisitos clave de las partes interesadas. El órgano rector también debería tener en cuenta las buenas prácticas.	Dirigir la preparación y el uso de estrategias y políticas que garanticen que la organización se beneficie de los desarrollos en IS y CBS. Alentar la presentación de propuestas para el aseguramiento de los Activos de Información y los usos de TI que estén relacionados con la Ciberseguridad y permitan a la organización responder a nuevas oportunidades o desafíos, emprender nuevos servicios o mejorar procesos	Supervisar el progreso de las propuestas de SI y CBS aprobadas para garantizar que están logrando los objetivos en los plazos requeridos utilizando los recursos asignados. Supervisar el uso adecuado de los Activos de Información y la infraestructura de TI para garantizar que está logrando los beneficios previstos.
ADQUISICIÓN	Los órganos rectores deben evaluar las opciones para proporcionar IS y CBS la realización de las propuestas aprobadas, equilibrar los riesgos y la relación calidad-precio de las inversiones propuestas.	Ordenar que las soluciones asociadas a SI y CBS (servicios, sistemas e infraestructura) se adquieran de manera adecuada, incluida la preparación de la documentación, y al tiempo que se garantiza que se proporcionan las capacidades requeridas. Ordenar que los acuerdos de suministro (internos y externos) apoyen las necesidades de SI y CBS de la organización. Indicar que su organización y proveedores desarrollen una comprensión compartida de la intención de la organización al realizar cualquier acción encaminada a la SI y CBS	Los órganos de gobierno deben supervisar las inversiones en SI y CBS para garantizar que proporcionan las capacidades requeridas. Controlar hasta qué punto su organización y proveedores mantiene la comprensión compartida de la intención de la organización al realizar cualquier acción relacionada con SI y CBS.
DESEMPEÑO	Evaluar los planes propuestos por los líderes de procesos dueños de los activos de información. Estas propuestas deben abordar el funcionamiento normal continuo de la organización y el tratamiento del riesgo asociado con el uso de TI. Evaluar los riesgos para la operación continua del negocio que surgen de las actividades de SI y CBS. Evaluar los riesgos para la integridad de la información y la protección de los activos de TI, incluida la propiedad intelectual asociada y la memoria de la organización. Evaluar las opciones para garantizar decisiones efectivas y oportunas sobre el uso de los Activos de Información y Activos de TI relacionados con SI y CBS, en apoyo de los objetivos comerciales. Evaluar periódicamente la efectividad y el rendimiento del SGSI.	Garantizar la asignación de recursos suficientes para que el SGSI satisfaga las necesidades de la organización, de acuerdo con las prioridades acordadas y las limitaciones presupuestarias. Dirigir a los responsables de los Activos de Información, para garantizar que la SI y CBS respalde a la organización, cuando sea necesario por razones de cumplimiento, con datos correctos y actualizados que estén protegidos contra pérdidas o mal uso.	Los órganos de gobierno deben supervisar en qué medida el SGSI apoya el negocio. Los órganos rectores deberían controlar en qué medida los recursos y presupuestos asignados a SI y CBS se priorizan de acuerdo con los objetivos de la Entidad. Los órganos rectores deben supervisar en qué medida las políticas de SI y CBS, como la protección de los datos personales son seguidas adecuadamente.
CONFORMIDAD	Los organismos rectores deben evaluar periódicamente en qué medida la el SGSI cumple con las obligaciones (normativas, legislativas, contractuales), políticas	Los órganos rectores directos deben indicar a los responsables que establezcan mecanismos regulares y rutinarios para garantizar el buen uso de los Activos de Información y activos relacionados en	Supervisar el cumplimiento y la conformidad del SGSI a través de prácticas apropiadas de informes y auditoría, asegurando que las revisiones sean oportunas, integrales

	internas, normas, lineamientos y directrices legales. Los órganos rectores deben evaluar periódicamente la conformidad interna de la organización con su marco para el gobierno de IS y CBS	cumplimiento de las obligaciones, políticas internas, normas y directrices pertinentes. Ordenar que las políticas se establezcan y apliquen para permitir que la organización cumpla con sus obligaciones internas en el uso adecuado de los Activos de Información. Indicar que los funcionarios y contratistas de la Entidad sigan las pautas relevantes para el comportamiento y el desarrollo profesional respecto de la SI y CBS. Ordenar que todas las acciones relacionadas con la SI y CBS sean éticas	y adecuadas para la evaluación del grado de satisfacción de la organización. Supervisar las actividades de relacionadas con la SI y CBS, incluida la eliminación de activos y datos, para garantizar que se cumplan; las políticas y lineamientos de SI y CBS, obligaciones medioambientales, de privacidad, de gestión estratégica del conocimiento, de preservación de la memoria de la organización y otras obligaciones relevantes.
COMPORTAMIENTO HUMANO	Los órganos rectores deben evaluar las actividades de IS y CBS, para garantizar que los comportamientos humanos se identifiquen y se consideren adecuadamente.	Indicar que las actividades de SI y CBS son consistentes con el comportamiento humano identificado. Indicar que cualquier persona puede identificar e informar oportunamente los eventos de seguridad de la información, los riesgos, las oportunidades, los problemas y las preocupaciones en cualquier momento. Estos riesgos e incidentes deben gestionarse de acuerdo con las políticas y procedimientos publicados y escalarse a los tomadores de decisiones relevantes	Los órganos de gobierno deben supervisar las actividades de TI para garantizar que los comportamientos humanos identificados sigan siendo relevantes y que se les preste la atención adecuada. Los órganos rectores deberían supervisar las prácticas laborales para garantizar que sean coherentes con uso apropiado de los activos de información y TI

7.2 Modelo de Tres Líneas de Defensa en Seguridad de la Información

Ante los riesgos y amenazas de SI y CBS que acechan continuamente a la ADRES, se propone la adopción del concepto de "líneas de defensa" que ya está implementado para temas administrativos y de gestión de procesos, que permitan identificar estos riesgos, valorarlos, medirlos, priorizarlos y gestionar las respuestas ante su posible materialización; y realizar un seguimiento periódico.

En este modelo la **Primera línea** se definen aquellas funciones de la organización encargadas de la operación en el día a día respecto del aseguramiento, protección y gestión de los activos de información, la responsabilidad de evaluar, controlar y mitigar los riesgos, así como de diseñar e implantar los controles efectivos.

La **Segunda línea** serían todas aquellas funciones asociadas al control sobre los activos de información y activos relacionados, a la gestión efectiva de los riesgos de seguridad de la información y al cumplimiento y supervisión en la implementación de prácticas efectivas de mitigación y la prevención.

Finalmente, una **Tercera línea** que sería auditoría interna, que ofrece un aseguramiento independiente sobre la efectividad, control interno y verificación de la gestión de riesgos, incluida la operación de la primera y segunda línea de defensa.

7.2.1 Funcionamiento del Modelo

El modelo de líneas de defensa está basado en los siguientes principios:

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

1. Estructurar el **gobierno de la organización** para rendir cuentas, definir acciones, asegurar y asesorar.
2. Establecer los **roles dentro del órgano de gobierno** para que funcione de forma eficaz; alineando los objetivos y actividades a los intereses de cada parte.
3. Definir **responsabilidades para alcanzar objetivos** tanto en primera como segunda línea.
4. Establecer los roles de tercera línea como la auditoría interna. Este principio también sirve para asesorar a los demás órganos para asegurarse del cumplimiento de los objetivos.
5. La auditoría interna es independiente de las responsabilidades de la dirección para ser totalmente objetiva y creíble.
6. Creación y protección del valor. Todas las funciones trabajan colectivamente con el objetivo de alinearse y lograr los intereses de todas las partes involucradas.

7.2.2 Roles clave del modelo

Este nuevo enfoque está pensado para que la gestión de riesgos sea más flexible y efectiva. Para lograrlo se han definido los diferentes roles que participan activamente en la gestión de riesgos de SI y CBS.

- **El órgano de gobierno:** Es quién establece la dirección de la organización y define la visión, misión y valores. También es quien elige el grado de aceptación de riesgos. Este agente se encarga de delegar responsabilidades para alcanzar los objetivos de la organización.
- **La Dirección:** Se divide entre roles de primera línea y de segunda línea. Los que están en la **primera línea** se encargan de dirigir las acciones, mantener la comunicación con el órgano de gobierno y establecer los procesos para la gestión de operaciones y riesgos. Asimismo, garantiza el cumplimiento de todas las expectativas legales, éticas y reglamentarias. La **segunda línea de la dirección** vigila y mide el desarrollo, implementación y mejora continua de las prácticas enfocadas a la gestión de riesgos.
- **Auditoría Interna:** La auditoría interna que constituye la **tercera Línea de defensa**, es independiente del órgano de gobierno y la dirección. Se encarga de asegurarse que la gestión de riesgos sea adecuada según los objetivos establecidos y promueve la mejora continuada. La independencia y objetividad son las dos características principales de este rol.

En primer lugar, los órganos de gobierno deben rendir cuentas de su supervisión a los stakeholders de la organización, comprometiéndose a vigilar sus intereses y a comunicarse de manera transparente sobre el logro de los objetivos. También deben fomentar una cultura que promueva el comportamiento ético y la responsabilidad, estableciendo estructuras y procesos para la gobernanza, así como delegando la responsabilidad y proporcionando recursos a la Alta Dirección para el logro de los objetivos de la organización. Asimismo, determinan el apetito de la organización por el riesgo y ejercen la supervisión de la gestión del riesgo (incluido el control interno). Además, mantienen la supervisión del cumplimiento de las expectativas legales, reglamentarias y éticas y establecen y supervisan una función de auditoría interna independiente, objetiva y competente.

En segundo lugar, la Alta Dirección, la cual comprende a la primera y segunda línea en el modelo, debe distinguir las labores a realizar por cada una de ellas. Mientras la primera línea se enfoca en la gestión operativa y de riesgos, asegurando el cumplimiento de leyes, regulaciones y aspectos éticos, la segunda comprende actividades como soporte y supervisión de la eficacia de la gestión de riesgos.

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

En tercer lugar, la función de la Auditoría Interna es la de rendir cuentas ante los órganos de gobierno y ser independiente de la Alta Dirección, prestando un asesoramiento independiente y objetivo y proveyendo, en su caso, de las salvaguardas necesarias para conseguirlo.

Finalmente, los proveedores externos deben proporcionar un aseguramiento adicional en cuanto a aspectos legales o regulatorios (protección a los stakeholders) o bien complementar a los proveedores internos de aseguramiento.

El modelo se basa en la estructura de enfoque estratégico, táctico y operacional propuesto por MINTIC, como se muestra en la siguiente gráfica.

Ilustración: Equipo de Gestión de Seguridad de la información en las entidades



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, en Roles y Responsabilidades MSPI, octubre 2021.

De acuerdo con los lineamientos definidos por MINTIC, se define para la ADRES el modelo desde las siguientes perspectivas:

7.2.3 Perspectiva estratégica del modelo de gobierno

7.2.3.1 Órgano de Gobierno

Se plantea la creación formal de un Comité de Seguridad de la Información que permita configurar una estructura de dirección que evalúe, dirija y supervise el Sistema de Gestión de la Seguridad de la Información de la ADRES, garantizando así el cumplimiento y participación de las partes interesadas, en especial los participantes en las responsabilidades de las tres líneas de defensa establecidas en el modelo.

Este órgano rector o de gobierno se enfoca en el aseguramiento de los activos de información de la ADRES y deberá brindar las garantías y recursos necesarios para una adecuada gestión de la protección de estos activos; y tendrá como responsabilidades las definidas en el capítulo 6.1 del presente documento.

El Comité base de dirección integrado por los siguientes roles de la ADRES:

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- Director de Dirección de Gestión de Tecnologías de la Información y las Comunicaciones - DGTIC
- Jefe de Oficina de Planeación y Gestión del Riesgo - OAPCR
- Director Dirección Administrativa y Financiera – DAF
- Jefe de la Oficina Asesora Jurídica - OAJ
- Responsable de Seguridad de la Información/Oficial de cumplimiento
- Jefe de Oficina de Control Interno (Invitado)
- Líderes de Proceso (Invitado, según la temática)

Relación con control Interno – Tercera línea de defensa

Este órgano rector o de gobierno se coordinará con la tercera línea de defensa, control interno, con el fin de orientar y programar el plan de auditoría a realizar sobre el Sistema de Gestión de Seguridad de la Información.

7.2.4 Perspectiva Táctica del Modelo de Gobierno

7.2.4.1 Segunda línea de defensa

La segunda línea de defensa desarrolla las siguientes responsabilidades

- Validación de cumplimiento de las definiciones del sistema de gestión de la seguridad de la información
- Proponer políticas y lineamientos en seguridad digital.
- Coordinar la ejecución del plan de control operacional del SGSI.
- Promover el comportamiento ético y la responsabilidad sobre la seguridad digital
- Validar el aseguramiento de los activos de información con la primera línea de defensa, terceros y proveedores.
- Coordinación entre las tres líneas de defensa
 - Definir protocolo de coordinación.
 - Identificar áreas grises que deban requerir una evaluación externa.
 - Participar en la elaboración de mapas de riesgo sobre los activos de información con la primera y tercera línea de defensa.
 - Definir protocolo de aseguramiento con proveedores.

7.2.4.2 Tercera línea de defensa

La tercera línea de defensa desarrolla las siguientes responsabilidades

- Auditoría Interna.
- Aseguramiento independiente del SGSI.
- Alineación con supervisores regulatorios.
- Alineación con Auditoría de tercera parte en caso de ser requerida.
- Rendición de cuentas a partes interesadas.

7.2.5 Perspectiva operacional

7.2.5.1 Primera línea de defensa

La primera línea de defensa desarrolla las siguientes responsabilidades:

- Uso adecuado de los activos de información a su cargo.
- Es responsable de:
 - Identificar, evaluar y valorar los riesgos asociados a los activos de información con relación a su *confidencialidad, integridad y disponibilidad*.
 - Mitigar y gestionar los riesgos de seguridad digital que se encuentren fuera de los límites de aceptación del apetito de riesgo.
 - Definir con el apoyo de la segunda línea de defensa los controles asociados a los riesgos identificados.
- Definir y ejecutar las acciones con base en los hallazgos y observaciones propuestas por la tercera línea de defensa.
- Atender a las políticas y lineamientos definidos.
- Definir y ejecutar procedimientos para el cumplimiento de las políticas y lineamientos establecidos en coordinación con la segunda línea de defensa.
- Gestionar los controles asociados a los activos de información a su cargo.

Seguridad Informática

Dada la importancia de las tecnologías de información y la infraestructura asociada, y que estas en gran medida custodian activos de información; se definen las siguientes responsabilidades para la seguridad informática:


- Asociadas a servicios tecnológicos.
 - Respuesta a incidentes relacionados con activos de información de los procesos de TI y activos tecnológicos que tienen impacto en la seguridad digital.
 - Realizar pruebas de vulnerabilidad y desarrollo de las oportunidades de mejora sobre las brechas encontradas.
 - Realizar monitoreo de seguridad sobre la infraestructura de TI.
 - Validar la adecuada aplicación de los controles establecidos en el SOA (Acuerdo de aplicabilidad).
- Asociadas a sistemas de información.
 - Establecer y validar los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad.
 - Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano.
 - Desarrollar pruebas de vulnerabilidad sobre los sistemas de información y aplicaciones.

7.2.5.2 Segunda línea de defensa

Las responsabilidades de la segunda línea de defensa a nivel operacional son:

- Coordinar la gestión de riesgos.
- Facilitar la implementación de prácticas efectivas de control de la gestión de la primera línea de defensa.
- Desarrollar actividades de soporte a la primera línea de defensa frente a la concientización y capacitación respecto de la seguridad digital.
- Vigilar el buen uso de los activos de información respecto de su confidencialidad, integridad y disponibilidad.

Coordinación con el comité nacional de seguridad digital – Coordinación sectorial

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

En el desarrollo de esta coordinación se establecen mesas de trabajo a nivel sectorial que serán coordinadas por el Ministerio de la salud y protección social.

7.3 Equipos de respuesta a incidentes de seguridad digital

El equipo de respuesta a incidentes estará compuesto por:

- Dueño del activo de información.
- Custodio del activo, si aplica.
- Responsable del control, aplica cuando no está a cargo del dueño del activo de información.
- Líder o responsable del proceso afectado
- Responsable de soporte por parte de IT
- Segunda línea de defensa – OSI

Para su gestión se utilizará lo definido en el procedimiento de atención a incidentes.

8. 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 APTI-PL01, 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.

8.1 Criterios de la seguridad de la información

- **Confidencialidad:** Hace referencia a la protección de información cuya divulgación no está autorizada – (la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados – ISO27001).
- **Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su almacenamiento final o destrucción - (mantenimiento de la exactitud y completitud de la información y sus métodos de proceso -ISO27001).
- **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera de acuerdo con la clasificación y retención establecida bien sea por la normatividad vigente o por las políticas de la Compañía, al igual que los recursos necesarios para su uso, en los términos previstos en las normas que apliquen con relación al tipo de dato almacenado – (acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran – ISO27001).

8.2 Criterios de calidad de la Información

- **Exactitud:** La exactitud se mide a base de información correcta y exacta. Usualmente se recomienda que para validar la exactitud se compare la información con otra ya investigada y verificar los datos en fuentes impresas. Es importante considerar que la información no actualizada tiende a no ser exacta.

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- **Autoría:** La autoría está dada por el responsable del sitio -puede ser una persona, un grupo de personas reunidas por un objetivo determinado, o una entidad-, su prestigio y las fuentes utilizadas.
- **Objetividad:** permite la presentación del conocimiento de manera neutral, por ello, es una característica imprescindible de todos los contenidos que exponen los resultados de una investigación, análisis científico o gestión que pretenda aportar información.
- **Organización:** Se espera que la información se encuentre ordenada lógicamente y que cada segmento de esta información se relacione con las demás.
- **Actualidad:** Es la calidad de validar que la información se encuentre actualizada, con la incorporación de nuevos recursos y contenido acorde al momento.
- **Cobertura y contenido:** La información manifiesta especial cuidado en el tratamiento y el enfoque dado al desarrollo de un tema, tópico o teoría de un campo disciplinar o área del conocimiento.
- **Acceso:** En esta categoría se engloban los aspectos relativos al cómo se accede a la información, tiempo de espera y seguridad.

8.3 Sanciones previstas por incumplimiento

El incumplimiento de las disposiciones en las políticas aquí definidas será sancionado de conformidad a su gravedad, de acuerdo con la normativa vigente al interior de la ADRES establecidas por el control Disciplinario.

8.4 Unidad de seguridad de la información y la ciberseguridad

La Junta Directiva de la ADRES, será la responsable de aprobar esta Política y la autorización de sus modificaciones.

La Dirección de la ADRES, asigna las funciones relativas a la Seguridad de la Información y Ciberseguridad al Oficial o Responsable de Seguridad de la Información quien tendrá a cargo las funciones relativas del rol, lo cual incluye la supervisión de todos los aspectos inherentes tratados en el presente documento, el control del cumplimiento de la Política de Seguridad de la Información y Ciberseguridad, así como garantizar que las políticas específicas, procesos, procedimientos y/o controles que se deriven de esta estén alineados con la Política y ésta con las estrategias y modelos del negocio.

Se asigna al Comité de Seguridad de la Información (Definidos en la estructura de Gobierno prevista), del cual el Oficial de Seguridad de la Información y Ciberseguridad hace parte, la función de controlar el cumplimiento de las políticas específicas, procesos, procedimientos y/o controles de Seguridad de la Información y Ciberseguridad.

Todo el personal, sea cual fuere su nivel jerárquico, es responsable de la implementación y cumplimiento de esta Políticas de Seguridad de la Información y Ciberseguridad dentro y fuera de sus dependencias, así como el cumplimiento por parte de su equipo de trabajo.

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

La violación a la Política de Seguridad de la Información y Ciberseguridad será motivo para adelantar acciones disciplinarias, civiles y penales según aplique. La ADRES también llevará a cabo acciones judiciales donde lo considere apropiado.

8.5 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, 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 íntegro 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 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.
- La Oficina Asesora de Planeación y Control de Riesgos, en coordinación con la Dirección de Gestión de Tecnologías de Información y Comunicaciones, definirán anualmente el plan de capacitación y sensibilización frente a Seguridad de la Información y la Ciberseguridad, 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 en torno a la Seguridad de la Información.
- Los Servidores Públicos, contratistas y terceros de la ADRES sin excepción deben:

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- 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 (cuando aplique) de acuerdo con las condiciones de complejidad que sean definidas para cada una de ellas.
- Cumplir a cabalidad los lineamientos para el uso de firma digital certificada y/o firma electrónica que definan de manera conjunta la Dirección Administrativa y Financiera y la Dirección de Gestión de Tecnologías de Información y Comunicaciones.
- 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 ésta al no poder ser consultada, copiada o utilizada por 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.
- 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.

8.6 Política de Gestión de Activos de Información.

Este grupo de políticas hacen referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios y contratistas los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los Activos de Información.

El objetivo es proteger los activos de acciones perjudiciales o ilegales que podrían ser realizadas por individuos en forma intencional o no intencional y establecer los lineamientos a los responsables para ejercer un uso apropiado de los activos de información, dispositivos electrónicos y recursos de la red de acuerdo con las políticas y estándares de la entidad, así como el cumplimiento de leyes, normas y reglamentos que se rigen a nivel nacional, e internacionales que apliquen en Colombia.

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

8.6.1 Identificación y clasificación de Activos de Información

- Los activos de información de la ADRES serán identificados y/o actualizados por lo menos una vez al año, o antes si el propietario de la información así lo considera, de acuerdo con el nivel de impacto o criticidad del activo. Este lineamiento debe ser cumplido por los jefes de dependencia de acuerdo con la guía "Metodología de Valoración y Clasificación de Activos".
- Los propietarios o dueños de la información deben garantizar la identificación clara de todos los activos correspondientes a sus procesos, y consolidarlos de acuerdo con la metodología de selección, caracterización y clasificación de los activos de información consignada en la herramienta tecnológica Eureka.
- Es responsabilidad de los dueños de la información asegurar que posee todos los elementos necesarios para evaluar el nivel adecuado de clasificación, teniendo en cuenta el posible impacto causado por una clasificación en un nivel de seguridad inferior al adecuado.
- 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 tiene las siguientes atribuciones en esta gestión de activos de información:
 - La DGTIC es 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 Responsable 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 auditoría 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.

8.6.2 Disposición de Activos de Información

- 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. Para lo cual se define:

- *Almacenamiento de bases de datos:* Repositorios de información destinados para la correcta custodia de la información que se genera dentro de los diferentes sistemas de información de la Entidad.
 - *Almacenamiento colaborativo:* Entorno donde dos o más usuarios pueden trabajar al mismo tiempo en un mismo documento o archivo, todo para hacer cualquier tarea más dinámica y ágil dentro del ciclo de vida de la información antes de su disposición final. Por lo tanto, corresponderá a la información de gestión o acceso recurrente.
 - *Almacenamiento de transferencia de información:* Repositorios de información cuyo propósito es la transferencia de documentos o archivos con terceros, dicha transferencia, se puede llevar a cabo de manera temporal o permanente.
 - *Almacenamiento histórico:* Corresponde a los repositorios de información, cuya finalidad es conservar documentos, que por su contenido histórico deben ser respaldados conforme con las políticas de la Entidad y las Tablas de Retención Documental que se definan en cada proceso.
- Los recursos de red que ha dispuesto la ADRES, tales como Directorios compartidos, Portal web, Intranet, Repositorio del SIGI, OneDrive etc, no deben ser utilizados para el almacenamiento de información que no es para propósitos laborales, ejemplos de información no permitida son: Material pornográfico, videos, películas, música, fotos, etc.
 - El almacenamiento de información institucional que se genere directamente sobre las estaciones de trabajo o en estaciones de cómputo externas a la Entidad no es permitido y de hacerse es de responsabilidad única del servidor público o contratista que lo realice.
 - El líder de cada proceso o quien este defina en su equipo de trabajo es el encargado de realizar la verificación del correcto uso de las herramientas de almacenamiento definidas al interior de la Entidad, dicha validación se debe efectuar como mínimo en las fechas definidas dentro del monitoreo de riesgos de seguridad de la información.
 - 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 establecido 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 personal que la Dirección Administrativa y Financiera destine para tal fin a título propio o tercerizado.
 - 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.
 - 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 y 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.

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

8.6.3 Uso adecuado de Activos de Información

- Todos los usuarios deben reportar oportunamente el robo, pérdida, adulteración o divulgación no autorizada de información de la ADRES.
- Solo se puede acceder, usar, consultar o compartir información de la ADRES si está autorizado para ello.
- Los funcionarios son responsables de ejercer un buen juicio sobre el uso de aplicaciones de interés personal y serán sujetos de control por parte del responsable de Seguridad de la Información.
- Por razones de seguridad y mantenimiento de la red, el funcionario autorizado dentro de la entidad puede monitorear equipos, sistemas y el tráfico de red en cualquier momento y sus actividades serán registradas, dejando huella de su traza, cumpliendo los principios de protección de datos personales definidos en la Ley.
- La ADRES se reserva el derecho de auditar las redes y sistemas de manera periódica para asegurar el cumplimiento del buen uso de los activos de información.
- En ninguna circunstancia un funcionario de la ADRES está autorizado a participar en actividades que sean ilegales bajo la leyes nacionales e internacionales, utilizando recursos e información de la entidad.
- Actividades que están estrictamente prohibidas, sin excepciones:
 - Violaciones a los derechos de cualquier persona o empresa protegida por derechos de autor, secretos de marca, patentes u otra propiedad intelectual o a leyes o reglamentos similares, incluyendo, pero no limitado a la instalación o distribución de software "pirata" u otros productos de software que no tengan licencia apropiada para su uso en la empresa.
 - La copia no autorizada de materiales con derechos de autor, incluyendo, pero no limitado a la digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos de autor, la música con derechos de autor y la instalación de software con derechos de autor para el cual la empresa o el usuario final no cuenta con una licencia activa, está estrictamente prohibido.
 - El acceso a datos, servidores o cuentas para cualquier propósito que no sea para la realización de actividades del negocio, incluso si cuenta con acceso autorizado, está prohibido.
 - La exportación de software, información técnica, software o tecnología de cifrado, en violación de las leyes internacionales o regionales de control de exportaciones, es ilegal. Debe ser consultado el manejo adecuado antes de la exportación de cualquier material de esta índole.
 - Introducción de programas maliciosos en la red o en servidores (por ejemplo, virus, gusanos, caballos de Troya, bombas de correo electrónico, etc.).
 - Dar contraseñas de sus cuentas a otras personas o permitir el uso de sus cuentas por otros. Esto incluye a amigos y familiares cuando el trabajo se está haciendo en casa.
 - El uso de un activo de cómputo de la empresa para participar, reclutar o transmitir materiales que están en violación de las leyes locales de acoso sexual u hostilidad en el lugar de trabajo.
 - Hacer ofertas fraudulentas de productos, artículos o servicios procedentes de cualquier cuenta propiedad de la ADRES.
 - Efectuar brechas de seguridad o interrupciones de la comunicación en red. Las violaciones de seguridad incluyen, pero no se limitan a acceder a datos para los que no se es destinatario o conectarse a un servidor o cuenta a la cual el empleado no está expresamente autorizado a acceder, a menos que estas funciones estén dentro del alcance de sus funciones regulares. Para los propósitos de esta sección, "interrupción" incluye, pero no se limita al espionaje en la red, inundaciones de ping, suplantación de paquetes, denegación de servicios, etc., con fines maliciosos.

- El Barrido de Puertos y escaneos de seguridad están expresamente prohibidos a menos que se realice una notificación y autorización previa ante el Oficial de Seguridad de la Información.
- La ejecución de cualquier forma de análisis de red que intercepte datos no destinados a la máquina del empleado, a menos que esta actividad sea parte del trabajo normal del empleado.
- Eludir la autenticación de usuarios y la seguridad de cualquier equipo de cómputo, de red o cuenta.
- La introducción de sistemas Honeypots, Honeynets o tecnología similar en la red empresarial sin autorización.
- Interferir o negar servicios a cualquier usuario diferente a él mismo (por ejemplo, ataque de denegación de servicio)
- El uso de cualquier programa / script / comando o el envío de mensajes de cualquier tipo, con la intención de interferir o deshabilitar las sesiones de terminal de algún usuario, a través de cualquier medio, de forma local o a través de Internet / Intranet / Extranet.

8.6.4 Etiquetado de información


- La rotulación de los activos de información se define de acuerdo con lo establecido en la guía "Metodología de clasificación y valoración de activos de información" y de conformidad con lo establecido en las Tablas de Retención Documental. Asimismo, deberá efectuarse conforme a los lineamientos que adopte la entidad.

8.6.5 Gestión de medios removibles

- 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.

8.6.6 Devolución de activos de información

- La devolución de los activos de información tales como computadores de escritorio, computadoras portátiles, teléfonos inteligentes, diademas, tabletas, etc., asignados a los funcionarios, contratistas o terceros se define de acuerdo con lo establecido en la guía de Gestión Administrativa definida por la Dirección Administrativa y Financiera.
- 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 Dirección Administrativa y Financiera de la ADRES defina para tal fin.

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

8.7 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 realice 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 a cambiar sus contraseñas cuando ingresan por primera vez.
 - Exigir 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,

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

contratistas, proveedores) frente Acceso Físico a las instalaciones de la ADRES, esto de acuerdo con lo consignado en 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.

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

8.8 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 TI 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.

8.9 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 transferencia o transmisión 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 transferencia o transmisión 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.
- Los funcionarios que gestionen el intercambio de información y utilicen firmas digitales en sus documentos deberán:

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- Evitar la utilización no autorizada de sus datos en la creación de la firma, actuando con la debida diligencia.
- Revocar la firma digital al momento de desvinculación de la entidad.
- Reportar cuando la información firmada enviada o recibida halla quedado en entredicho o se considere que los datos de la firma están en riesgo.
- Hacer uso responsable de los mecanismos de aplicación de firma digital, teniendo en cuenta que son de uso personal e intransferible.
- Los poseedores de mecanismos de firma digital deben estar debidamente autorizados y se debe tener control e inventario de los funcionarios autorizados al uso de firma digital de la ADRES.
- La mensajería instantánea en la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES, está asociada a los servicios que se tengan licenciados para el 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 el envío 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 de la Política de Comunicaciones de ADRES, el cual está a cargo de la Dirección General de la Entidad. De igual manera dentro de esta política se encuentran 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 o 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

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

Entidad y de la gestión 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) Sea objeto de una reclamación por violación, que se considera como una violación de la propiedad intelectual, o que de otro modo es censurable.

8.10 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:
 - Análisis de Impacto de Negocio
 - Activos de información críticos.
 - Procedimientos para la Gestión de la Continuidad de Negocio.
 - Árboles de comunicación de crisis.
 - 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 en TI 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.

8.11 Política para la Gestión de Incidentes de Seguridad

Esta política establece los mecanismos de coordinación para dar respuesta a los incidentes de seguridad de la información y habilita a la entidad para una remediación rápida, recopilación de datos y reporte de los eventos que afectan la infraestructura de información y tecnología.

Esta política se aplica a todos los funcionarios, contratistas y terceros que prestan sus servicios a la organización. Lo que no está permitido en la presente política, está prohibido.

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- El responsable de seguridad de la información con su grupo de apoyo es responsable de evaluar si los eventos que se reporten sobre los servicios o sistemas de información se deben tratar como incidentes de seguridad de la información.
- El responsable de seguridad de la información es el responsable de dar respuesta, realizar el aislamiento y recuperación de los accesos a sistemas de comunicaciones y cómputo afectados por el incidente.
- Cada responsable de área o proceso debe garantizar que los incidentes sean apropiadamente registrados y almacenados de acuerdo con el procedimiento de gestión de incidentes de seguridad.
- Todos los funcionarios, contratistas y terceros que presten sus servicios a la ADRES deben informar al responsable del área o proceso la ocurrencia de eventos y/o incidentes de seguridad de la información tan pronto como sea posible.
- Todos los funcionarios, contratistas y terceros que presten sus servicios a la ADRES deben informar a la DGTIC cualquier debilidad de seguridad de la información o acción sospecha que observen en los servicios de informática, sistemas de información, aplicaciones o instalaciones de la Entidad.
- 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 tengan 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 líder 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 definan 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) por el equipo de respuesta a incidentes de la entidad.
- Cualquier incidente de seguridad de la información se debe registrar y se debe realizar el tratamiento de este, empleando el procedimiento de gestión de incidentes de seguridad de la información OSTI-PR03.
- Cualquier dispositivo de uso personal como teléfonos inteligentes, computadores portátiles, tabletas, u otros dispositivos de cómputo que estén implicados en incidentes de seguridad de la información en la ADRES, pueden ser sometidos a cadena de custodia o protección para fines de investigación o evidencia ante procesos administrativos o legales, previa coordinación del procedimiento con el propietario del equipo.
- Para prevenir la ocurrencia de incidentes de seguridad de la información la entidad, aplicará los procedimientos de su Sistema de Gestión de Seguridad de la Información para llevar a cabo actividades de prevención de incidentes, supervisión y filtrado de anomalías que puedan afectar a la seguridad de la información o los recursos de información y tecnología.
- En caso de ser requerido por autoridad competente o grupos especializados en el tratamiento de incidentes de seguridad de la información de la ADRES puede suministrar el plan de respuesta o remediación específico para un incidente para que se evalúe su efectividad, solicitar apoyo, demostrar debida diligencia u otros propósitos definidos por la entidad, dentro del marco del Decreto 338 de 2022.

8.12 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 SGSI 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, transmitir y eliminar) de los titulares cuando la ADRES actúe 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.

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

8.13 Mejoramiento Continuo

- La ADRES en cabeza del Responsable u Oficial de cumplimiento de Seguridad de la Información Comunicaciones a manera de autoevaluación, realizará por lo menos una vez 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 o en su defecto el instrumento que se defina para tal fin.
- El responsable 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 y la Oficina Asesora de Planeación y Control de Riesgos deben formular 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 desde el Direccionamiento Estratégico de la entidad.
- La Oficina de Control Interno de la ADRES debe realizar seguimientos a la implementación del Sistema de Gestión de Seguridad de la Información -SGSI 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.

9. POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

9.1 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 Soporte y Operaciones TI 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.
 - 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.

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- 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.

9.2 Política de seguridad de correo electrónico institucional

La ADRES hace uso de herramientas colaborativas tecnológicas como el correo electrónico, en el cual todos los mensajes generados o transmitidos se consideran como información confidencial y propia de la Entidad, la cual puede ser monitoreada sin la autorización del usuario, en consecuencia, de lo anterior se ha implementado los siguientes lineamientos en relación con la seguridad en el correo electrónico:

- La única cuenta de correo electrónico autorizada para el envío y recepción de información correspondiente a las actividades propias de ADRES es la que fue asignada a cada usuario por parte del área de tecnología y la cual pertenece al dominio adres.gov.co.
- La cuenta de correo electrónico autorizada debe ser usada únicamente con fines propios de la ADRES y es de responsabilidad directa del remitente toda aquella información que sea emitida a través de ella.
- Es responsabilidad del área de tecnología realizar copias de seguridad de todas las cuentas de la plataforma (correos entrantes y salientes).
- Es responsabilidad del Auditor Interno realizar validaciones aleatorias al sistema de copias de seguridad del correo electrónico con el fin de garantizar la fiabilidad y calidad de este.
- Es responsabilidad de los líderes de proceso realizar validaciones aleatorias a las copias de seguridad del correo electrónico de sus colaboradores
- Es obligatorio para todos los usuarios que tengan la cuenta de correo electrónico autorizada asignada por la Entidad contenga la firma corporativa, nombre de la persona responsable de la cuenta, área a la que pertenece, cargo y número telefónico con extensión.
- Es obligación del usuario reportar al área de tecnología (mesa de servicios) si sospecha que su cuenta está siendo usada por una tercera persona o considera que los correos son con fines sospechosos, maliciosos o como spam.
- Está prohibido difundir contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas sin licencia, amenazas, estafas, esquemas de enriquecimiento piramidal, virus, SPAM o código malicioso.
- Es responsabilidad del área de talento humano notificar oportunamente al área de tecnología, sobre todo personal que por cualquier motivo deje de laborar en la empresa, con el fin de dar de baja inmediatamente los recursos de correo asignados han dicho personal.
- Es responsabilidad el área de tecnología realizar una copia de la información del correo electrónico inhabilitado de la persona que se retira para respaldo – VALIDAR CON TI

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- La única persona autorizada para solicitar acceso a la copia del correo electrónico de respaldo de la cuenta inhabilitada es el jefe inmediato de la persona que se retiró.
- Está prohibido que los usuarios envíen mensajes masivos con excepción de los cargos debidamente autorizados.
- Es responsabilidad de los usuarios que requieran el envío de documentos adjuntos y que estos contengan información correspondiente a ciudadanos o información de carácter privado de la Entidad, deben usar los mecanismos de seguridad tales como formatos PDF con contraseñas de apertura del documento y/o bloqueo para la edición de datos que atenten contra la integridad de la información o violación a la privacidad de estos.

9.3 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 login 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.

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022


9.4 Política de escritorios y pantalla limpios

- Todos los funcionarios contratistas y colaboradores, deben conservar el escritorio limpio de información de la ADRES que pueda ser adulterada, copiada o utilizada por terceros que no tengan autorización a ella.
- Se debe garantizar que los usuarios tengan la pantalla de su estación de trabajo limpia de toda información que pueda ser aprovechada por terceros que no tengan autorización sobre la información utilizada.
- Se debe aplicar mecanismos de protector de pantalla estándar en todas las estaciones de trabajo y equipos portátiles de la entidad, de tal forma que se active en el menos tiempo posible y que para su desactivación se requiera código de seguridad.
- Los funcionarios y colaboradores no deben dejar en el escritorio documentos o información de la entidad sin la custodia adecuada.
- En el uso de los elementos comunes en salas de reuniones como tableros y otros elementos que puedan contener información de la ADRES
- Se deben establecer las medidas de control necesarias que permitan comprobar el correcto cumplimiento de estos lineamientos.

9.5 Respaldo y Restauración de la Información

Todos los activos de información deben ser protegidos y respaldados, de acuerdo con los procedimientos operativos definidos en cada uno de los procesos. Las diferentes áreas de la Adres deben gestionar las pruebas en forma controlada, para asegurar que las copias de seguridad puedan ser correctamente respaldadas y leídas. La DGTIC estará encargada de proteger y recuperar los activos de información garantizando la infraestructura definida para este fin.

- Los contenidos para el respaldo de información o back-up deben determinarse considerando las necesidades de la ADRES, sus aplicaciones y la criticidad de los activos de información y acorde con los criterios identificados en la caracterización de estos. El respaldo efectuado debe reflejar la criticidad de los activos de 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 almacenamiento de bases de datos, almacenamiento de transferencia de información y almacenamiento histórico, así como la de los buzones de correo electrónico de los Servidores Públicos y Contratistas.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones debe realizar pruebas periódicas de restauración en ambientes de prueba de la información que se encuentre dentro de las unidades almacenamiento de bases de datos y almacenamiento de transferencia de información, esto con el propósito de evaluar la correcta generación de las copias de seguridad.
- Es responsabilidad del líder de cada proceso o quien este delegue de realizar las copias de respaldo de la Información que se encuentra en el almacenamiento colaborativo de cada proceso, la periodicidad de respaldo será independiente en cada proceso y debe ser definida conforme a la criticidad de los documentos propios del proceso. Dichas copias de respaldo tendrán un periodo de retención de un año, salvo las excepciones que explícitamente el solicitante defina dentro de su requerimiento.

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- Cada proceso debe realizar pruebas periódicas de restauración en ambientes de prueba de la información que se encuentre dentro de las unidades almacenamiento histórico asignadas y debe ser definida conforme a la criticidad de los documentos propios del proceso, esto con el propósito de evaluar la correcta generación de las copias de seguridad.
- 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.
- 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.
- 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 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.

9.5.1 Plan de copias y métodos aplicables

Se contará con herramientas de Back Up para realizar una toma especializada de los respaldos de la información a los sistemas de información, bases de datos y repositorios de información definidos en la infraestructura de TI


Los requisitos de protección de la información serán definidos por los dueños de los activos, así como los propietarios de los sistemas de información y bases de datos y la DGTI deberá:

- Documentar un plan de copia de seguridad donde se establezca esquemas de qué, cuándo, con qué periodicidad y cuál es la criticidad para realizar las copias de respaldo de información.
- Definir la custodia y almacenamiento de las copias
- Mantener un inventario y bitácora de las copias que se realizan y de las copias que se restauran
- Realizar un proceso de depuración y borrado de Backup de Base de Datos cuando de requiera

9.5.2 Ciclos de Back Up

La frecuencia de realización del respaldo de la información debe estar determinada por las necesidades de negocio y los requerimientos normativos, legales y reglamentarios, y de cada proceso, teniendo en cuenta, las Tablas de Retención Documental de la ADRES, el Análisis de Impacto del Negocio (BIA) que determina la criticidad de los procesos.

Los ciclos de back-up incluirán copias periódicas para retención (semanales, mensuales, trimestrales y/o anuales) que deberán ser administrados y determinados por la dirección de Gestión de


	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

Tecnologías de la Información, para satisfacer los requisitos del negocio, de auditoría, continuidad o regulatorios.

9.6 Acceso remoto

El alcance de esta política es para todos los colaboradores, contratistas y proveedores que requieran acceso a la infraestructura de TI, los sistemas de información o aplicaciones de la ADRES de manera remota. Su objetivo es asegurar que los activos de información que se utilizan a través del acceso remoto estén protegidos y en cumplimiento de los requerimientos y lineamientos de la ADRES.

- El custodio de la información debe implementar controles para limitar el tiempo de acceso y la información utilizada en el entorno de acceso remoto (teletrabajo, trabajo remoto, trabajo en casa), basados en los requerimientos presentados por el dueño de la información.
- El acceso remoto a los activos de información de la Entidad sólo debe ser permitido luego de cumplir los requisitos de autenticación.
- Está prohibido el uso de software de control remoto para ingresar y utilizar los recursos informáticos de la Entidad sin autorización formal del Oficial de Seguridad de la Información.
- La DGTIC debe proporcionar los controles de seguridad y lineamientos necesarios para los entornos en los que el acceso remoto esté aprobado.
- El Oficial de Seguridad de la Información debe definir las medidas de seguridad para los usuarios que trabajan de forma remota.
- Está prohibido realizar alguna actividad de tipo remoto (teletrabajo, trabajo en casa o trabajo remoto) sin la debida solicitud por parte del director o jefe de la dependencia 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 prestar 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.

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

9.7 Política de protección contra código malicioso

Como parte de la arquitectura de TI de ADRES se requiere tener una configuración de sistemas de antivirus y antimalware que tenga al menos:

- Mecanismos de administración que permitan el control y despliegue de las políticas y reglas de control establecidas, así como sus actualizaciones y sincronización automática o en el menor tiempo posible.
- Facilitar la protección de la mayoría de medios posibles, como internet, correo electrónico, software ejecutable, scripts, entre otros; y restringir la ejecución automática de aplicaciones que no estén debidamente autorizadas.
- Controlar y analizar las posibles descargas de software malicioso.
- Monitoreo permanente de la red de datos frente a la detección y búsqueda de virus.
- Se debe realizar acciones de contención y eliminación ante un incidente o posibilidad de encontrarse alguna variante de código malicioso
- Se debe evitar que los usuarios (funcionarios, 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.

9.7.1 Responsabilidades de los usuarios

- El custodio de la información debe establecer los procedimientos, instructivos y controles para tratar el código malicioso.
- El custodio de la información es responsable por que los sistemas contra código malicioso analicen los archivos adjuntos de los correos electrónicos, los archivos descargados de Internet, los medios de almacenamiento y las páginas de Internet accedidas.
- El custodio de la información es responsable por que los sistemas contra código malicioso se ejecuten automáticamente al encender los sistemas, permanezcan activos y actualizados, y analicen periódicamente la totalidad del software y archivos de los activos de información.
- El custodio de la información es responsable por prevenir la ejecución y el uso del código móvil no autorizado.

9.7.2 Por parte de los Usuarios:

- Evitar cualquier acción que permitan o faciliten generar alguna posibilidad de contagio de virus.
- Eliminar todo archivo, documento anexo o mensaje desconocido sospechoso que sea entregado a través de los correos electrónicos, internet, o medios extraíbles.
- Reportar cualquier situación que se pueda estar relacionada con virus o malware, a la mesa de ayuda para realizar el respectivo análisis dentro del procedimiento de manejo de incidentes
- Utilizar únicamente el software autorizado para la detección y protección de virus y malware y por lo tanto no deberá utilizar otro tipo de soluciones.

9.7.3 Monitoreo y Capacitación

- La ADRES realizará el monitoreo constante de la red de datos y equipos de TI asociados y de uso en esta red respecto de los servicios de TI y el intercambio e interoperabilidad, así como los medios de almacenamiento de información definidos en ambientes colaborativos. La entidad se reserva el derecho de monitorear estaciones de trabajo, portátiles o equipos móviles que participen en el uso de los activos de información de la ADRES y su interoperabilidad.

- La ADRES, dentro del desarrollo de su programa de capacitación y sensibilización, programará y planeará capacitaciones frente a la prevención y tratamiento contra los virus y diferentes códigos maliciosos con el fin de que los funcionarios y colaboradores conozcan y utilicen adecuadamente las acciones de mitigación implementadas en la Entidad con el fin de disminuir la posibilidad de mitigación de estos escenarios de riesgo.

9.8 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.

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

Está política es aplicable a todos los procesos de la ADRES y a terceros que deseen desarrollar mecanismos de interoperabilidad.

- 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.

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

- Definir e implementar controles criptográficos en las redes para garantizar la protección de la información transmitida por medio de servicios como correo electrónico, red de datos, y otros.
- Definir e implementar los procedimientos respecto a la administración de claves, de la recuperación de la información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado
- Brindar apoyo a los propietarios de información, en la aplicación o uso de técnicas de cifrado autorizadas por la ADRES. Respecto de la preparación, transmisión o resguardo de la información
- 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.
- Los dueños del activo de información deberán:
 - Atender los requerimientos de las partes interesadas en relación con la necesidades para la protección de información para la preparación, resguardo y transmisión de información.
 - Realizar con base en el análisis de riesgos la información que requiere ser cifrada para determinar la técnica y procedimiento apropiado que garantice su seguridad al nivel requerido.
 - Revisar periódicamente las funcionalidades criptográficas aplicadas a sus activos de información respecto de su eficacia.
- Se definen los siguientes niveles de cifrado para atender las necesidades y requerimientos en los procesos de la ADRES
 - Cifrado de archivos
 - Cifrado de Bases de datos
 - Cifrado de las comunicaciones
 - Cifrado de correo electrónico y firma digital
 - Almacenamiento cifrado

9.10 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.

9.11 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.

10. RIESGOS

El modelo de Seguridad de la Información y Ciberseguridad de la ADRES trabaja el riesgo asociado como una función entre la amenaza y las vulnerabilidades que conforman la causa del escenario de riesgo para su identificación, evaluación y valoración, acorde con la metodología integral de riesgos adoptada y en concordancia con los lineamientos de función pública que aplica la Oficina de Planeación y Gestión del Riesgo de la Adres.

La medición y actualización de la calificación de riesgo de Seguridad de la Información y Ciberseguridad se debe realizar a todos Activos de Información de todos los procesos de la entidad de manera periódica y por lo menos una vez al año, esta responsabilidad recae en la Oficina de Planeación y Gestión del Riesgo y en el Oficial de Seguridad de la Información y Ciberseguridad, en conjunto los propietarios o dueños de los activos de información

11. CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN

11.1 Enfoque preventivo

El enfoque preventivo del Sistema de Gestión de la Seguridad de la Información en la ADRES se basa en las funciones de Identificación de posibles amenazas y la Protección de las vulnerabilidades existentes (NIST CSF 1.1). Con relación a la Identificación se desarrollan las siguientes actividades:

- Gestión de activos desarrollada con base en la política definida en el numeral 7.7 del presente documento, desarrollando y manteniendo un inventario de activos de información y activos relacionados con su tratamiento y descripción, teniendo en cuenta su dueño o propietario, su existencia, y a que proceso pertenecen.
- Análisis del entorno del negocio de la ADRES respecto de su rol en la sociedad, la infraestructura tecnológica que la soporta, la cadena de valor de los proveedores que apoyan el desarrollo de los procesos del negocio y la interacción continua con los diferentes participantes en el ecosistema financiero de salud del país. Desarrollando un análisis del impacto del negocio en el contexto externo e interno, respecto de amenazas e incidentes de seguridad de la información y ciberseguridad para y generar una resiliencia efectiva en la operación normal, bajo ataque y en fase de recuperación.
- Gestión de Gobierno, con base en las definiciones del numeral "6 Modelo de Gobierno de Seguridad de la Información" del presente manual, desarrollar un control operacional del sistema teniendo en cuenta las definiciones roes y responsabilidades definidas.
- Evaluar los riesgos asociados a los escenarios de seguridad de la información y la ciberseguridad (Agentes de amenaza, tipos de amenazas, dimensiones afectadas, tipos de activos afectados, identificación de vectores de ataque y responsables del escenario) con base en la gestión integral del riesgo definida en la ADRES, gestionando los controles asociados y estrategias de mitigación de los riesgos
- Analizar y evaluar los riegos de seguridad de la información y la ciberseguridad asociados a la cadena de proveedores y a los participantes en el ecosistema financiero de la salud.


Con relación a la Protección se desarrollan las siguientes actividades:

- Gestionar las identidades y credenciales de los participantes en el negocio de la ADRES, y gestionar el control de acceso de estos con base en su rol y privilegios asignados
- Definir y desarrollar un programa de capacitación y concienciación en materia de seguridad de la información y ciberseguridad con el fin de adquirir habilidades, cambiar hábitos y estar informado aplicable a todos los participantes del SGSI
- Proteger la integridad de los datos, gestionando su aseguramiento y garantizando las capacidades de TI para el negocio (Respaldo de la información, gestión del cambio, ciclo de vida del desarrollo y líneas base de la configuración de la seguridad con base en el principio de menor funcionalidad).
- Aplicar el uso de tecnologías de la información, estableciendo redes y comunicaciones protegidas, mecanismos de monitoreo y prevención de pérdida de datos (DLP) y monitoreo de actividades y registros de operación (Logs).

11.2 Enfoque reactivo

El enfoque reactivo del Sistema de Gestión de la Seguridad de la Información en la ADRES se basa en las funciones de Detección de las amenazas y eventos o anomalías existentes (NIST CSF 1.1). Con relación a la Detección se desarrollan las siguientes actividades:

- Gestión adecuada y cooperativa d ellos incidentes
- Supervisión continua de la operación del SGSI
- Establecer un esquema de seguridad de la información y manejo de eventos como sus siglas en ingles SIEM y operar un servicio de centro de operaciones de seguridad digital como sus siglas en inglés SOC.

	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
			Versión:	04
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

11.3 Respuesta y comunicación

El enfoque de respuesta y comunicación del Sistema de Gestión de la Seguridad de la Información en la ADRES se basa en las funciones de Responder ante cualquier incidente de seguridad de la información y ciberseguridad materializado.

Con relación a la Respuesta se desarrollan las siguientes actividades:

- Como parte del modelo de atención a incidentes en la respuesta se establecen los protocolos de activación de CSIRT.
- Restablecimiento de las funciones operacionales.
- Registros de actividades y generación de informes correspondientes.

11.4 Recuperación y aprendizaje

El enfoque de recuperación y aprendizaje del Sistema de Gestión de la Seguridad de la Información en la ADRES se basa en las funciones de Responder ante cualquier incidente de seguridad de la información y ciberseguridad materializado.

Con relación a la Recuperación y aprendizaje se desarrollan las siguientes actividades:

- Recuperar el negocio en niveles aceptables garantizando su continuidad
- Generar la capacidad de anticipar eventos y adaptarse constantemente al cambio y recuperarse de los incidentes y circunstancias que afecten a la entidad, como un mecanismo de generación de resiliencia.
- Establecer mecanismos de aprendizaje continuo y generación de conocimiento alrededor de la gestión de incidentes.

12. 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.

13. 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.

14. VIGENCIA

La presente política entra en vigor el día 21 de diciembre de 2022.

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.	Olga Marcela Vargas Valenzuela Asesora OAPCR

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

		Cambio de codificación de la política conforme al mapa de procesos actual de la Entidad.	
03	18 de Junio de 2021	Actualización de lineamientos definidos en los capítulos 7.1 Obligaciones y Deberes del Recurso Humano, 7.2 Gestión de Activos de Información, 7.3 Clasificación de la Información 7.7 Continuidad del Negocio, 8.1 Gestión de la Tecnología y 8.3 Respaldo y restauración de la información. Actualización de encabezado conforme con nueva imagen institucional de la ADRES	Olga Marcela Vargas Valenzuela Asesora OAPCR
04	04 de mayo de 2023	Actualización general del manual	Daniel Eduardo Cabezas Murillo Contratista OAPCR

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Rodolfo Uribe Duarte Contratista Oficina Asesora de Planeación y Control de Riesgos Fecha: 15 de junio de 2022	Olga Marcela Vargas Jefe Oficina Asesora de Planeación y Control de Riesgos Fecha: 12 de agosto de 2022	Félix León Martínez Director General de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud- ADRES Comité Institucional de gestión y desempeño Fecha: 12 de diciembre de 2022

ADRES	PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
	MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Versión:	04
			Fecha:	12/12/2022

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	<p>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.</p> <p>Fortalecer el grado de uso y apropiación efectivo en temas tecnologías de la Información, Cultura en seguridad de la información.</p> <p>Prevenir fuga o pérdida de información.</p> <p>Lograr la apropiación de las Políticas en Seguridad y Privacidad de la información.</p>	<p>Comunicación efectiva y asertiva en el marco del desarrollo de las funciones.</p> <p>Fortalecimiento permanentemente frente al Sistema de Seguridad de la Información y las buenas prácticas en el uso de las tecnologías de información.</p> <p>Lograr la adopción de buenas prácticas que permitan garantizar la confidencialidad, disponibilidad e integridad de la información.</p> <p>Mitigar los riesgos por pérdida, o uso indebido de la información cumpliendo con la normatividad vigente.</p>
Entidades y Empresas	<p>Implementar Sistemas de Información, herramientas o servicios para el intercambio de información.</p> <p>Articulación interinstitucional mediante el establecimiento de acuerdos de cooperación.</p>	<p>Fomentar alianzas con Entidades y Empresas privadas comprometidas con la misionalidad de la entidad.</p> <p>Lograr la adopción de buenas prácticas que permitan garantizar la confidencialidad, disponibilidad e integridad de la información.</p> <p>Mitigar los riesgos por pérdida, o uso indebido de la información cumpliendo con la normatividad vigente.</p>
Ciudadanía, comunidad en general	<p>Fortalecer la seguridad en la información suministrada a la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES</p> <p>Garantizar la protección de los datos personales de la comunidad en general conforme al procesamiento de información dentro de las diferentes líneas misionales.</p>	<p>Cumplir tanto la Política General como Políticas Específicas de Seguridad de la Información reduciendo las probabilidades de afectación a la información.</p>
Gobierno	<p>Generar informes de los incidentes de seguridad presentados al Interior de la Entidad o externos que afecten la operación de esta.</p> <p>Brindar información acerca de la ejecución de la Política de Gobierno Digital.</p> <p>Compartir los Incidentes de Seguridad de la Información detectado por los</p>	<p>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.</p> <p>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.</p>

PROCESO	ARQUITECTURA Y PROYECYOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-MA01
		Versión:	04
MANUAL	Políticas Específicas de Seguridad y Privacidad de la Información	Fecha:	12/12/2022

PARTE INTERESADA	NECESIDADES	EXPECTATIVAS
	<p>diferentes grupos de respuesta a incidentes tanto a nivel Público como privado a los cuales la Entidad tenga acceso.</p> <p>Dar cumplimiento a los lineamientos, directrices que han sido establecidos para la implementación del Sistema de Gestión de Seguridad de la Información.</p>	<p>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.</p>
Proveedores	<p>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.</p>	<p>Conocer tanto la Política General como Políticas Específicas de Seguridad y Privacidad de la información de la Entidad.</p>