

La Sociedad de Activos Especiales SAE identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Entidad, razón por la cual es necesario que se establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada. Este documento describe las políticas y normas de seguridad de la información definidas por la Sociedad de

## Política de Seguridad y Privacidad de la Información Sociedad de Activos Especiales SAS

### Contenido

INTRODUCCIÓN.....	4
OBJETIVOS.....	5
ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - APLICABILIDAD .....	5
VIGENCIA Y ACTUALIZACIÓN DEL MANUAL .....	6
TÉRMINOS Y DEFINICIONES.....	6
SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	14
NIVEL DE CUMPLIMIENTO .....	14
CONDICIONES GENERALES .....	14
EXCLUSIONES.....	14
REFERENCIAS INFORMATIVAS Y LEGALES .....	15
POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....	16
POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN .....	17
1. POLÍTICA DE ORGANIZACIÓN INTERNA .....	17
2. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES .....	19
POLÍTICA PARA USO DE CONEXIONES REMOTAS .....	24
POLÍTICAS DE SEGURIDAD DEL RECURSO HUMANO .....	25
POLÍTICA RELACIONADA CON LA VINCULACIÓN DE FUNCIONARIOS .....	26
POLÍTICA APPLICABLE DURANTE LA EJECUCIÓN DEL EMPLEO Y PERSONAL PROVISTO POR TERCEROS .....	27
POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS .....	29
POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN .....	31
POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS .....	31
POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN .....	33
POLÍTICA DE USO Y MANEJO DE MEDIOS DE ALMACENAMIENTO.....	36
POLÍTICAS DE CONTROL DE ACCESO .....	38
POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED.....	38
POLÍTICA DE GESTIÓN DE ACCESO DE USUARIOS .....	39
POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS .....	42

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

---

POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS .....	43
POLITICA PARA USO DE TOKENS DE SEGURIDAD.....	46
POLÍTICAS DE CRIPTOGRAFIA .....	48
POLÍTICAS DE SEGURIDAD FISICA Y MEDIO AMBIENTAL .....	49
POLÍTICA DE AREAS SEGURAS.....	49
POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES .....	53
POLITICAS DE SEGURIDAD EN LAS OPERACIONES.....	56
POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS.....	56
POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO .....	58
POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN.....	59
POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN .....	61
POLITICA DE CONTROL AL SOFTWARE OPERATIVO .....	62
POLÍTICA DE GESTIÓN DE VULNERABILIDADES .....	63
POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES .....	64
POLÍTICA DE GESTION Y ASEGURAMIENTO DE LAS REDES DE DATOS.....	64
POLÍTICA DE USO DEL CORREO ELECTRONICO.....	65
POLÍTICA DE USO ADECUADO DE INTERNET .....	67
POLÍTICA DE INTERCAMBIO DE INFORMACIÓN .....	68
POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.....	71
POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD .....	71
POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS.....	72
POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA.....	75
POLÍTICAS QUE RIGEN DE LA RELACION CON TERCERAS PARTES.....	76
POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES .....	76
POLÍTICA DE GESTION DE LA PRESTACION DE SERVICIOS DE TERCERAS PARTES .....	77
POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD .....	78
POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD .....	78
POLÍTICAS DE INCLUSION DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.....	80

---

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

---

POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION.....	80
POLÍTICA DE REDUNDANCIA.....	81
POLÍTICAS DE CUMPLIMIENTO .....	82
POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES .....	82
POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES .....	83
CONTROL DE CAMBIOS.....	85
ELABORACIÓN Y APROBACIÓN DEL DOCUMENTO .....	85

## INTRODUCCIÓN

La Sociedad de Activos Especiales SAE identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Entidad, razón por la cual es necesario que se establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por la Sociedad de Activos Especiales SAE. Para la elaboración de este, se toman como base las buenas prácticas establecidas por la norma ISO/IEC 27001:2013 y las recomendaciones del estándar ISO/IEC 27002:2013, el Modelo de Seguridad y Privacidad de la Información, las guías y herramientas desarrolladas por el Ministerio de las Tecnologías y las comunicaciones MINTICs.

Las políticas incluidas en este manual se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información de la Sociedad de Activos Especiales SAE y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La Seguridad de la Información es una prioridad para la Entidad y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

### OBJETIVOS

- ✓ Buscar que los principios de disponibilidad, integridad y confidencialidad de la información se cumplan por parte de los funcionarios, proveedores, terceros y contratistas.
- ✓ Promover el uso de mejores prácticas de seguridad de la información y datos personales, para ser la base de aplicación del concepto de Seguridad Digital.
- ✓ Brindar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas
- ✓ Realizar la gestión de riesgos periódicamente para mantener los activos de información protegidos.
- ✓ Apoyar los lineamientos para dar cumplimiento con la normatividad legal vigente en temas a de seguridad de la información y datos personales
- ✓ Minimizar el riesgo de los procesos de la entidad.
- ✓ Mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.
- ✓ Incluir en la gestión de proyectos de la SAE, la seguridad y privacidad de la información, para asegurar que los riesgos se identifiquen y traten como parte del proyecto.
- ✓ Mantener la confianza de los funcionarios, proveedores, terceros y contratistas.
- ✓ Apoyar la innovación tecnológica.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, proveedores, terceros y contratistas y clientes de la SAE SAS.
- ✓ Contribuir en el desarrollo y ejecución del plan estratégico institucional.

### ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - APLICABILIDAD

Esta política aplica a toda la entidad, sus procesos, funcionarios, proveedores, contratistas y terceros de la SAE S.A.S y la ciudadanía en general sin excepción, que posean algún tipo de acceso o sean responsables por los activos de información, activos físicos, infraestructura física y recurso humano de la Sociedad de Activos Especiales SAE, que se encuentre disponible en cualquier formato ya sea de manera digital, impresa, en medio audiovisual o archivados de la Entidad.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Seguridad Digital, enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la SAE S.A.S, así como la protección de la información digital, medios impresos y físicos digitales y no digitales.

### VIGENCIA Y ACTUALIZACIÓN DEL MANUAL

Las Políticas contenidas en el presente documento estarán vigentes desde la fecha de su aprobación y mientras no exista una revisión posterior de las mismas.

La actualización y mantenimiento del Manual de Seguridad y Privacidad de la Información es responsabilidad del Oficial de Seguridad de la Información con la debida aprobación del Comité Directivo, se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

En las revisiones periódicas se deben tener en cuenta factores como: incidentes de seguridad, nuevas vulnerabilidades detectadas, cambios dentro de la infraestructura organizacional o tecnológica, cambios en los procesos, en los objetivos del sistema o de la organización, nuevas exigencias normativas en temas de seguridad digital, entre otros.

La versión oficial de este documento para funcionarios, proveedores, terceros y contratistas será la que se encuentre publicada y aprobada en la intranet de la SAE SAS.

### TÉRMINOS Y DEFINICIONES

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

Termino	Definición
<b>Acceso a la Información Pública</b>	Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
<b>Activo</b>	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
<b>Activo de Información</b>	En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
<b>Archivo</b>	Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
<b>Amenazas</b>	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
<b>Ánalisis de Riesgo</b>	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

<b>Auditoría</b>	Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
<b>Autorización</b>	Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
<b>Bases de Datos Personales:</b>	Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
<b>Ciberseguridad</b>	Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernetica. (CONPES 3701).
<b>Ciberespacio</b>	Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
<b>Confidencialidad</b>	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados (ISO/IEC 27000).
<b>Control</b>	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

<b>Datos Abiertos</b>	Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
<b>Datos Personales</b>	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
<b>Datos Personales Públicos</b>	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
<b>Datos Personales Privados</b>	Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
<b>Datos Personales Mixtos</b>	Para efectos de esta política es la información que contiene datos personales públicos junto con datos privados o sensibles.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

<b>Datos Personales Sensibles</b>	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
<b>Declaración de aplicabilidad</b>	Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
<b>Derecho a la Intimidad</b>	Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
<b>Disponibilidad</b>	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 27000).
<b>Encargado del Tratamiento de Datos</b>	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
<b>Gestión de incidentes de seguridad de la información</b>	Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

<b>Incidente de seguridad de la información</b>	Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
<b>Información Pública Clasificada</b>	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
<b>Información Pública Reservada</b>	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
<b>Integridad</b>	Propiedad de la información relativa a su exactitud y completitud. (ISO/IEC 27000).
<b>Ley de Habeas Data</b>	Se refiere a la Ley Estatutaria 1266 de 2008.
<b>Ley de Transparencia y Acceso a la Información Pública</b>	Se refiere a la Ley Estatutaria 1712 de 2014.
<b>Mecanismos de protección de datos personales</b>	Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

<b>MSPI</b>	El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.(GobiernoDigital.mintic.gov.co).
<b>Partes interesadas (Stakeholder)</b>	Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
<b>Plan de continuidad del negocio</b>	Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
<b>Plan de tratamiento de riesgos</b>	Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
<b>Privacidad</b>	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 la correlativa obligación de proteger dicha información en observancia del marco legal vigente
<b>Registro Nacional de Bases de Datos</b>	Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

<b>Responsabilidad Demostrada</b>	Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
<b>Responsable del Tratamiento de Datos</b>	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
<b>Riesgo</b>	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
<b>Seguridad de la información</b>	Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
<b>Sistema de Gestión de Seguridad de la Información SGSI</b>	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
<b>Titulares de la información</b>	Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
<b>Tratamiento de Datos Personales</b>	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

<b>Trazabilidad</b>	Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
<b>Vulnerabilidad</b>	Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

## SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad y Privacidad de la Información pretenden instituir y afianzar la cultura de seguridad y privacidad de la información entre los funcionarios directos o a través de servicios temporales, contratistas, personal externo y proveedores de la SAE. Por tal razón, es necesario que las violaciones a las Políticas de Seguridad de la Información y Datos Personales sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

## NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la SAE SAS, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

## CONDICIONES GENERALES

### EXCLUSIONES.

- No se excluye ningún numeral de la norma ISO/IEC 27001:2013.
- Las exclusiones a los controles se encuentran definidos en la Declaración de Aplicabilidad (SOA).

### REFERENCIAS INFORMATIVAS Y LEGALES.

- Norma ISO/IEC 27001:2013: Requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Norma ISO/IEC 27002:2013: Código de Prácticas para la Gestión de la Seguridad de la Información.
- Norma ISO/IEC 27005:2011: Gestión de Riesgo de Seguridad de la Información.
- Normatividad vigente relacionada con la Seguridad Digital en Colombia
- Circular Externa 002 de 2015 – Superintendencia de Industria y Comercio
- Conpes 3995 Política Nacional de Confianza y Seguridad Digital
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- Circular Externa 005 de 2017 - Superintendencia de Industria y Comercio
- Ley 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales
- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Resolución 1126 de 2016 – SAE SAS Por medio de la cual se adopta el orientador estratégico de Manual de Tratamiento de Datos Personales de la Sociedad de Activos Especiales S.A.
- Resolución 579 de 2017 – SAE SAS Por medio de la cual se modifica el artículo cuatro de la resolución 1126 de 2016
- Modelo de seguridad y privacidad de la información del Ministerio de las Tecnologías y las Comunicaciones
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Guías del Modelo de Seguridad y Privacidad de la Información (MSPI) del Mintic
- Sistema de Gestión de Continuidad del Negocio (SGCN) norma ISO 22301
- 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.
- Resolución 113 mayo 27 de 2015 Por medio de la cual se adopta el orientador estratégico de

### Seguridad de la Información de la SAE SAS

- Resolución 027 de 2015 por medio de la cual se adopta el Comité Directivo de la Sociedad de Activos Especiales SAS y se reglamenta su funcionamiento.
- Resolución 137 de 2015 por medio de la cual se conforma el Comité del Sistema Integrado de Gestión y se asignan roles y responsabilidades y se designa representante de la alta dirección para el Sistema Integrado de Gestión de la Sociedad de Activos Especiales SAS
- Resolución 601 de 2019 por medio de la cual se adicionan unas funciones al Comité Directivo de la Sociedad de Activos Especiales SAS.
- Resolución número 00500 de marzo 10 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”

## POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las presentes Políticas de Seguridad de la Información, se originan como una herramienta para sensibilizar y concientizar a cada uno de los directivos, funcionarios, contratistas y terceros que prestan sus servicios a la SAE SAS, en la importancia de la información y los procesos críticos, permitiendo desarrollar sus funciones para cumplir con el plan estratégico de la entidad.

## PRINCIPIOS DE SEGURIDAD

A continuación, se establecen los 12 principios de seguridad que soportan el MSPI de SAE S.A.S:

- a. SAE S.A.S ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- b. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, proveedores y terceros.
- c. SAE S.A.S protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.
- d. SAE S.A.S protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- e. SAE S.A.S protegerá su información de las amenazas originadas por parte del personal.
- f. SAE S.A.S protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- g. SAE S.A.S controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- h. SAE S.A.S implementará control de acceso a la información, sistemas y recursos de red.

- i. SAE S.A.S garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- j. SAE S.A.S garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- k. SAE S.A.S garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- l. SAE S.A.S garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

## POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política tiene por objetivo establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la SAE.

### 1. POLÍTICA DE ORGANIZACIÓN INTERNA

La SAE establece un esquema de seguridad y privacidad de la información en donde existen roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información y datos personales.

La seguridad y privacidad de la información es una responsabilidad de la Sociedad de Activos Especiales SAE compartida por todos Presidencia, Vicepresidentes, Gerentes, Jefes de Oficina, Gerentes Regionales, por lo cual se establece el Comité Directivo, el cual es integrado por representantes de todos los Directivos mencionados, destinado a garantizar el apoyo manifiesto al sistema integrado de gestión y a las iniciativas e implementación de la seguridad y privacidad de la información.

Este Comité tiene entre sus funciones:

- Revisar y proponer a la Alta Dirección, para su aprobación, la Política y las funciones generales en materia de seguridad y privacidad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad y privacidad.
- Aprobar las principales iniciativas para incrementar la seguridad y privacidad de la información, de acuerdo con las competencias y responsabilidades asignadas.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad y privacidad de la información.
- Garantizar que la seguridad y privacidad sea parte del proceso de planificación de la información.

- Evaluar y coordinar la implementación de controles específicos de seguridad y privacidad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad y privacidad de la información dentro de las instalaciones de la Sociedad.
- Coordinar el proceso de administración de la continuidad de la operación de los sistemas de tratamiento de la información de la Sociedad frente a interrupciones imprevistas.
- Revisar el Sistema de Seguridad de la Información a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.
- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la Entidad,
- Comunicar en la Entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año).

### Normas que rigen la organización interna

Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para la SAE, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad y privacidad de la información.

Normas dirigidas a: COMITÉ DIRECTIVO

- Debe definir y establecer los roles y responsabilidades relacionados con la seguridad y privacidad de la información en niveles directivo y operativo.
- Debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- Debe asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad y privacidad de la información de la Sociedad.
- Aprobar y monitorear el programa integral de gestión de datos personales.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- Incluir la seguridad y privacidad de la información en la gestión de proyectos.
- Mantener los contactos apropiados con las autoridades pertinentes.
- Mantener los contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
- Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Revisar los diagnósticos del estado de la seguridad de la información
- Poner en conocimiento de la entidad, los documentos generados al interior del comité relacionados con Seguridad de la Información que impacten de manera transversal a la misma.

### Normas dirigidas a: OFICINA DE CONTROL INTERNO

- Debe validar y monitorear de manera periódica la implantación de los controles de seguridad y privacidad de la información establecidos.
- Recomendará y acompañará a la Oficina de gestión de la Información, en la generación de lineamientos para gestionar la seguridad de la información de la SAE y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- Debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la Sociedad. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

## 2. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

Esta política tiene por objetivo garantizar la seguridad del trabajo realizado por conexiones remotas y el uso de dispositivos móviles.

La SAE provee las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales que hagan uso de servicios de la Sociedad. Así mismo, velará porque los funcionarios hagan un uso responsable de estos, con el objetivo de mitigar los riesgos.

### Normas para uso de dispositivos móviles

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- Establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la SAE.
- Investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la Sociedad.
- Establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz, multifactor) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- Activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- Contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de SAE; dichas copias deben acogerse al Procedimiento de Copias de Respaldo de la Información.
- Instalar un software de antivirus en los dispositivos móviles institucionales.
- Asignar permisos de acceso a Wifi por la red de visitantes a dispositivos móviles cuando sean autorizados por los jefes de área.
- Asignar permisos de acceso a Wifi por la red de ciudadanos a través de PIN, administrado desde la Oficina de Atención al Ciudadano y en la Regionales quien haga sus veces.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La SAE proveerá dispositivos móviles (teléfonos móviles, tabletas, computadores portátiles), siempre que las condiciones del cargo y la función lo permitan y, en todos los casos, sujeto a disponibilidad presupuestal. Del mismo modo proporcionará las condiciones para el manejo de los dispositivos móviles institucionales y personales, velando porque los servidores hagan un uso responsable de los servicios y equipos facilitados por la entidad.
- La sociedad no asumirá los costos que por cualquier concepto se deriven de la utilización de dispositivos móviles personales para fines laborales, pero podrá autorizar su uso.
- Suspender, bloquear y retirar, los dispositivos móviles institucionales que no sean utilizados durante un lapso de tiempo considerable.
- Activar los códigos o números de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.
- Mantener un inventario actualizado con la identificación de los dispositivos móviles que estén utilizando los trabajadores para fines laborales.

### Normas dirigidas a: TODOS LOS USUARIOS

- Evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- No modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega, ni modificar los elementos de imagen institucional.
- Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, deben aceptar y aplicar la nueva versión.
- Evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- No deben almacenar música, videos, fotografías o información personal en los dispositivos móviles institucionales asignados.
- Si por necesidad del servicio requieren utilizar el dispositivo móvil personal, el jefe de área deberá informar a la Oficina de Gestión de la Información a través de la mesa de ayuda, para adoptar las medidas de seguridad correspondientes.
- Instalar un software de antivirus en los dispositivos móviles institucionales y en los personales solicitar al usuario que lo implemente cuando hagan uso de los servicios provistos por la SAE.
- Toda información alojada en dispositivos móviles corporativos, almacenada por razón o con ocasión del ejercicio de funciones, deberá administrarse (incluye la transferencia, el almacenamiento en la nube y su encripción bien se trate de datos en tránsito o en reposo) de acuerdo con la política de manejo de datos adoptada por la SAE.
- En general, adoptar conductas orientadas a minimizar los riesgos asociados al uso de dispositivos móviles.
- Se encuentra prohibida la grabación ya sea en audio y/o video, de las reuniones o sesiones realizadas con ocasión del ejercicio de las funciones de los trabajadores y el giro ordinario de los negocios de SAE, donde se traten temas e información confidencial y que no sean de conocimiento público. La clasificación de dicha información la realizará cada líder de proceso y/o responsable de la reunión o sesión antes de iniciar, dando la autorización de grabación, de lo contrario todo lo tratado en reuniones o juntas será de carácter confidencial; y no será posible su grabación.
- En caso de robo o pérdida del dispositivo corporativo deberá colocarse la denuncia respectiva y darse aviso inmediato a la OGI para que se implementen las acciones necesarias tendientes a recuperar y asegurar la información que guarde relación con SAE. Esto sin perjuicio de las acciones que se deban iniciar en caso de indebida utilización o custodia y de la reposición por parte del trabajador.
- Las citaciones a reuniones masivas deben realizarse a través de Comunicaciones y Gerencia de Talento Humano por los canales definidos para tal fin.

### Normas dirigidas a: Trabajadores de planta o en misión usuarios de dispositivos personales

Los usuarios trabajadores de planta o en misión, que dispongan de sus dispositivos personales para el ejercicio de su actividad laboral en SAE, deberán:

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- Autorizar el uso del dispositivo para fines laborales, mediante comunicación escrita que deberá reposar en su historia laboral en donde además se indiquen los datos de identificación de este y sus características técnicas.
- Toda información institucional alojada en dispositivos móviles personales, almacenada por razón o con ocasión del ejercicio de funciones, deberá administrarse (incluye la transferencia, el almacenamiento en la nube y su encripción bien se trate de datos en tránsito o en reposo) de acuerdo con la política de manejo de datos adoptada por la SAE.
- La información alojada en dispositivos móviles personales almacenada por razón o con ocasión del ejercicio de funciones se encuentra calificada como confidencial y por lo tanto revestida de reserva, en consecuencia, el trabajador deberá velar por su correcta salvaguarda y será responsable por su custodia y el uso que a ésta se le dé.
- Implementar un software de antivirus en los dispositivos móviles cuando hagan uso de los servicios provistos por la SAE.
- De manera general, la información relacionada con la gestión laboral no podrá de ningún modo permanecer almacenada en un dispositivo móvil personal más allá del tiempo estrictamente requerido para hacer su correcta transferencia o a los archivos que SAE tenga dispuestos para el efecto.
- De ser necesario cuando la información institucional se vea expuesta podrá ser borrada del dispositivo personal de manera remota.

### USO DEL WHATSAPP Y OTRAS APLICACIONES

- El uso de aplicaciones como WhatsApp en dispositivos institucionales, se encuentra autorizado para fines relacionados a la labor, en todo caso, no se permite por esta aplicación, el envío de fotografías, audios y videos y cualquier otro tipo de archivos clasificados como información pública reservada o información pública clasificada.
- No podrán utilizarse a través de WhatsApp o en redes sociales en general, cuya aplicación se encuentre instalada en dispositivos institucionales, expresiones injuriosas, discriminatorias o que atenten contra la dignidad de las personas, como tampoco efectuar manifestaciones personales que puedan comprometer a la empresa.
- Salvo casos de urgencia manifiesta, o cuando el trabajador se encuentre en comisión, podrá hacerse uso de la aplicación para el envío de mensajes en horario diferente al laboral, fines de semana o festivos.

### Grupos de WhatsApp

- Se podrán conformar grupos en whatsapp en los dispositivos corporativos o en los personales, con fines laborales, en todo caso corresponderá al trabajador aceptar o no, ser parte de estos.

### Acciones Disciplinarias

- Además del retiro del dispositivo por su uso indebido, la Sociedad de Activos Especiales podrá iniciar las acciones disciplinarias y las que de ésta se deriven, cuando se presente incumplimiento por parte del trabajador, a lo previsto en esta política.

### Ingreso de dispositivos terminales móviles por parte de terceras personas, funcionarios públicos de otras entidades y/o visitantes en general.

- Por regla general los visitantes no podrán ingresar a las instalaciones de la sociedad, equipos terminales móviles, en casos excepcionales se autorizará su ingreso por parte del Profesional Coordinador del Grupo Interno de Trabajo de Servicios Administrativos, previa justificación dada por el jefe de la Dependencia a donde se dirige la persona o grupo de personas y bajo su responsabilidad, de ello deberá dejarse constancia en el registro que lleva la vigilancia.
- La recepción y guarda de los dispositivos móviles, es responsabilidad de la empresa de seguridad y vigilancia, que deberá implementar los controles requeridos tendientes a garantizar la debida custodia en tanto las personas permanezcan en las instalaciones.

### POLITICA PARA USO DE CONEXIONES REMOTAS

La SAE instaurará las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Sociedad; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

#### Normas para uso de conexiones remotas

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- Debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la SAE.
- Debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado previa autorización de los

jefes de oficina y por períodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

- Debe monitorear las conexiones remotas a los recursos de la plataforma tecnológica de la SAE de manera permanente.
- Debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica, a través de herramientas o aplicaciones adquiridas por la SAE.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la SAE y deben acatar las condiciones de uso establecidas para dichas conexiones.
- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.
- Los usuarios deberán solicitar acceso por conexión remota a través de los jefes de área y por el canal de servicios que disponga la Oficina de Gestión de la Información.
- Las conexiones remotas serán controladas y monitoreadas a través de las herramientas de seguridad con las cuales cuenta la entidad.
- Es responsabilidad en todo momento tener el control de acceso al computador desde donde se realiza la conexión remota.
- La información institucional deberá siempre estar almacenada dentro del entorno de conexión remota.
- Los computadores portátiles asignados por la SAE tendrán las herramientas de seguridad necesarias para proteger el acceso por conexión remota.
- Las conexiones estarán disponibles en el horario de trabajo definido por la SAE.

### POLÍTICAS DE SEGURIDAD DEL RECURSO HUMANO

Esta política tiene por objetivo asegurar que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

### POLÍTICA RELACIONADA CON LA VINCULACIÓN DE FUNCIONARIOS

La SAE reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos estratégicos y con el interés de contar con personal calificado, garantizará que la vinculación de nuevos funcionarios se realice siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos. Asegurando que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles a desempeñar.

#### Normas relacionadas con la selección y vinculación de Funcionarios

Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA - GERENCIA DE TALENTO HUMANO

- La GERENCIA DE TALENTO HUMANO debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por todos los candidatos a ocupar un cargo en SAE, antes de su vinculación definitiva, de acuerdo con la leyes, reglamentaciones y ética pertinentes. Deberán ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener a acceso y a los riesgos percibidos.
- La GERENCIA DE TALENTO HUMANO debe garantizar que los funcionarios de la Sociedad firmen un Acuerdo y/o Cláusula de Confidencialidad, Autorización de datos personales y Aceptación de Políticas de Seguridad y Privacidad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.
- La GERENCIA DE TALENTO HUMANO debe garantizar que todos los funcionarios de la SAE y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en SAE recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos relacionados a la seguridad y privacidad de la información de SAE.
- La GERENCIA DE TALENTO HUMANO debe garantizar que cuando un trabajo ya sea por nombramiento o promoción, implique que el colaborador tenga acceso a las instalaciones de procesamiento de información y en si en particular maneja información confidencial, se realicen verificaciones adicionales más detalladas.

Normas dirigidas a: SUPERVISORES DE CONTRATO, VICEPRESIDENTES, GERENTES Y JEFES DE OFICINA

- Cada Supervisor de Contrato, vicepresidente, Gerente y jefe de Oficina debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad, Autorización de datos personales

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

y de la documentación de Aceptación de Políticas para los Funcionarios provistos por terceras partes, antes de otorgar acceso a la información de la SAE.

- Cada Supervisor de Contrato, vicepresidente, Gerente y jefe de Oficina debe garantizar que los terceros y proveedores de la Sociedad firmen un Acuerdo y/o Cláusula de Confidencialidad, Autorización de datos personales y Aceptación de Políticas de Seguridad de la Información dentro de las obligaciones del contrato.

### Normas dirigidas a: FUNCIONARIOS PROVISTOS POR TERCERAS PARTES

- Los Funcionarios provistos por terceras partes que realicen labores en o para la SAE, deben firmar un Acuerdo y/o Cláusula de Confidencialidad, Autorización de Datos Personales y un documento de Aceptación de Políticas de Seguridad y Privacidad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.
- Los Funcionarios provistos por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad, autorización de datos personales y aceptación de las Políticas de Seguridad y Privacidad de la Información de la Sociedad.

### POLÍTICA APLICABLE DURANTE LA EJECUCIÓN DEL EMPLEO Y PERSONAL PROVISTO POR TERCEROS

La SAE en su interés por proteger su información y los recursos de procesamiento de la misma garantizará el compromiso del Comité Directivo en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad y privacidad de la información en búsqueda de la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad y privacidad de la información de la Entidad, igualmente se garantizará la imposición inmediata de sanciones disciplinarias cuando se incumplan las políticas de seguridad de la información.

Normas aplicables durante la ejecución del empleo y personal provisto por terceros

### Normas dirigidas a: COMITÉ DIRECTIVO

- El Comité Directivo debe demostrar su compromiso con la seguridad y privacidad de la información por medio de la creación y aprobación de las políticas, normas y demás lineamientos que deseé establecer la entidad.
- El Comité Directivo debe promover la importancia de la seguridad y privacidad de la información entre los funcionarios de la SAE y el personal provisto por terceras partes, así

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.

- El Comité Directivo debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente de la Sociedad, el tratamiento de las faltas de cumplimiento a las políticas de seguridad y privacidad de la información o los incidentes de seguridad que lo ameriten.

### Normas dirigidas a: OFICINA DE COMUNICACIONES

- La OFICINA DE COMUNICACIONES debe apoyar en el diseño y ejecución de manera permanente de un programa de concienciación en seguridad y privacidad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

### Normas dirigidas a: GERENCIA DE TALENTO HUMANO

- La GERENCIA DE TALENTO HUMANO debe incluir dentro del programa de capacitación de la SAE a los funcionarios de la SAE en el programa de concientización en seguridad y privacidad de la información para evitar posibles riesgos de seguridad.
- La GERENCIA DE TALENTO HUMANO debe aplicar el proceso disciplinario de la Sociedad cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad y privacidad de la información.
- La GERENCIA DE TALENTO HUMANO y quien ejecute las funciones de Oficial de Seguridad de la Información deberán garantizar que exista un canal de comunicación para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad y privacidad de la información (“denuncias internas”) [oficialseguridad@saesas.gov.co](mailto:oficialseguridad@saesas.gov.co)
- La GERENCIA DE TALENTO HUMANO debe entregar los resultados obtenidos en el programa de capacitación con respecto a los temas de Seguridad y Privacidad de la Información.

### Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA - GERENCIA DE TALENTO HUMANO

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- EL GERENCIA DE TALENTO HUMANO debe convocar a los funcionarios a las charlas y eventos programados como parte del programa de concientización en seguridad y privacidad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada. Al finalizar la formación se debe evaluar la comprensión de los funcionarios, personal provisto por terceras partes y contratistas para comprobar la transferencia de conocimiento.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes, que por sus funciones hagan uso de la información de la SAE, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad y privacidad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.
- Los funcionarios y personal provisto por terceras partes deben asistir o realizar las capacitaciones programadas por la Gerencia de Talento Humano.
- Los funcionarios deben hacer una lectura a conciencia del material publicado en la Plataforma Virtual y en especial deben interiorizar y aplicar los conceptos relacionados con la Seguridad y Privacidad de la Información.
- Los funcionarios deben tomar conciencia de la seguridad y privacidad de la información en todo momento durante la vinculación laboral y deberán consultar las políticas, procedimientos, instructivos y formatos publicados en la intranet de la SAE.

### POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

La SAE asegurará que sus funcionarios y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura, con el objetivo de proteger los intereses de la SAE como parte del proceso de cambio o terminación de empleo.

Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros

Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA - GERENCIA DE TALENTO HUMANO

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- LA GERENCIA DE TALENTO HUMANO debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la Sociedad, llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.
- La GERENCIA DE TALENTO HUMANO debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a La Oficina de Gestión de la Información a través de los canales definidos en los procedimientos.
- LA GERENCIA DE TALENTO HUMANO debe reportar oportunamente a la OFICINA DE GESTIÓN DE LA INFORMACIÓN la desvinculación de funcionarios de planta, practicantes, temporales.
- La GERENCIA DE TALENTO HUMANO debe comunicar a los funcionarios las responsabilidades y deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo.

Normas dirigidas a: SUPERVISORES DE CONTRATO, VICEPRESIDENTES, GERENTES Y JEFES DE OFICINA

- Cada Supervisor de Contrato, vicepresidente, Gerente y jefe de Oficina debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a la OFICINA DE GESTIÓN DE LA INFORMACIÓN asegurando que los requerimientos o labores pendientes sean trasladadas al competente para así continuar con el respectivo trámite de información.

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La OFICINA DE CONTROL DE LA INFORMACIÓN garantizará la gestión de usuarios en la plataforma tecnológica, de acuerdo con la solicitud de la Gerencia de Talento Humano. Así mismo garantizará la inactivación temporal o definitiva de las claves de acceso a los diferentes aplicativos y/o sistemas de información.
- La OFICINA DE CONTROL DE LA INFORMACIÓN deberá inactivar el acceso a los usuarios durante el periodo de vacaciones desde el dominio y en las licencias o incapacidades superiores a cinco días

Normas dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de los funcionarios en vacaciones hacer entrega de las actividades a su cargo de acuerdo con el procedimiento de la Gerencia de Talento Humano y configurar

---

mensaje en el correo para dicho periodo indicando a quien deben dirigir las comunicaciones.

### POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

Esta política tiene por objetivo identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

### POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

La SAE como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

Normas de responsabilidad por los activos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Las Vicepresidencias, Gerencias y Jefes de Oficinas, de la SAE, deben actuar como propietarias de la información física y electrónica, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Los recursos de procesamiento de información de la SAE se encuentran sujetos a auditorías por parte de la Oficina de Control Interno, y de los entes externos de supervisión, por lo que, los propietarios de los activos de información deberán ser facilitadores de estas.
- Los propietarios de los activos de información deberán incluir y mantener un inventario de estos activos de acuerdo con el P-TE4-158 Procedimiento Gestión y Clasificación de activos de información.
- Los propietarios de los activos de información deben asegurarse de que los activos están clasificados y protegidos apropiadamente.
- Los propietarios de los activos de información deben asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

- Los propietarios de los activos de información no necesariamente tienen algún derecho de propiedad sobre el activo.

Normas dirigidas a: VICEPRESIDENCIA ADMNISTRATIVA.

- La Vicepresidencia Administrativa y Financiera debe garantizar el levantamiento y actualización del inventario de los documentos físicos, teniendo en cuenta las diferentes localizaciones del archivo a través del Grupo Interno de Archivo y Correspondencia.

Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN

- La Oficina de Gestión de la Información es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la SAE y, en consecuencia, debe asegurar su apropiada operación y administración.
- La Oficina de Gestión de la Información debe garantizar el levantamiento y actualización del inventario de activos de información tecnológicos, teniendo en cuenta los diferentes recursos tecnológicos y los sistemas de información contenidos en ellos, incluyendo los niveles de clasificación de acuerdo con la Ley de Transparencia.
- La Oficina de Gestión de la Información debe autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la SAE.
- La Oficina de Gestión de la Información debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad y privacidad de la información y hacer un uso adecuado de ellos.
- La Oficina de Gestión de la Información es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de autorizar su uso.
- La Oficina de Gestión de la Información es responsable de recibir las estaciones de trabajo fijas y/o portátiles para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores.
- La Oficina de Gestión de la Información debe realizar un análisis de riesgos de seguridad y privacidad de la información de manera periódica, sobre los procesos de la SAE.
- La Oficina de Gestión de la Información debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

### Normas dirigidas a: OFICINA DE CONTROL INTERNO

- La OFICINA DE CONTROL INTERNO debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la Sociedad.

### Normas dirigidas a: VICEPRESIDENTES, GERENTES Y JEFES DE OFICINA

- Los vicepresidentes, Gerentes y Jefes de Oficina, o quien ellos designen, deben garantizar que los recursos tecnológicos asignados a sus funcionarios sean devueltos a la Oficina de Gestión de la Información, cuando estos se retiran de la Sociedad o son trasladados de área.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los recursos tecnológicos de la SAE deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Sociedad.
- Los recursos tecnológicos de la SAE provistos a funcionarios y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores de la Sociedad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la SAE.
- Los funcionarios no deben almacenar información de la Sociedad en los dispositivos móviles y computadores personales.
- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de propiedad de SAE son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al Vicepresidente, Gerente o Jefe de Oficina o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

### POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

La SAE definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

---

Una vez clasificada la información, la SAE proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios de la Sociedad y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

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

De igual manera se deben implementar un conjunto de procedimientos para el etiquetado de la información de acuerdo con su clasificación.

### Normas para la clasificación y manejo de la información

Con el fin de asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

#### Normas dirigidas a: COMITÉ DIRECTIVO

- El Comité Directivo debe aprobar los niveles de clasificación de la información propuestos por el (la) Oficial de Seguridad de la Información en el Procedimiento Gestión y Clasificación de activos de información y este debe estar alineado a lo requerido por la Ley de Transparencia.

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe monitorear con una periodicidad establecida la aplicación de la guía de clasificación de la Información.
- La Oficina de Gestión de la Información debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.
- La Oficina de Gestión de la Información debe garantizar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son datos de baja o cambian de usuario.
- La Oficina de Gestión de la Información debe implantar otros mecanismos de control necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información que se encuentra en los recursos tecnológicos bajo su custodia.

Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA – GRUPO DE ARCHIVO

- El grupo de Archivo debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.
- El grupo de Archivo debe garantizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.
- El grupo de Archivo debe verificar el cumplimiento de los Acuerdos de Niveles de Servicio y Acuerdos de intercambio con el proveedor de custodia externo de los documentos físicos de la Sociedad.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Para los efectos de esta política se entiende como propietario un área de la entidad, o grupo de trabajo que tiene la responsabilidad delegada sobre la gestión de controlar todo el ciclo de vida de un activo. El propietario identificado no necesariamente tiene algún derecho de propiedad sobre el activo.

El propietario debe definir quiénes tienen acceso y qué pueden hacer con la información, así como de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y, a la vez, de definir qué se hace con la información una vez ya no sea requerida.

- Los propietarios de los activos de información deben clasificar su información de acuerdo con la guía de clasificación de la Información establecida.
- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios deben cumplir con el P-TE4-158 Procedimiento Gestión y Clasificación de activos de información y los lineamientos de la guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la SAE.
- La información física y digital de la SAE debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

- No está permitido dejar abandonada en las impresoras información que tenga el carácter público, público clasificado y público reservado, una vez se haya impreso algún documento la persona responsable, deberá realizar la recepción del mismo de manera inmediata para evitar que los documentos confidenciales sean divulgados de manera no autorizada.
- Los escritorios o puestos de trabajo de los funcionarios de la Sociedad de Activos Especiales SAS. deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio, esto para evitar el acceso no autorizado a la información, en igual sentido, se deben mantener las pantallas de los computadores asignados para desarrollar sus funciones en una posición en la que se evite que personal no autorizado pueda ver la información que se encuentre desplegada en ellas.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.
- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario, cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados. Se realizará un bloqueo automático después que registre una inactividad de más de 5 minutos, con el fin de proteger la información asignada.
- Todos los usuarios son responsables de los accesos a los sistemas de información y a la red corporativa, por ninguna razón se deben entregar las claves de acceso. Si por necesidad del servicio, se requiere acceder a su computador, deberán informar a través de la mesa de ayuda, con el fin de tomar las medidas de control correspondientes.

## POLÍTICA DE USO Y MANEJO DE MEDIOS DE ALMACENAMIENTO

Esta política tiene por objetivo evitar la divulgación, modificación, el retiro o la destrucción no autorizada de información almacenada en los medios.

Normas uso y manejo de medios de almacenamiento

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe establecer las condiciones de uso de medios de almacenamiento en la plataforma tecnológica de la SAE.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Oficina de Gestión de la Información debe implantar los controles que regulen el uso de medios removibles y de almacenamiento en la plataforma tecnológica de la Sociedad, de acuerdo con la clasificación de activos de información adoptada por la SAE.
- La Oficina de Gestión de la Información debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la Sociedad, ya sea cuando son dados de baja o reasignados a un nuevo usuario.
- La Oficina de Gestión de la Información debe autorizar el uso de medios removibles o medios de almacenamiento en la plataforma tecnológica de la Sociedad de acuerdo con el perfil del cargo del funcionario solicitante, previa aprobación del jefe de área.
- La Oficina de Gestión de la Información debe proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte de los medios que contienen información.
- La Oficina de Gestión de la Información a través de la herramienta de control para medios removibles documenta la autorización.
- La Oficina de Gestión de la Información deberá contar con un proveedor para la recolección, disposición y custodia de medios.
- La Oficina de Gestión de la Información deberá proteger los medios que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de medios de almacenamiento establecidos por La Oficina de Gestión de la Información.
- Los funcionarios de la SAE y el personal provisto por terceras partes no deben modificar la configuración de las herramientas que controlan el uso de medios de almacenamiento establecidos por La Oficina de Gestión de la Información.
- Los funcionarios y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados y en caso de pérdida deberá informar al Oficial de Seguridad de la Información y/o a La Oficina de Gestión de la Información.
- Los funcionarios, contratistas y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la SAE. Si por necesidad del

servicio lo requiere, deberá registrarla al ingreso a la Sociedad y notificar al responsable por parte de la SAE de su visita.

### **POLÍTICAS DE CONTROL DE ACCESO**

Esta política tiene por objetivo limitar el acceso a información y a instalaciones de procesamiento de información.

#### **POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED**

La Oficina de Gestión de la Información de la SAE, como responsable de las redes de datos y los recursos de red de la Sociedad, debe garantizar que dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

De igual manera, debe permitir el acceso de los usuarios de la red y a los servicios de red para los que haya sido autorizados específicamente

#### Normas de acceso a redes y recursos de red

##### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la SAE.
- La Oficina de Gestión de la Información debe asegurar que las redes inalámbricas de la Sociedad cuenten con métodos de autenticación fuerte para su acceso.
- La Oficina de Gestión de la Información, debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la SAE, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.
- La Oficina de Gestión de la Información, debe restringir y controlar la asignación y uso de derechos de acceso de uso privilegiado.
- Los derechos de acceso de uso privilegiado se deben asignar de acuerdo con la necesidad de su uso y de manera individual.

##### Normas dirigidas a: VICEPRESIDENTES, GERENTES Y JEFES DE OFICINA

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Gerencia de Talento Humano es la responsable de pedir la creación del usuario en el dominio y la asignación del computador o escritorio virtual si se requiere
- Los Vicepresidentes, Gerentes y Jefes de Oficina deben autorizar la creación o modificación de las cuentas de acceso a las redes, sistemas de información o recursos de red de la SAE.
- La Oficina de Control Interno debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de garantizar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
- Los propietarios de los activos de información deben determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para los roles de usuario específicos con relación a sus activos, con la cantidad de detalle y severidad de los controles.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la SAE, debe estar autorizado y firmar previamente el Acuerdo de Confidencialidad.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos y de la Sociedad deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- Los computadores que se conecten a la red de SAE deben tener instalado antivirus y aplicaciones licenciadas a excepción del software libre.
- Solamente se concede acceso a la información que la persona necesita para la realización de sus tareas, las cuales son asociadas a los roles y perfiles definidos por las áreas y los sistemas de información.

### POLÍTICA DE GESTIÓN DE ACCESO DE USUARIOS

Esta política tiene por objetivo asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

Normas de registro, acceso e inactivación de usuarios

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Oficina de Gestión de la Información debe establecer un procedimiento formal para la administración y control de acceso de los usuarios en la plataforma tecnológica.
- La Oficina de Gestión de la Información debe gestionar la identificación única que permita asociar a los usuarios con sus actividades y hacerlos responsables de sus acciones. El uso de identificaciones compartidas solo se debe permitir cuando sea necesario por razones operativas o del negocio, previa aprobación y documentación.
- La Oficina de Gestión de la Información debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la SAE; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
- La Oficina de Gestión de la Información debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
- La Oficina de Gestión de la Información debe garantizar que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.
- La Oficina de Gestión de la Información debe verificar periódicamente las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y sistemas de información.
- La Oficina de Gestión de la Información debe revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios, como mínimo tres veces al año.

### Normas de Gestión de derechos de acceso privilegiado

La Oficina de Gestión de la Información de la SAE velará porque los recursos de la plataforma tecnológica y los servicios de red de la Sociedad sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dicha plataforma y servicios.

### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.
- La Oficina de Gestión de la Información debe establecer cuentas de usuario personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.
- La Oficina de Gestión de la Información debe garantizar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.
- La Oficina de Gestión de la Información debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas y/o previa autorización del jefe de Área.
- La Oficina de Gestión de la Información debe garantizar que los usuarios o perfiles de usuario que traen por defecto el hardware y software sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- La Oficina de Gestión de la Información debe garantizar que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- La Oficina de Gestión de la Información debe garantizar que los usuarios de acceso privilegiado cumplan con las políticas de seguridad configuradas en el computador asignado, en caso de requerirse permisos específicos deberá solicitarlo a través del jefe de área y deberá quedar documentado.
- La Oficina de Gestión de la Información debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.
- El uso inapropiado de los privilegios del sistema de administración es un factor que contribuye a las fallas o violaciones de los sistemas.

- Las autorizaciones para los derechos de acceso privilegiado se deben revisar periódicamente para asegurar que no se hayan obtenido privilegios no autorizados

### Normas dirigidas a: OFICINA DE CONTROL INTERNO

La Oficina de Control Interno debe revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoria de la plataforma tecnológica y los sistemas de información.

### Normas de Gestión de información secreta para la autenticación de usuarios

La asignación de información de autenticación secreta es controlada desde los acuerdos de confidencialidad y reserva de la información.

Todos los usuarios deben mantener su propia información secreta para autenticación, para el caso de claves de acceso a aplicaciones por primera vez, la información secreta es temporal y se debe obligar al usuario cambiar la clave en su primer ingreso.

La información secreta para la autenticación por defecto, del fabricante, se debe modificar después de la instalación de los sistemas o software.

## POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

El objetivo de esta política es hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la SAE deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.
- A los funcionarios que les fuese asignada una cuenta y contraseña de otras entidades deberán cumplir con las políticas de SAE, así como las políticas de seguridad de la entidad que asigna dicha cuenta.
- Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la Sociedad deben acogerse a lineamientos para la configuración de cuentas de usuario y contraseñas implantados por la

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

Sociedad, con el fin de garantizar una gestión y administración adecuada de las cuentas de usuario y contraseñas.

- Los usuarios de los recursos tecnológicos y los sistemas de información de la SAE realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.
- El usuario tiene la responsabilidad de mantener la confidencialidad de la información secreta para autenticación, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad.
- No exponer la información secreta para la autenticación a menos que pueda almacenar en forma segura.
- El usuario tiene la responsabilidad de cambiar la información secreta para la autenticación siempre que haya cualquier indicio de que pueda comprometer la información.
- Cuando se usan contraseñas como información secreta para la autenticación, seleccione contraseñas de calidad con una longitud mínima suficiente, fácil de recordar, combinén letras números y caracteres especiales (ver P-TE4-094 Procedimiento Administración y Control de Acceso a usuarios en la plataforma tecnológica).
- No aceptar que los sistemas de información o portales a los que acceden recuerden contraseñas automáticamente.

### Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN

- Las autorizaciones para los derechos de acceso privilegiado se deben revisar a intervalos frecuentes.

## POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APlicativos

El objetivo de esta política es evitar el acceso no autorizado a sistemas y aplicaciones.

### Normas de control de acceso a sistemas y aplicativos

### Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos y la Política de Control de Acceso
- Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.
- Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares, después de cualquier cambio, ascenso, cambio a un cargo a un nivel inferior o terminación del empleo.

### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe establecer un procedimiento de autorización y controles entre los que se pueden mencionar: usuarios que tienen permiso de ingreso a cargue o actualización de datos dentro de los aplicativos, usuarios que tienen permiso para consulta de la información y a qué nivel, mínimos privilegios, restricciones de acceso únicamente a las funcionalidades y datos requeridos para proteger el acceso a los sistemas y aplicativos de la SAE.
- La Oficina de Gestión de la Información debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe garantizar que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- La Oficina de Gestión de la Información debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
- La Oficina de Gestión de la Información debe proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.
- La Oficina de Gestión de la Información debe establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
- La Oficina de Gestión de la Información debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Oficina de Gestión de la Información debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.
- La Oficina de Gestión de la Información debe controlar estrictamente el acceso a los códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de verificación y validación) con el fin de evitar la introducción a la funcionalidad no autorizada y para evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual.

### Normas dirigidas a: DESARROLLADORES (INTERNAOS Y EXTERNOS).

- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para acceder a la información y a la funcionalidad de las aplicaciones de acuerdo con la política de control acceso.
- Dentro de las buenas prácticas de desarrollo se debe tener en cuenta que las restricciones de acceso se deben basar en los requisitos de la aplicación individual del negocio y de acuerdo con la política de control de acceso.
- Los desarrolladores deben garantizar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deben garantizar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Los desarrolladores deben garantizar que los controles de autenticación cuando fallen lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- Los desarrolladores deben garantizar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez

establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

- Los desarrolladores deben garantizar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.
- Los desarrolladores deben asegurar que desde la administración de usuarios de las aplicaciones se pueda controlar el acceso a los datos e información, así como los derechos de acceso ejemplo (leer, escribir, borrar y ejecutar). Limitar la información contenida en las salidas. Proveer controles de acceso físico o lógico.
- Los desarrolladores deben cumplir con las políticas de desarrollo definidas sin excepciones.
- Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
- Los testers deben garantizar en la etapa de pruebas que los desarrollos de las aplicaciones cumplan con las políticas de desarrollo y con los requisitos funcionales y no funcionales establecidos y se debe documentar.
- Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben generar pruebas para aceptación.
- Para el ambiente de prueba, se deben seleccionar, proteger y controlar los datos.

## POLITICA PARA USO DE TOKENS DE SEGURIDAD

La SAE proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los Funcionarios hagan un uso responsable de estos.

Normas para uso de tokens de seguridad

Normas dirigidas a: AREAS USUARIAS DE TOKENS DE SEGURIDAD

- Cada área usuaria de tokens de seguridad debe asignar un funcionario administrador de los mismos con la potestad para autorizar las solicitudes de acceso.

Normas dirigidas a: ADMINISTRADORES DE LOS TOKENS DE SEGURIDAD

- Los Administradores de los tokens de seguridad deben procesar las solicitudes de dichos tokens según los requerimientos de cada entidad proveedora de éstos y adjuntar la documentación necesaria.

- Los Administradores de los tokens deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.
- Los Administradores de los tokens deben crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada funcionario creado.
- Los Administradores de los tokens deben entregar a los funcionarios designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta y tula (o sobre) de seguridad para custodia de los mismos.
- Los Administradores de los tokens 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 los mismos.
- Los Administradores de los tokens deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.

### Normas dirigidas a: USUARIOS DE TOKENS DE SEGURIDAD

- Los usuarios que requieren utilizar los tokens de seguridad deben contar con una cuenta de usuario en los portales o sitios de uso de los mismos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado.
- Los usuarios deben devolver el token asignado en estado operativo al Administrador de los tokens cuando el vínculo laboral con la SAE se dé por terminado o haya cambio de cargo, para obtener el paz y salvo, el cual será requerido para legalizar la finalización del vínculo con la Sociedad.
- Cada usuario de los portales o sitios de uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.
- El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad, en la tula o sobre asignado para cada token, dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.
- Los usuarios deben notificar al Administrador de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las entidades emisoras de dichos tokens.
- Los usuarios no deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token.

- Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como funcionarios de la SAE. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica a que haya lugar.
- Los usuarios deben mantener los tokens asignados en un lugar seco y no introducirlos en agua u otros líquidos.
- Los usuarios deben evitar exponer los tokens a campos magnéticos y a temperaturas extremas.
- Los usuarios deben evitar que los tokens sean golpeados o sometidos a esfuerzo físico.
- Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.
- Los usuarios no deben usar los tokens fuera de las instalaciones de la SAE para evitar pérdida o robo de estos.

## POLÍTICAS DE CRIPTOGRAFIA

La SAE garantizará que la información de la Sociedad, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

### Normas de controles criptográficos

#### Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN

- La Oficina de Gestión de la Información, debe garantizar que la información digital clasificada como reservada o restringida, sea almacenada y/o transmitida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- La Oficina de Gestión de la Información, debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
- La Oficina de Gestión de la Información, debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.

- La Oficina de Gestión de la Información, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores deben cifrar la información reservada o restringida y garantizar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Los desarrolladores deben garantizar que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por La Oficina de Gestión de la Información.

## POLÍTICAS DE SEGURIDAD FÍSICA Y MEDIO AMBIENTAL

### POLÍTICA DE ÁREAS SEGURAS

La SAE proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Las protecciones físicas que se implementen en la Sociedad deben cubrir los aspectos básicos de las necesidades de la misma en cuanto a: controles de entradas físicos, seguridad de oficinas, espacios y medios, protección contra amenazas externas y ambientales.

En ese sentido, se deben establecer perímetros de seguridad en las áreas donde se encuentren instalados los centros de procesamiento de la Información, Suministro de Energía Eléctrica, Aire Acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los Sistemas de Información de la Sociedad de Activos Especiales SAS.

Normas de áreas seguras

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- Los perímetros de seguridad deberán estar delimitados por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas para controles de acceso físico.
- Todas las instalaciones de procesamiento de información deberán estar ubicadas dentro del perímetro de un edificio o área de construcción físicamente sólida. Las paredes externas del área deben ser sólidas y casi todas las puertas que comunican con el exterior deben estar

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

adecuadamente protegidas contra accesos no autorizados para lo cual se implementará un sistema de Control biométrico que será administrado por la Oficina de Gestión de la Información.

- Las solicitudes de acceso al Centro de Cómputo, a los centros de cableado y donde se ubiquen los servidores de la entidad deben ser aprobadas por funcionarios de La Oficina de Gestión de la Información autorizado. Adicionalmente estas instalaciones deberán contar con mecanismos de control de acceso, como mínimo puertas de seguridad, el ingreso de terceros a estas áreas debe estar registrado mediante una bitácora.
- La Oficina de Gestión de la Información debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- La Oficina de Gestión de la Información debe proveer las condiciones físicas y medioambientales necesarias para garantizar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- La Oficina de Gestión de la Información debe garantizar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.
- La Oficina de Gestión de la Información debe garantizar que los recursos de la plataforma tecnológica de la SAE ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.
- La Oficina de Gestión de la Información debe garantizar que el centro de cómputo y los centros de cableado se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La Oficina de Gestión de la Información debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.
- La Oficina de Gestión de la Información negará el uso de equipos de computación móvil, fotográficos, de vídeo, y/o audio, a menos que hayan sido formalmente autorizadas por el responsable del proceso involucrado y el responsable de Seguridad de la Información.

Normas dirigidas a: VICEPRESIDENTES, GERENTES Y JEFES DE OFICINA

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- Los Vicepresidentes, Gerentes y Jefes de Oficina que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en sus áreas.
- Los Vicepresidentes, Gerentes y Jefes de Oficina que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.
- Los Vicepresidentes, Gerentes y Jefes de Oficina deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios de la Sociedad.

Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA –RECURSOS FÍSICOS Y GERENCIA DE TALENTO HUMANO

- El área de Recursos Físicos debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la SAE.
- El área de Recursos Físicos debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de garantizar la seguridad física de las instalaciones de la Sociedad.
- El área de Recursos Físicos debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones De la SAE.
- El área de Recursos Físicos debe garantizar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.
- El área de Recursos Físicos procurará mantener en una buena ubicación de los equipos, aislados de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.
- Deberá verificarse la existencia de un área de recepción atendida por el personal determinado para tal fin, el acceso las áreas, edificios y sedes de la Sociedad, estará restringido exclusivamente al personal autorizado. De proceder el ingreso de personal externo y sin vínculo con la Entidad, se implementarán métodos de registro para cada ingreso y egreso en forma precisa.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Gerencia de Talento Humano deberá mantener al día la información de funcionarios de planta y demás funcionarios, y reportará esta información detallada con los retiros efectuados a la Oficina de Gestión de la Información para que se proceda a la exclusión del sistema, esto con el fin de garantizar el ingreso único de las personas autorizadas.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los ingresos y egresos de personal a las instalaciones de la SAE deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- Todos los funcionarios o terceros deberán portar el carné que acredite la prestación de sus servicios a la Sociedad de Activos Especiales SAS o el carácter de visitantes y no podrán ingresar a las áreas donde haya acceso restringido sin la debida autorización.
- Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- Los funcionarios de la SAE y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.
- No se permite comer, beber y fumar en las instalaciones y áreas de procesamiento de la información de la Sociedad.

### Normas de ingreso a las instalaciones de SAE

#### Normas dirigidas a: TODOS LOS USUARIOS

- Se deberá supervisar o inspeccionar a los visitantes y registrar la fecha y horario de su ingreso y egreso, en este sentido, sólo se permitirá el acceso con propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- Se deberá controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas, teniendo en cuenta para ello lo dispuesto en las leyes y decretos para tales fines. En ese sentido, La oficina de Gestión de la Información deberá actuar transversalmente para administrar permisos en casos de control biométrico u otras herramientas para el perímetro digital.
- Se utilizarán controles de autenticación para autorizar y validar todos los accesos a las distintas áreas de la entidad, teniendo en cuenta para ello lo siguiente:

- Cuando se vayan a realizar reuniones al interior de la entidad en las que se requiera el ingreso de Funcionarios de otras entidades o personal externo no vinculado a SAE, se deberá llevar un registro que incluirá como mínimo: la fecha y horario de ingreso, la nombre completo e identificación de las personas autorizadas para ingresar y se determinará de manera breve el asunto o motivo de la visita o el área a la que se dirige.
- Se implementará el uso de una identificación única visible para todo el personal interno y externo; los funcionarios de la entidad deberán portar en todo momento el carnet, que les asigne, así como, los visitantes deberán utilizar el carnet, documento o sticker que los identifica de esta manera durante todo el tiempo que dure la visita a la entidad y deberán entregar al momento de su registro en recepción un documento que no sea la cédula.
- Se deberá llevar un registro constante de los ingresos y egresos a las sedes de funcionamiento de la Sociedad, respecto del cual se realizará una auditoria semestral por parte del funcionario designado por la Vicepresidencia Administrativa y Financiera. Este registro deberá contar con criterios mínimos de identificación como: números de contacto, identificaciones con fotografía, validación de cédulas, entre otros.

### Normas de Condiciones Ambientales y de Infraestructura

#### Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA –RECURSOS FISICOS

- Se debe revisar regularmente las condiciones ambientales y de infraestructura con el fin de verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de la Sociedad de Activos Especiales SAS, esta revisión se realizará cada trimestre como mínimo.
- De manera preventiva y cuando se considere necesario, la Gerencia General podrá autorizar que se realice una revisión de las áreas externas o edificaciones que colindan con las sedes de funcionamiento de la entidad con el fin de realizar los requerimientos que correspondan y mitigar así el impacto de las posibles amenazas que se puedan presentar.

### POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

La SAE para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la Sociedad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

#### Normas de seguridad para los equipos institucionales

### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe proveer los mecanismos y estrategias necesarios para garantizar la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la SAE.
- La Oficina de Gestión de la Información debe garantizar la realización de mantenimiento preventivo y correctivo de los recursos de la plataforma tecnológica de la Sociedad.
- La Oficina de Gestión de la Información, en conjunto con la Coordinación de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.
- La Oficina de Gestión de la Información debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la Sociedad y configurar dichos equipos acogiendo los estándares generados.
- La Oficina de Gestión de la Información debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la Sociedad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- La Oficina de Gestión de la Información debe aislar los equipos de áreas sensibles, como la que efectúan operaciones financieras para proteger su acceso de los demás funcionarios de la red de la SAE.
- La Oficina de Gestión de la Información debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la Sociedad, ya sea cuando son dados de baja o cambian de usuario.
- La Oficina de Gestión de la Información debe verificar periódicamente los equipos de cómputo de la Sociedad, especialmente aquellos que se encuentran ubicados en áreas sensibles.
- La Oficina de Gestión de la Información debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
- La Oficina de Gestión de la Información debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.

Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA – GRUPO DE RECURSOS FÍSICOS

- El Grupo de Recursos Físicos debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.
- El Grupo de Recursos Físicos debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.
- El Grupo de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la SAE cuente con la autorización documentada y aprobada previamente por el Coordinador de Recursos Físicos. Periódicamente, se llevarán a cabo revisiones precisas e inventarios de los bienes a cargo de la entidad con el fin de detectar el retiro no autorizado de activos, este control será efectuado por el personal que designe la Vicepresidencia Administrativa y Financiera.
- El Grupo de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la Sociedad posean pólizas de seguro.
- El Grupo de Recursos Físicos implementará el Sistema de Energía Ininterrumpible UPS y/o plantas eléctricas, para asegurar el Apagado Regulado y Sistemático de los Equipos de Cómputo de la sociedad y asegurar así la continuidad de las operaciones mientras se restablecen las fallas en el suministro de energía eléctrica.

Normas dirigidas a: TODOS LOS USUARIOS

- La Oficina de Gestión de la Información es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Sociedad.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los Funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione La Oficina de Gestión de la Información.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la SAE el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de La Oficina de Gestión de la Información, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Sociedad, solo

puede ser realizado por los funcionarios de La Oficina de Gestión de la Información, o personal de terceras partes autorizado por dicha Oficina.

- Los usuarios deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Los funcionarios de SAE no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.
- Los funcionarios de SAE no deben almacenar información en el escritorio del computador y este deberá permanecer libre para evitar la exposición de información.
- Los funcionarios de SAE no deben dejar información fuera de los gabinetes o muebles cuando esta no se requiera.
- Los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.

## POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

### POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La Oficina de Gestión de la Información, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de la SAE, asignará funciones específicas a sus funcionarios, quienes deben garantizar la adecuada operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de garantizar la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos serán adecuadamente controlados y debidamente autorizados.

La Oficina de Gestión de la Información garantizará una capacidad de procesamiento adecuada en los recursos tecnológicos y sistemas de información de la Sociedad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

Normas de asignación de responsabilidades operativas

Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Oficina de Gestión de la Información debe garantizar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Sociedad.
- La Oficina de Gestión de la Información debe proporcionar a sus funcionarios: manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la SAE.
- La Oficina de Gestión de la Información debe proveer los recursos necesarios para la implantación de controles con el fin de garantizar la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.
- La Oficina de Gestión de la Información, a través de sus funcionarios, debe garantizar la realización de estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.
- La Oficina de Gestión de la Información debe contar con contactos de apoyo o soporte externo, para el manejo de dificultades operaciones o técnicas inesperadas.
- La Oficina de Gestión de la Información debe contar con procedimientos de reinicio o recuperación del sistema para uso en el caso de falla del sistema.
- La Oficina de Gestión de la Información debe controlar los cambios en la SAE, en los procesos de negocio, en instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
- La Oficina de Gestión de la Información debe aplicar controles de detección que indiquen los problemas oportunamente.
- La Oficina de Gestión de la Información debe separar los ambientes de desarrollo, pruebas, preproducción y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.
- La Oficina de Gestión de la Información debe usar diferentes perfiles para sistemas en producción y de pruebas.

- La Oficina de Gestión de la Información debe aplicar controles para que los datos sensibles no se copien en ambiente de pruebas, a menos que se suministren controles equivalentes.

Normas dirigidas a: GERENCIA DE TALENTO HUMANO

- La Gerencia de Talento Humano debe tener en cuenta la capacidad y crecimiento de los recursos humanos e indicar con anticipación a la Oficina de Gestión de la Información para que se incluya en el plan de gestión capacidad.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de la Sociedad.

## POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

La SAE proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

Normas de protección frente a software malicioso

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la SAE y los servicios que se ejecutan en la misma.
- La Oficina de Gestión de la Información debe garantizar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, garantizando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Oficina de Gestión de la Información debe garantizar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- La Oficina de Gestión de la Información, a través de sus funcionarios, debe garantizar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- La Oficina de Gestión de la Información, a través de sus funcionarios, debe garantizar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- La Oficina de Gestión de la Información debe llevar a cabo revisiones regulares de las actualizaciones e instalación del software de detección y reparación de software malicioso para analizar los computadores y medios como una medida de control.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por La Oficina de Gestión de la Información; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben garantizar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que, a través de ella, La Oficina de Gestión de la Información tome las medidas de control correspondientes o reenviar los correos a [oficialseguridad@saesas.gov.co](mailto:oficialseguridad@saesas.gov.co)

### POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La SAE garantizará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de La Oficina de Gestión de la Información, encargada de la generación de copias de respaldo, definirán la estrategia a seguir para el respaldo y almacenamiento de la información.

### Normas de copias de respaldo de la información

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, garantizando su integridad y disponibilidad.
- La Oficina de Gestión de la Información, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- La Oficina de Gestión de la Información debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- La Oficina de Gestión de la Información debe definir los requisitos de retención y de protección.
- La Oficina de Gestión de la Información debe definir aplicar herramientas de copias de respaldo que protejan la información respaldada.
- La Oficina de Gestión de la Información debe monitorear la ejecución de las copias de respaldo y darle tratamiento a las fallas de las copias de respaldo programadas, para asegurar que se realiza de manera completa y de acuerdo con las políticas establecidas.

#### Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con La Oficina de Gestión de la Información, las estrategias para la generación, retención y rotación de las copias de respaldo de la LOS ACTIVOS información.

#### Normas dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de los usuarios de la plataforma tecnológica de la SAE identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

- Es responsabilidad de los usuarios de la plataforma tecnológica de la SAE ubicar la información de los procesos de negocio en el servidor de archivos para que la Oficina de Gestión de la Información realice las copias de respaldo correspondiente.

### POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLOGICOS Y LOS SISTEMAS DE INFORMACIÓN

La SAE, a través de la Oficina de Gestión de la Información, realizará monitoreo permanente del uso que dan los funcionarios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información de la Sociedad. Además, velará por la custodia de los registros de auditoría cumpliendo con los períodos de retención establecidos para dichos registros.

Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN

- La Oficina de Gestión de la Información, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de la SAE.
- La Oficina de Gestión de la Información, a través de sus funcionarios, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- La Oficina de Gestión de la Información debe garantizar la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información de la SAE. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.
- La Oficina de Gestión de la Información debe garantizar que al inicio de sesión se informe a los funcionarios y terceros que ingresan a la red de SAE, que está siendo grabado y monitoreado y que los recursos de la red son para uso y cumplimiento de sus funciones.
- La Oficina de Gestión de la Información debe entregar herramientas de monitoreo que permitan llevar un control adecuado para los eventos que se lleguen a presentar
- La Oficina de Gestión de la Información debe entregar las evidencias necesarias en caso de presentarse un incidente de seguridad que incumpla con los principios de Integridad, Confidencialidad y/o Disponibilidad de la Información a la persona autorizada por la Presidencia de la SAE.

- La Oficina de Gestión de la información debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.
- La Oficina de Gestión de la información debe verificar que los administradores de sistemas no tengan permiso para borrar o desactivar registros.
- La Oficina de Gestión de la información debe verificar que los relojes de todos los sistemas de procesamiento de información deben sincronizarse con una única fuente de referencia de tiempo.

### Normas dirigidas a: OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

- El Oficial de Seguridad de la Información debe determinar los períodos de retención de los registros (logs) de auditoría de los recursos tecnológicos y los sistemas de información de la Sociedad.

### Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

- Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.
- Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por La Oficina de Gestión de la Información.
- Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.

### POLITICA DE CONTROL AL SOFTWARE OPERATIVO

La SAE, a través de Oficina de gestión de información, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, garantizará el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

### Normas de control al software operativo

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la Sociedad.
- La Oficina de Gestión de la Información debe garantizar que el software operativo instalado en la plataforma tecnológica de la SAE cuenta con soporte de los proveedores.
- La Oficina de Gestión de la Información debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- La Oficina de Gestión de la Información debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe garantizar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- La Oficina de Gestión de la Información debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Sociedad.
- La Oficina de Gestión de la Información debe conservar versiones anteriores del software de aplicación como una medida de contingencia.

### POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La SAE, a través de La Oficina de Gestión de la Información y la Oficina de Control Interno, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

### Normas para la gestión de vulnerabilidades

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, a través de un tercero, que cumplan con estándares nacionales e internacionales.
- La Oficina de Gestión de la Información debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.
- La Oficina de Gestión de la Información debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- La Oficina de Gestión de la Información, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
- La Oficina de Gestión de la Información, a través de sus funcionarios debe probar y evaluar los parches antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar. Si no es posible hacer una prueba adecuada de los parches, debido a los costos o a la falta de recursos, se puede considerar un retraso en la colocación del parche para evaluar los riesgos asociados con base a una experiencia reportada por otros usuarios.
- La Oficina de Gestión de la Información debe implementar controles para la instalación de software por parte de los usuarios.

## POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

## POLÍTICA DE GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS

La SAE proveerá, a través de La Oficina de Gestión de la Información, los mecanismos de control necesarios para garantizar la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Sociedad.

Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe adoptar medidas para garantizar la disponibilidad de los recursos y servicios de red de la SAE.
- La Oficina de Gestión de la Información debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- La Oficina de Gestión de la Información debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Sociedad.
- La Oficina de Gestión de la Información debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
- La Oficina de Gestión de la Información debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la Sociedad, acogiendo buenas prácticas de configuración segura.
- La Oficina de Gestión de la Información, a través de sus funcionarios, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la Sociedad en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- La Oficina de Gestión de la Información debe instalar protección entre las redes internas de la SAE y cualquier red externa, que este fuera de la capacidad de control y administración de la Sociedad.
- La Oficina de Gestión de la Información debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos De la SAE.

## POLÍTICA DE USO DEL CORREO ELECTRONICO

La SAE, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios, contratistas y terceras partes, proporcionará y garantizará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

### Normas de uso del correo electrónico

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN Y OFICINA DE COMUNICACIONES

- La Oficina de Gestión de la Información debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- La Oficina de Gestión de la Información debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.
- La Oficina de Gestión de la Información debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- La Oficina de Gestión de la Información debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- La Oficina de Gestión de la Información, con el apoyo de la Vicepresidencia Administrativa y Financiera, debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

### Normas dirigidas a: TODOS LOS USUARIOS

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la Sociedad o provisto por un tercero, en ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los usuarios de correo electrónico institucional 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 funcionarios de la Sociedad y el personal provisto por terceras partes.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la SAE. El correo institucional no debe ser utilizado para actividades personales.

- El envío de correo electrónico masivos debe ser autorizado por el área de Talento Humano, está prohibido el envío correo a grupos masivos.

### POLÍTICA DE USO ADECUADO DE INTERNET

La SAE consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para garantizar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la Sociedad.

Normas de uso adecuado de internet

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- La Oficina de Gestión de la Información debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- La Oficina de Gestión de la Información debe monitorear continuamente el canal o canales del servicio de Internet.
- La Oficina de Gestión de la Información debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- La Oficina de Gestión de la Información debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
- La Oficina de Gestión de la Información, con el apoyo la de la Oficina de Comunicaciones, debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios del servicio de Internet de la SAE deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- Los usuarios del servicio de Internet deben velar por el buen uso de internet y adoptar los controles que realiza la Oficina de Gestión de la Información.

### POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La SAE garantizará la protección de la información en el momento de ser transferida o intercambiada con otras entidades, acogiendo y aplicando el procedimiento de intercambio de información de acuerdo con su nivel de clasificación; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La Sociedad propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

#### Normas de intercambio de información

Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA – VICEPRESIDENCIA JURIDICA

- La Vicepresidencia Jurídica, en acompañamiento con la Oficina de Gestión de la Información, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la Sociedad y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la SAE a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.
- La Vicepresidencia Jurídica debe establecer en los contratos que se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios de la Sociedad que les ha sido entregada en razón del cumplimiento de los objetivos misionales de la SAE.

Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe definir y establecer el procedimiento estandarizado de intercambio de información con los diferentes terceros que, hacen parte de la operación de la

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

SAE, reciben o envían información de los beneficiarios de la Sociedad, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.

- La Oficina de Gestión de la Información debe velar porque el intercambio de información de la SAE con entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.
- La Oficina de Gestión de la Información debe autorizar el establecimiento del vínculo de transmisión de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

### Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Los propietarios de los activos de información deben velar porque la información de la SAE o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.
- Los propietarios de los activos de información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- Los propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información de la SAE por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente, la entrega de esta información será autorizada por la Gerencia General.
- Los propietarios de los activos de información deben garantizar que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la SAE, así como del procedimiento de intercambio de información.
- Los propietarios de los activos de información deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada, para lo cual deben requerir el acompañamiento de la Oficina de Gestión de la Información.

Normas dirigidas a: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA – COORDINACION DE CORRESPONDENCIA

- La Coordinación de Correspondencia debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- La Coordinación de Correspondencia debe garantizar que todo envío de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por la SAE, y que estos permitan ejecutar rastreo de las entregas.

Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Normas dirigidas a: TERCEROS CON QUIENES SE INTERCAMBIA INFORMACION DE LA SAE

- Los terceros con quienes se intercambia información de la SAE deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de la Sociedad, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.
- Los terceros con quienes se intercambia información de la Sociedad deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Normas dirigidas a: TODOS LOS USUARIOS:

- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la Sociedad o de sus beneficiarios.
- No está permitido el intercambio de información sensible de la Sociedad por vía telefónica.
- Los usuarios no deben tener conversaciones confidenciales en lugares públicos o mediante canales de comunicación no seguros, oficinas abiertas y lugares de reunión.

### POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

#### POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

La SAE asegurará que el software adquirido y desarrollado tanto al interior de la Sociedad, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él durante todo el ciclo de vida. Las áreas propietarias de sistemas de información, La Oficina de Gestión de la Información incluirá requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurará de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

##### Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN, OFICINA DE GESTIÓN DE LA INFORMACIÓN

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de la Sociedad formalmente asignada.
- La Oficina de Gestión de la Información debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
- Las áreas propietarias de los sistemas de información, en acompañamiento con La Oficina de Gestión de la Información y la Oficina de Control Interno deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.
- Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
- La Oficina de Gestión de la Información debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Normas dirigidas a: DESARROLLADORES (INTERNAOS O EXTERNAOS)

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Los desarrolladores deben garantizar que todo sistema de información adquirido o desarrollado debe usar herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores deben garantizar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- Los desarrolladores deben utilizar usar los protocolos sugeridos por La Oficina de Gestión de la Información en los aplicativos desarrollados.
- Los desarrolladores deben garantizar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

## POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

La SAE velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados durante el ciclo de vida, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se garantizará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Sociedad.

Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe implantar los controles necesarios para garantizar que las migraciones entre los ambientes de desarrollo, pruebas, preproducción y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La Oficina de Gestión de la Información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la SAE.
- La Oficina de Gestión de la Información debe asegurarse que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- La Oficina de Gestión de la Información debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- La Oficina de Gestión de la Información, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- La Oficina de Gestión de la Información debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la Sociedad.
- La Oficina de Gestión de la Información debe establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para garantizar la solución de problemas que se presenten en el software aplicativo de la SAE; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Los desarrolladores deben garantizar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Los desarrolladores deben garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos (logout) que permita terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de datos de los sistemas de información construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores deben garantizar el cierre la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y garantizar que dichos archivos solo tengan privilegios de lectura.
- Los desarrolladores deben garantizar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

### Normas dirigidas a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno debe verificar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

## POLÍTICA PARA LA PROTECCIÓN DE LOS DATOS DE PRUEBA

La Oficina de Gestión de la Información de la SAE protegerá los datos de prueba que se entregarán a los desarrolladores, garantizando que no revelan información confidencial de los ambientes de producción.

### Normas para la protección de los datos de prueba

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.
- La Oficina de Gestión de la Información debe realizar pruebas de aceptación para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de pruebas para aceptación y criterios de aceptación relacionados.

- La Oficina de Gestión de la Información debe asegurar la protección de los datos usados para pruebas.
- La Oficina de Gestión de la Información debe aplicar los mismos controles de acceso a los ambientes de desarrollo, pruebas, preproducción y producción.
- La Oficina de Gestión de la Información debe controlar a través de autorización por la mesa de ayuda la copia de información de operacional a un ambiente de pruebas.

## POLÍTICAS QUE RIGEN DE LA RELACION CON TERCERAS PARTES

### POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

La SAE establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de garantizar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los funcionarios responsables de la realización y/o firma de contratos o convenios con terceras partes garantizarán la divulgación de las políticas, normas y procedimientos de seguridad de la información para dichas partes.

Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN Y VICEPRESIDENCIA JURIDICA

- La Oficina de Gestión de la Información y la Vicepresidencia Jurídica deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.
- La Oficina de Gestión de la Información y la Vicepresidencia Jurídica deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Oficina de Gestión de la Información debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Sociedad.
- La Oficina de Gestión de la Información debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- La Oficina de Gestión de la Información debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica De la SAE.
- La Oficina de Gestión de la Información debe evaluar y aprobar los accesos a la información de la Sociedad requeridos por terceras partes.
- La Oficina de Gestión de la Información debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

### Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

- Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de la SAE a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.
- Los Supervisores de contratos con terceros deben verificar que estos cuenten con un acuerdo de confidencialidad y autorización de datos personales y deberán estar documentados.

## POLÍTICA DE GESTION DE LA PRESTACION DE SERVICIOS DE TERCERAS PARTES

La SAE propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

### Normas de gestión de la prestación de servicios de terceras partes

### Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- La Oficina de Gestión de la Información debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Sociedad.
- La Oficina de Gestión de la Información deben verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- La Oficina de Gestión de la Información debe implementar controles de exactitud y completitud, para asegurar la integridad de la información o del procesamiento de la información suministrada por una tercera parte.
- La Oficina de Gestión de la Información debe establecer las obligaciones aplicables a los proveedores para proteger la información de la SAE.
- La Oficina de Gestión de la Información debe establecer el manejo de incidentes y contingencias asociadas con el acceso de proveedores, incluidas las responsabilidades de la SAE y de los proveedores.

### Normas dirigidas a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno debe realizar auditorías al cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros.

### Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

- los Supervisores de contratos con terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.
- Los Supervisores de contratos con terceros, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

## POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

La SAE promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

### Normas para el reporte y tratamiento de incidentes de seguridad

#### Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los activos de información deben informar a la Oficina de Gestión de la Información, los incidentes de seguridad que les hayan sido reportados.

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- La Oficina de Gestión de la Información debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Crisis aquellos en los que se considere pertinente.
- La Oficina de Gestión de la Información debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su recurrencia.
- La Oficina de Gestión de la Información debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
- La Oficina de Gestión de la Información debe implementar un punto de contacto para la detección y reporte de incidentes de seguridad, estos pueden ser reportados a través de la mesa de ayuda o al correo [oficialseguridad@saesas.gov.co](mailto:oficialseguridad@saesas.gov.co)
- La Oficina de Gestión de la Información debe reportar las violaciones a la seguridad a la Gerencia de Talento Humano con el fin de iniciar el proceso formal disciplinario.
- La Oficina de Gestión de la Información debe realizar la retroalimentación de los reportes de eventos de seguridad de la información, una vez haya sido tratada y cerrada.

#### Normas dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de los funcionarios de la SAE y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a la Oficina de Gestión de la Información para que se registre y se le dé el trámite necesario.
- Todos los funcionarios y contratistas deben tomar conciencia de su responsabilidad de reportar los eventos de seguridad de la información.
- Es responsabilidad de los funcionarios de la SAE y del personal provisto por terceras partes que usan los servicios y sistemas de información que observen y reporten cualquier debilidad de seguridad de la información.

## POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

### POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN

La SAE proporcionará los recursos suficientes para garantizar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la Sociedad y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La SAE mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Normas dirigidas a: COMITÉ DE CRISIS

- El Comité de Crisis debe reconocer las situaciones que serán identificadas como emergencia o desastre para la Sociedad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

- El Comité de Crisis debe liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres
- El Comité de Crisis debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
- El Comité de Crisis debe, producto del análisis BIA deben seleccionar las estrategias de recuperación más convenientes para la Sociedad.
- El Comité de Crisis debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- El Comité de Crisis debe garantizar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información, debe elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

### Normas dirigidas a: VICEPRESIDENTES, GERENTES Y JEFES DE OFICINA

- Los vicepresidentes, Gerentes y jefes de Oficina deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para garantizar su efectividad.

## POLÍTICA DE REDUNDANCIA

La SAE propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la Sociedad.

### Normas de redundancia

#### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe analizar y establecer los requerimientos de

redundancia para los sistemas de información críticos para la Sociedad y la plataforma tecnológica que los apoya.

- La Oficina de Gestión de la Información debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la SAE.
- La Oficina de Gestión de la Información, a través de sus funcionarios, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para garantizar el cumplimiento de los requerimientos de disponibilidad de la Sociedad.

## POLÍTICAS DE CUMPLIMIENTO

### POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

La SAE velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a: VICEPRESIDENCIA JURIDICA – OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Vicepresidencia Jurídica, la Gerencia de Asuntos Legales y la Oficina de Gestión de la Información deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la sociedad y relacionados con seguridad de la información.

Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe garantizar que todo el software que se ejecuta en la Sociedad esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- La Oficina de Gestión de la Información debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la Sociedad para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.
- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.
- Los usuarios no deben copiar total ni parcialmente libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derechos de autor.

### POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la SAE a través de la Oficina de Gestión de la Información, propenderá por la protección de los datos personales de sus depositarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la SAE, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la Sociedad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la SAE exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la Sociedad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la Sociedad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

### Normas de privacidad y protección de datos personales

### Normas dirigidas a: AREAS QUE PROCESAN DATOS PERSONALES

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

---

recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Sociedad.

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

### Normas dirigidas a: OFICINA DE GESTIÓN DE LA INFORMACIÓN

- La Oficina de Gestión de la Información debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

### Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la Sociedad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.
- Es deber de los usuarios, solicitar la autorización para el tratamiento de datos personales, en caso de que se requiera.

### Normas dirigidas a: USUARIOS DE LOS PORTALES DE LA SAE

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

- Los usuarios de los portales de la SAE deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.
- Los usuarios de los portales de la SAE deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales de la SAE.
- Los usuarios de los portales de la SAE deben aceptar el suministro de datos personales que pueda hacer la Sociedad a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoría interna o externa.
- Los usuarios, proveedores, terceros y contratistas de la SAE deberán conocer y cumplir con el orientador estratégico que adopto el manual de tratamiento de datos personales.
- Los usuarios de la SAE deberán identificar los riesgos relacionados con los datos personales, de acuerdo con las funciones realizadas y deberá reportarlos al área de planeación.

## CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de Cambios
	Desde	Hasta	
1	27/04/2018	04/09/2018	Versión Inicial del SIG. Anteriormente existía una versión no controlada de este documento
2	05/09/2018	22/07/2021	Cambios en las políticas de dispositivos móviles
3	22/07/2021		Se realizó una revisión general a todas las políticas y se actualizaron de acuerdo con la nueva normatividad vigente y los controles de la ISO 27001:2013. Se ajustaron responsables de algunas políticas de acuerdo con la operación actual de SAE.

## ELABORACIÓN Y APROBACIÓN DEL DOCUMENTO

Elaboró:	Técnica: Dianalin Neme Prada	Profesional Especializado III	Oficina Asesora de Planeación
----------	------------------------------	-------------------------------	-------------------------------

# MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍA

	<b>Metodológica:</b> Paola Andrea López Jaramillo	Profesional III	Oficina Asesora de Planeación
<b>Aprobó:</b>	Antonio Orlando Olaya Tarquino	Jefe de Oficina de Gestión de la Información	Oficina de Gestión de la Información