

Políticas de Seguridad y Privacidad de la Información

Instituto Colombiano Agropecuario - ICA

Abril 2020

Las presentes Políticas son parte integral del Manual del SGSI del ICA

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

TABLA DE CONTENIDO

OBJETIVO	7
1. GENERALIDADES	7
1.1. APLICACIÓN	7
1.2. DEFINICIONES	7
1.3. NORMAS APLICABLES	10
2. INTRODUCCIÓN	11
3. POLITICA DE ALTO NIVEL DEL SGSI	12
4. AUTORIDADES Y ROLES DE SEGURIDAD DE LA INFORMACIÓN	12
5. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	13
5.1. ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	13
5.1.1. Políticas para la Seguridad de la Información	13
5.1.2. Revisión de las Políticas para la Seguridad de la Información	13
6. POLÍTICA de la ORGANIZACIÓN en LA SEGURIDAD DE LA INFORMACIÓN	14
6.1. ORGANIZACIÓN INTERNA	14
6.2. POÍÍTICA en DISPOSITIVOS MOVILES Y TELETRABAJO	14
6.2.1. Política para Dispositivos Móviles	14
6.2.2. Política de Teletrabajo	16
7. POLÍTICA DE SEGURIDAD EN LOS RECURSOS HUMANOS	19
7.1. ANTES DE LA VINCULACIÓN	19
7.2. DURANTE DE LA VINCULACIÓN	20
7.3. DESPUES DE LA VINCULACIÓN	22
8. POLÍTICA DE GESTIÓN DE ACTIVOS	22
8.1. RESPONSABILIDAD POR LOS ACTIVOS	22
8.1.1. Inventario de Activos	22
8.1.2. Propiedad de los Activos de Información	23
8.1.3. Uso Aceptable de los Activos de Información	24
8.1.4. Devolución de los Activos de Información	24
8.2. POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN	24
8.2.1. Clasificación de la Información	24
8.2.2. Etiquetado de la Información	25
8.2.3. Manejo de Activos de Información	25
8.3. POLÍTICA DE MANEJO DE MEDIOS	25

8.3.1.	Gestión de Medios Removibles	25
8.3.2.	Disposición de los Medios	26
8.3.3.	Transferencia de Medios Físicos	26
9.	POLÍTICA DE CONTROL DE ACCESO.....	27
9.1.	POLÍTICA Requisitos del Negocio para Control de Acceso.....	27
9.2.	POLÍTICA DE GESTIÓN DE ACCESO A USUARIOS.....	28
9.3.	POLÍTICA DE RESPONSABILIDAD DE LOS USUARIOS	30
9.4.	POLÍTICA CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	31
10.	POLÍTICA DE CRIPTOGRAFIA.....	32
11.	POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO	34
11.1.	ÁREAS SEGURAS	34
11.1.1.	Perímetros de Seguridad Física.....	34
11.1.2.	Controles de Acceso Físico.....	35
11.1.3.	Seguridad de Oficinas, Recintos e Instalaciones.....	36
11.1.4.	Protección Contra Amenazas Externas y Ambientales	37
11.1.5.	Trabajo en Áreas Seguras	37
11.1.6.	Áreas de Despacho y Carga.....	38
11.2.	EQUIPOS.....	38
11.2.1.	Ubicación y Protección de Equipos.....	38
11.2.2.	Servicio de Suministro	38
11.2.3.	Seguridad de Cableado	38
11.2.4.	Mantenimiento de Equipos	38
11.2.5.	Retiro de Activos.....	39
11.2.6.	Seguridad de Equipos y Activos Fuera de las Instalaciones	39
11.2.7.	Disposición Segura o Reutilización de Equipos	39
11.2.8.	Equipos de Usuarios Desatendidos	39
11.2.9.	Política de Escritorio Limpio y Pantalla Limpia	40
12.	POLÍTICA DE SEGURIDAD DE LAS OPERACIONES.....	40
12.1.	Procedimientos de operaciones y responsables.....	40
12.1.1.	Procedimientos de Operación Documentado	40
12.1.2.	Gestión de Cambio	41
12.1.3.	Gestión de Capacidad	41
12.1.4.	Separación de los Ambientes, de Desarrollo, Pruebas y Operación	41
12.2.	PROTECCIÓN CONTRA CODIGO MALICIOSO	41

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

12.2.1.	Controles Contra Código Malicioso	41
12.3.	COPIAS DE RESPALDO	42
12.3.1.	Respaldo de la Información	42
12.4.	REGISTRO Y SEGUIMIENTO	42
12.4.1.	Registro de Eventos	42
12.4.2.	Protección de la Información de Registros	42
12.4.3.	Registros de Administrador de Operador	42
12.4.4.	Sincronización de Relojes	43
12.5.	CONTROL DE SOFTWARE OPERACIONAL	43
12.5.1.	Instalación de Software en Sistemas Operativos.....	43
12.6.	GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	43
12.6.1.	Gestión de las Vulnerabilidades Técnicas	43
12.7.	CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN.....	43
12.7.1.	Controles de Auditoría de Sistemas de Información	43
13.	POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES	44
13.1.	GESTIÓN DE LA SEGURIDAD LAS REDES	44
13.1.1.	Controles de Redes	44
13.1.2.	Seguridad de los Servicios de Red.....	44
13.1.3.	Separación en las Redes	44
13.2.	TRANSFERENCIA DE INFORMACIÓN.....	45
13.2.1.	Política y Procesamiento de Transferencia de Información	45
13.2.2.	Acuerdos Sobre Transferencia de Información	45
13.2.3.	Mensajería Electrónica	45
13.2.4.	Acuerdos de Confidencialidad o de No Divulgación	46
14.	POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.....	47
14.1.	REQUISITOS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN	48
14.1.1.	Análisis y Especificaciones de Requerimientos de Seguridad de la Información	48
14.1.2.	Seguridad de Servicios de las Aplicaciones en Redes Públicas	48
14.1.3.	Protección de Transacciones de los Servicios de las Aplicaciones.....	49
14.2.	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	50
14.2.1.	Política de Desarrollo Seguro.....	50
14.2.2.	Procedimientos en Control de Cambios en Sistemas	50
14.2.3.	Revisión Técnicas de las Aplicaciones después de Cambios en la Plataforma de Operación	51
14.2.4.	Restricciones en los cambios a los paquetes de Software.....	51

14.2.5.	Principios de Construcción de los Sistemas Seguros	51
14.2.6.	Ambiente de Desarrollo Seguro.....	52
14.2.7.	Desarrollo Contratado Externamente.....	52
14.2.8.	Pruebas de Seguridad de Sistemas	52
14.2.9.	Pruebas de Aceptación de Sistemas de Sistemas	52
14.3.	DATOS DE PRUEBA	52
14.3.1.	Protección de Datos de Prueba	52
15.	RELACION CON LOS PROVEEDORES	53
15.1.	SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON LOS PROVEEDORES.....	53
15.1.1.	Política de Seguridad de Información para las Relaciones con Proveedores	53
15.1.2.	Tratamiento de Seguridad dentro de los Acuerdos con Proveedores	54
15.1.3.	Cadena de Suministro de Tecnología de Información y Comunicaciones	54
15.2.	GESTIÓN DE PRESTACIÓN DE SERVICIO DE PROVEEDORES	54
15.2.1.	Seguimiento y Revisión de los Servicios de los Proveedores.....	54
15.2.2.	Gestión de Cambios en los Servicios de los Proveedores	54
16.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	54
16.1.	GESTIÓN DE INCIDENTES Y MEJORA EN LA SEGURIDAD DE LA INFORMACIÓN	55
16.1.1.	Responsabilidades y Procedimientos	55
16.1.2.	Reporte de Eventos de Seguridad de Información	55
16.1.3.	Reporte de Debilidades de Seguridad de Información	55
16.1.4.	Evaluación de los Eventos de Seguridad de la Información y Decisiones Sobre Ellos	56
16.1.5.	Respuesta a Incidentes de Seguridad de la Información	56
16.1.6.	Aprendizaje Obtenido de los Incidentes de Seguridad de la Información	56
16.1.7.	Recolección de Evidencia.....	56
17.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.....	56
17.1.	CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN.....	57
17.1.1.	Planificación de la Continuidad de la Seguridad de la Información.....	57
17.1.2.	Implementación de la Continuidad de la Seguridad de la Información.....	57
17.1.3.	Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información	57
17.2.	REDUNDANCIA	57
17.2.1.	Disponibilidad de las Instalaciones de Procesamiento de Información.....	57
18.	CUMPLIMIENTO	58
18.1.	CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	58
18.1.1.	Identificación de la Legislación Aplicable y de los Requisitos Contractuales.....	58

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

18.1.2.	Derecho de Propiedad Intelectual	58
18.1.3.	Protección de Registros.....	58
18.1.4.	Privacidad y Protección de Información de Datos Personales.....	58
18.2.	REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	61
18.2.1.	Revisión Independiente de la Seguridad de la Información	61
18.2.2.	Cumplimiento con las Políticas y Normas de Seguridad	61
18.2.3.	Revisión de Cumplimiento Técnico.....	61
19.	VIGENCIA DE LAS POLÍTICAS.....	61
	Las políticas descritas en este documento regirán a partir de la fecha de aprobación y publicación de la misma.	61

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

OBJETIVO

Establecer las Políticas complementarias alineadas a la Política de Alto Nivel del Sistema de Gestión de Seguridad de la Información - SGSI del Instituto Colombiano Agropecuario, en adelante ICA, en pro de gestionar adecuadamente la integridad, confidencialidad y disponibilidad de los activos de información, en el marco de la NTC/ISO 27001:2013 y su Anexo A.

1. GENERALIDADES

El presente Manual de Políticas complementarias de Seguridad de la Información hace parte integral del Modelo de Seguridad adoptado por el ICA y establecido en el Manual del SGSI.¹

1.1. APLICACIÓN

Las Políticas de Seguridad de la Información establecidas en el presente Manual, han sido orientadas para todos los Procesos, Funcionarios, Contratistas, Proveedores y/o Terceros, que dependan o interactúen con el ICA, en términos de seguridad de la información.

1.2. DEFINICIONES

- **Acceso lógico:** Es un acceso en red a través de la ICAnet de la Entidad o de Internet.
- **Activos de Información:** Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos del proceso.
- **Almacenamiento:** Se refiere a la forma en la que se almacena el activo, como en medios magnéticos, salas, cajas, PC's, Servidores, CD's, DVD's, USBs, Cintas magnéticas, etc.
- **Área solicitante²:** Es la dependencia del Instituto Colombiano Agropecuario ICA que solicita al Funcionario competente y/u ordenador del gasto, la contratación de Bienes o Servicios para satisfacer necesidades o solucionar problemas.
- **Autorización³:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Base de Datos⁴:** Conjunto organizado de datos personales que sea objeto de Tratamiento;
- **Cifrado:** Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación (letras, símbolos o números) del contenido que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos).
- **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la Entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la Entidad.

¹ Ver Manual del SGSI del ICA

² **Fuente:** Definiciones - Manual de Contratación GRFT-GC-MP-001

³ Fuente: Definiciones Ley 1581 de 2012

⁴ Fuente: Definiciones Ley 1581 de 2012

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- **Complementario:** Hace referencia a todo aquel elemento, objeto, individuo o fenómeno que se caracteriza por unirse a otro elemento para completarlo y, en lo posible, mejorarlo.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Contraseña:** Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.
- **Contratista:** Persona natural o jurídica que se vincula a la entidad con el objeto de prestar al Instituto un bien o un servicio determinado.
- **Creación:** Se refiere a la concepción de documentos o datos, el momento en el cual se origina el contenido (digital o físico) de un medio de información.
- **Custodio:** Persona delegada para ejercer el cuidado o vigilancia sobre un activo que le ha sido encargado.
- **Dato personal⁵:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Destrucción:** Se refiere a la actividad para la destrucción de la información que se maneja sobre el activo en el momento en el que este finaliza su ciclo de vida:
 - Incineración: Destrucción de información exponiéndola a altas temperaturas para quemarla.
 - Borrado Seguro: Aplica solo para medio magnéticos, es un borrado a bajo nivel.
 - Trituración: Esto aplica más que todo a la destrucción de papel por medio de máquinas trituradoras.
- **Dominio:** Áreas en las que se desarrolla la NTC/ISO 27001.
- **Encargado del Tratamiento⁶:** 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.
- **Etiquetado:** Colocar una etiqueta o rótulo para identificar un elemento.
- **Evento de Seguridad de la Información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

⁵ Fuente: Definiciones Ley 1581 de 2012

⁶ Fuente: Definiciones Ley 1581 de 2012

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- **Excepciones:** Todo aquello que se excluye de la generalidad o regla común.
- **ICAnet:** Hace referencia a la Intranet del Instituto Colombiano Agropecuario – ICA.
- **Incidente de seguridad de la Información:** Un evento o serie de eventos de seguridad de la Información no deseados o inesperados, que tiene una la probabilidad significativa de comprometer las operaciones del negocio o amenazar la seguridad de la información de los activos críticos que almacenen, procesen y/o gestionen información.
- **Integridad:** Propiedad de Salvaguardar la exactitud y estado completo de los activos.
- **Inventario de activos:** Listado de recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)
- **Lineamientos:** Describe en orden numérico y de acuerdo a su importancia las directrices específicas establecidas para la aplicación de la política.
- **Medio Removible:** Dispositivos de almacenamiento independientes del computador que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, discos duros extraíbles, DVD y CD.
- **Política de seguridad de la información:** Establece a alto nivel los objetivos y metas relacionados con la seguridad de la información.
- **Programas Utilitarios:** Los utilitarios o utilidades, son programas diseñados para realizar una función determinada, por ejemplo un editor, un depurador de código o un programa para recuperar datos perdidos o borrados accidentalmente en el disco duro.
- **Propietario de la información:** Es el responsable de definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida del mismo.
- **Responsable del Tratamiento⁷:** 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.
- **Rol:** El papel que desempeña un individuo o un grupo en una actividad determinada.
- **Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.
- **Servidor Público:** Es una persona que desempeña un empleo público. Se trata de un trabajador que cumple funciones en el organismo del estado.
- **Sistema de procesamiento de información:** Es un sistema que transforma los datos en información organizada, significativa y útil.

⁷ Fuente: Definiciones Ley 1581 de 2012

- **Teletrabajador:** Es la persona que utiliza las tecnologías de la información y comunicación como medio para realizar su actividad laboral fuera del local del empleador, en el marco de un contrato de trabajo o de una relación laboral dependiente, en la cual le sean garantizados todos sus derechos laborales.
- **Teletrabajo:** Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo⁸.
- **Titular**⁹: Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Token de seguridad:** (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación. Los tokens electrónicos se usan para almacenar claves criptográficas como firmas digitales o datos biométricos, como las huellas digitales.
- **Transporte de datos:** Considera las diferentes formas en la que se transporta la información de un lado a otro y los cuidados que se debe tener en este proceso, según su nivel de clasificación.
- **Tratamiento**¹⁰: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Usuario:** Es un individuo que utiliza una computadora, un sistema operativo o cualquier sistema informático. Por lo general es una única persona.
- **VPN:** (Virtual Private Network) Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

1.3. NORMAS APLICABLES

- Normograma del SGSI
- NTC/ISO 27001:2013
- NTC/ISO 27005:2009
- GTC/ISO 27002:2015
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL
- Política de Gobierno Digital.

⁸ Fuente: Definiciones Ley 1221 de 2008

⁹ Fuente: Definiciones Ley 1581 de 2012

¹⁰ Fuente: Definiciones Ley 1581 de 2012

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

2. INTRODUCCIÓN

La adopción de Políticas, y procedimientos en el Instituto Colombiano Agropecuario ICA, obedece a una decisión estratégica que cumple con las normas de Seguridad y Privacidad de la Información.

Éstas deben analizarse, diseñarse e implementarse para satisfacer las necesidades, los objetivos, los requisitos de seguridad, los procesos, el tamaño, la Tecnología y la estructura del Instituto.

En la actualidad, el ICA identifica la información como uno de los activos indispensables en la conducción y consecución de los objetivos definidos en el Plan Estratégico de la Entidad, razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida de manera adecuada independientemente del medio en la que ésta sea manejada, procesada, transportada o almacenada.

Adicional a lo expuesto, en la medida en que los sistemas de información se constituyen en un apoyo de los procesos del Instituto, se requiere contar con estrategias de Alto Nivel que permitan el control y administración efectiva de la información.

Las Políticas de Seguridad y Privacidad de la Información, establecen los objetivos e identifican y definen las responsabilidades para una protección apropiada de los activos de información de la Entidad, por ello con su implementación, se busca reducir el riesgo de que en forma accidental o intencional se divulguen, modifiquen, destruyan o usen en forma indebida

De igual forma, con la adopción de las Políticas de Seguridad y Privacidad de la información, se busca que el Instituto fortalezca la administración de la seguridad de sus activos de información, apoyados en controles tecnológicos, administrativos y operativos en los que intervienen personas y que generan que estas políticas contemplen los siguientes aspectos:

- Sean Holísticas, es decir, que la seguridad se debe ver como un todo de manera global e integrada.
- Se adecuen a las necesidades reales y recursos de la entidad.
- Definan estrategias y criterios generales a cumplir en distintas funciones y actividades que se ejecutan dentro del Instituto.

De esta manera, el propósito de la Entidad, a través de las Políticas de Seguridad y Privacidad de la Información, es la construcción de una descripción de lo que el ICA, debe proteger en el marco de la normatividad Legal Vigente relacionada con la Seguridad de la Información y la Política de Gobierno Digital.

Teniendo en cuenta lo expuesto, el ICA, define sus Políticas, por medio de las cuales asegura y mantiene la Confidencialidad, Integridad y Disponibilidad de la Información; por tanto cada Política es revisada, aprobada, establecida y socializada desde la alta dirección a todos los niveles de la Entidad, incluyendo Funcionarios, Contratistas, Proveedores y/o Terceros, para su estricto cumplimiento.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

3. POLITICA DE ALTO NIVEL DEL SGSI

Armonizados con el Plan Estratégico Institucional de la Entidad establece como Política de Alto Nivel del Sistema de Gestión de Seguridad de la Información - SGSI, la siguiente:

“la información es reconocida por el Instituto Colombiano Agropecuario (ICA) como uno de los activos más importantes para lograr los objetivos de la Entidad, es por eso que se compromete a disponer sus recursos tanto físicos, tecnológicos, financieros, informativos, de conocimiento y humanos para liderar y fortalecer la seguridad de la información a través del establecimiento, implementación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI); cuyo fin es el aseguramiento de la integridad, disponibilidad y confidencialidad de la información mediante la gestión y tratamiento adecuado de los riesgos, en el marco de los requisitos normativos y legales de la entidad y por lo tanto; participar activamente en el desarrollo del Plan de Cultura y Sensibilización de Seguridad de la Información”.

4. AUTORIDADES Y ROLES DE SEGURIDAD DE LA INFORMACIÓN

Para asegurar el adecuado entendimiento de cada una de las Políticas, a continuación se presentan las autoridades y los roles establecidos en el Modelo de Seguridad y Privacidad de la Información adoptado por la entidad¹¹ e insumo para la definición de cada uno de los lineamientos:

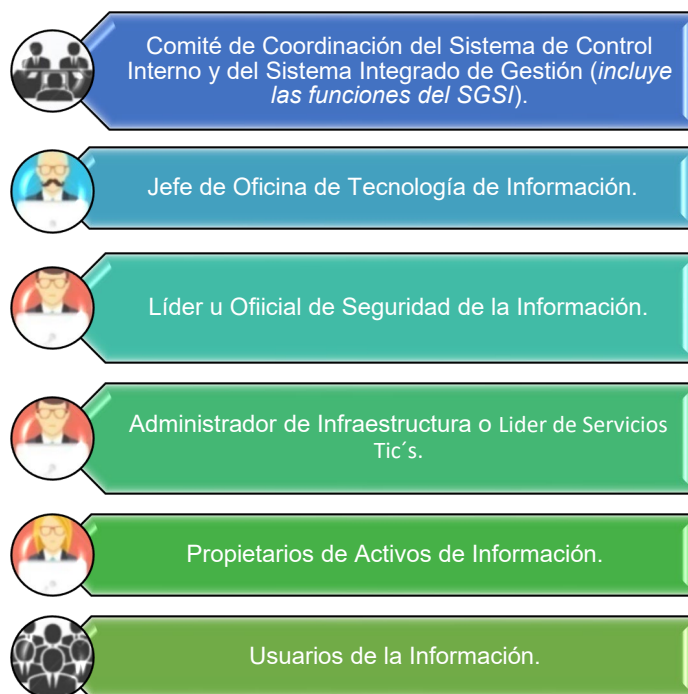


Ilustración 1. Autoridades y Roles de seguridad de la información del ICA

¹¹ Ver Manual del SGSI del ICA

5. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1. ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- **Dominio:** A.5.1.1 Políticas para la Seguridad de la Información.
- **Objetivo:** Brindar orientación y soporte por parte de dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
- **Alcance:** Se debe definir un conjunto de Políticas para la Seguridad de la Información, aprobada por la dirección, publicadas y comunicada a los Funcionarios, Contratistas, Proveedores y/o Terceros.
- **Lineamientos:**

5.1.1. Políticas para la Seguridad de la Información

- a. Las Políticas de Seguridad y Privacidad de la Información del ICA están relacionadas con la información o datos que se encuentran en los recursos tecnológicos, humanos, físicos, que manejan administran y custodian los Funcionarios, Contratistas, Proveedores y/o Terceros.
- b. Las Políticas definidas a continuación se encuentran estructuradas y orientadas con base en cada dominio o control del Anexo A de la NTC ISO 27001:2013, y están alineadas con las prácticas de gestión de la NTC ISO 27002:2015.
- **Exepciones:**
Cualquier excepción a los lineamientos precedentes, debe ser autorizada por la Oficina de Tecnologías de la Información y el Líder u oficial de Seguridad de la información de la Entidad.

5.1.2. Revisión de las Políticas para la Seguridad de la Información

- **Dominio:** A.5.1.2 Revisión de las Políticas para la Seguridad de la Información.
- **Objetivo:** Brindar orientación y soporte por parte de dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
- **Alcance:** La presente política establece revisiones necesarias al documento de Políticas de Seguridad y Privacidad de la Información de la entidad.
- **Lineamientos:**
 - a. La definición, actualización y mantenimiento del documento de Políticas de Seguridad y Privacidad de la Información del ICA, es responsabilidad del Líder u Oficial de Seguridad de Información quien debe revisar las Políticas al menos una vez al año o cuando ocurran cambios significativos para asegurar su conveniencia, adecuación, y eficacia continua; con la debida aprobación del responsable del Sistema de Gestión Integrado o quien haga de sus veces y deberá seguir los lineamientos definidos en el procedimiento de control de documentos.
 - b. En las revisiones periódicas se debe tener en cuenta factores como:
 - Prioridades de la Entidad.
 - Costos e impacto de los controles a implementar por la Entidad.
 - Incidentes de Seguridad de Información reportados.
 - Nuevas vulnerabilidades detectadas.
 - Cambios en los requerimientos regulatorios y/o legales.
 - Cambios en infraestructura tecnológica de la Entidad.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- Cambios en los objetivos del Sistema de Gestión de Seguridad de la Información “SGSI”.
- Cambios en los objetivos de la Entidad entre otros.

- **Exepciones:**

Cualquier excepción a los lineamientos precedentes, debe ser autorizada por la Oficina de Tecnologías de la Información y el Líder u Oficial de Seguridad de la información de la Entidad.

6. POLÍTICA DE LA ORGANIZACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN

6.1. ORGANIZACIÓN INTERNA

- **Dominio/ Control:** A.6.1 Organización Interna.
- **Objetivo:** Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la Seguridad de la Información dentro de la Entidad.
- **Alcance:** La presente Política identificar el alcance de la implementación del Sistema de Gestión de Seguridad de la Informamcion “SGSI” en el ICA.
- **Lineamientos:**
 - a. La Oficina de Tecnologia de Información, implementará el Sistema de Gestión de Seguridad de la Información “SGSI” en todos los Procesos:
 - Estrategicos.
 - Misionales.
 - Apoyo.
 - Evaluación y Control.
 - b. La Oficina de Tecnologia de Información, define en el Manual del Sistema de Gestión de Seguridad de Informacón “SGSI” los roles y responsabilidades.
 - c. La Entidad deberá mantener contacto con las autoridades pertinentes y los grupos de intereses especiales tales como: Policía Nacional, Profesionales especializados en Seguridad, Colcert Gobierno, entre otros.
 - d. Todos los nuevos proyectos que se planteen ejecutar en la entidad, independientemente de su naturaleza deberán contemplar los requisitos de Seguridad de la Información.
- **Exepciones:**
Cualquier excepción a los lineamientos precedentes, debe ser autorizada por la Oficina de Tecnologías de la Información y el Líder u Oficial de Seguridad de la información de la Entidad.

6.2. POLÍTICA EN DISPOSITIVOS MOVILES Y TELETRABAJO

6.2.1. Política para Dispositivos Móviles

- **Dominio/ Control:** A.6.2.1 Política para Dispositivos Móviles
- **Objetivo:** Garantizar la seguridad en el uso de los dispositivos móviles.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- **Alcance:** La presente Política aplica para todos los Funcionarios, Contratistas, Proveedores y/o Terceros o que por su rol, hagan uso de dispositivos móviles en la entidad.

- **Lineamientos:**

- La Oficina de Tecnologías de la Información efectuará labores de monitoreo tanto a los dispositivos móviles propios de la entidad como a los personales conectados a la red del Instituto (cuando a ello haya lugar) con el objeto de adoptar los mecanismos de protección de la información y aplicar las medidas correctivas cuando se requieran.
- La Oficina de Tecnologías de la Información debe establecer las configuraciones definidas para el manejo tanto de los dispositivos móviles propios de la entidad como de aquellos que sean personales y se encuentren conectados en la red del Instituto siguiendo, para ello, las reglas generales de la Guía para el uso aceptable de activos previamente adoptada.
- Todos los usuarios que tengan autorizado el uso de dispositivos móviles personales deben cumplir con las reglas generales establecidas en la Guía para el uso aceptable de activos¹².
- Para agregar un dispositivo móvil personal a la red del ICA, debe contar con:
 - El Sistema Operativo Licenciado y actualizado (parchado).
 - El antivirus licenciado y actualizado.
 - La ofimática o aplicaciones necesarias para su gestión licenciadas.

NOTA: De no contener lo anterior el Funcionarios, Contratista, Proveedores y Terceros se hace responsable por los incidentes que este riesgo genere a la entidad.

- No se permite el ingreso a la entidad ni el acceso a la red del ICA, a los equipos que son personales de escritorio, dado que la entidad no se hace responsable de estos elementos.
- No es permitido instalar aplicaciones institucionales a equipos personales móviles.
- Aquellos equipos móviles personales que se encuentren conectados a la red de la entidad y estos no sean avalados y autorizados por la Oficina de Tecnologia de Información serán considerados como: "Equipos NO autorizados, e incumplimiento a las Políticas de Seguridad y Privacidad de la Información definidas por la entidad.
- Los equipos móviles personales, no tiene soporte de la Mesa de Ayuda para errores que en ellos se presenten.
- Los dispositivos móviles personales, deben estar protegidos por contraseña.

- **Excepciones:**

Cualquier excepción a los lineamientos precedentes, debe ser autorizada por la Oficina de Tecnologías de la Información y el Líder u Oficial de Seguridad de la Información de la Entidad.

¹² Ver Guía para el uso aceptable de activos del ICA

6.2.2. Política de Teletrabajo

- **Dominio/ Control:** A.6.2.2 Teletrabajo.
- **Objetivo:** Establecer los lineamientos para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza Teletrabajo.
- **Alcance:** La presente Política aplica para todos los Funcionarios o contratistas que laboren bajo la modalidad de Teletrabajo.
- **Lineamientos:**
El ICA establece los siguientes lineamientos, en el marco de la Ley 1221 de 2008 “Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones”:

6.2.2.1. El ICA, como Empleador debe:

- a. Suministrar a los Teletrabajadores equipos de trabajo para la ejecución de sus obligaciones y/o funciones (cuando a ello haya lugar) o autorizar la utilización de equipos personales para el Teletrabajo, siempre y cuando se cumpla y acepten los mecanismos y medidas de Seguridad de Información definidos por la Entidad.
- b. Será responsable del licenciamiento del Software de los equipos suministrados a los Teletrabajadores para su gestión.
- c. Dar a conocer a los Teletrabajadores los lineamientos impartidos a través de la presente Política y con ello los riesgos de su proceso que se derivan por el uso de los equipos tecnológicos para la Seguridad de la información de la Entidad.
- d. Definir los tipos de usuarios que dispondrán de modalidad de Teletrabajo y los permisos de acceso remoto pertinentes.
- e. Establecer procedimientos para la solicitud y autorización del Teletrabajo.
- f. Establecer un procedimiento de conexión remota de emergencia para solventar problemas e incidencias puntuales.
- g. Establecer un compromiso por parte del Teletrabajador (en el documento que defina la entidad), frente al cumplimiento de los lineamientos adoptados a través de la presente política, así como en lo relacionado al uso exclusivo del equipo (asignado por la Entidad o Personales), que se destine para la ejecución de sus obligaciones y/o funciones (según sea el caso), aceptando y cumpliendo para tales efectos con las medidas de seguridad de la información implementadas por la entidad.
- h. Identificar los derechos y obligaciones de cada una de las partes que intervienen en el Teletrabajo.
- i. La Oficina de Tecnología de Información llevara el seguimiento de las conexiones remotas a los servicios relacionados con el Teletrabajo. Especialmente se debe prestar atención a los intentos de conexión sospechosos.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

6.2.2.2. El Teletrabajador del ICA, debe:

- a. No podrá instalar software que no esté autorizado. (Ver política uso aceptable de los activos).
- b. Deben cumplir con las Políticas de Seguridad y Privacidad de Información definidas y establecidas por la Entidad.
- c. Deben cumplir con las reglas generales establecidas en la Guía para el uso aceptable de activos.
- d. No deben almacenar información Sensible o Confidencial en los equipos asignado por la entidad o personales sin que esta información este encriptada para efectos de Seguridad.
- e. Si los equipos para la ejecución de las funciones son personales se debe:
 - Tener Sistema Operativo Licenciado y actualizado (parchado), o si se requiere instalar se debe hacer desde una fuente fiable.
 - Tener antivirus licenciado y actualizado.
 - Tener la ofimática o aplicaciones necesarias para su gestión licenciadas.
 - Mantener las aplicaciones actualizadas.
 - Utilizar el control de acceso definido por la entidad con sus correspondientes permisos.
 - Mantener configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.).
 - Parametrizar el bloqueo automático por inactividad y en lo posible, utilizar un cifrado de disco.
- f. Los equipos asignados por la entidad o personales, no deben dejarse desatendidos, y evitar transportar el equipo si no es necesario.
- g. Utilizar guayas de Seguridad para equipos portátiles y de escritorio tipo “todo en uno” asignado por la entidad o personales.
- h. Para el transporte de equipos portátiles entre la oficina y el lugar o lugares en que se ejecuten las funciones de Teletrabajo, es necesario disponer de un maletín que ofrezca buena resistencia a caídas, golpes, aplastamiento líquidos u otro riesgo al que se encuentre expuesto el equipo.
- i. Guardar bajo llave en el sitio o sitios en los que se ejecuten las funciones de Teletrabajo, el dispositivo mientras no se utiliza.
- j. Establecer medidas de Seguridad de la Información Institucional, con el objeto de evitar el acceso no autorizado a esta, que se encuentra en el dispositivo.

- k. Manejar cuentas de usuario independientes si el equipo para la ejecución de las funciones de Teletrabajo es personal.
- l. No utilizar en los equipos portátiles asignado por la entidad o personales conexiones poco confiables como:(Wi-Fi abiertas, redes Públicas de hoteles, bibliotecas, locutorios, aeropuertos, entre otros) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL (los que empiezan por HTTPS).
- m. Verificar que en el acceso a los servidores institucionales se utilicen certificados reconocidos y que la figura del “candado” de la conexión SSL, nos permite identificar que no existan posibles peligros o errores.
- n. Utilizar contraseñas seguras siguiendo los lineamientos de la Política de control de acceso del ICA.
- o. Borrar historial de navegación, las cookies, extensiones y/o plugins que hallan sido instalados del navegador web en el equipo asignado por la Entidad o personal.
- p. No debe usar el cuadro de dialogo en el que se sugiera recordar contraseña por Políticas de seguridad de la Información en el equipo asignado por la Entidad o personal.
- q. Debe cerrar las conexiones con servidores y paginas web mediante la opción “desconectar” o “cerrar sesión” al finalizar su labor en el equipo asignado por la Entidad o personal.
- r. Debe eliminar la información temporal y alojada en las carpeta de descargas, documentos, imágenes, papelera de reciclaje, escritorio virtual u otras que se encuentren en diferentes carpetas del equipo asignado por la Entidad o personal.
- s. Solicitar a la mesa de ayuda de la entidad, cuando sea necesario, la aplicación de las herramientas de borrado seguro sobre la información institucional alojada en el equipo asignado por la entidad o personal con el que se ejecuten las labores de Teletrabajo, previa autorización cuando sea el caso.
- t. Asegurarse de retirar cualquier memoria USB, disco duro externo ,CD, DVD o cualquier unidad extraíble, que se haya utilizado en el equipo asignado por la entidad o personal.
- u. En lo que respecta a la información que se encuentre contenida en medios físicos, los teletrabajadores están en la obligación de dar estricto cumplimiento a los lineamientos de Seguridad de la Información establecidos por la Entidad y que a continuación se relacionan:
 - Almacenar los documentos bajo llave mientras no se estén utilizando.
 - Dar cumplimiento a las medidas de seguridad adoptadas por el Instituto a través del Grupo de Gestión de Atención al Ciudadano y Gestión Documental

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

y que se deben aplicar en el traslado de los documentos de un lugar a otro, bien cuando ello se aplique al interior o al exterior de la entidad.

- Llevar a cabo la destrucción de los documentos, para lo cual será necesario romperlo o triturarlo con el objeto de evitar que la pieza documental se arroje de manera completa al contenedor o papelera y sea reutilizada para labores domésticas que de alguna manera ponga en riesgo la información institucional.
- No dejar los documentos en tránsito desentendidos en el lugar o lugares en los que se ejecutan las funciones de Teletrabajo.

- **Excepciones:**

Cualquier forma de Teletrabajo debe estar aprobada formalmente por la Gerencia General y se debe llevar un control de qué usuarios trabajan bajo esta modalidad. Toda excepción a los lineamientos, debe ser justificada por el Jefe o Supervisor de Contrato y autorizada por el Comité de Teletrabajo de la entidad o quien haga sus veces.

7. POLÍTICA DE SEGURIDAD EN LOS RECURSOS HUMANOS

- **Dominio:** A.7. Seguridad del Recurso Humano.
- **Objetivo:** Asegurar que los empleados y contratistas comprendan sus responsabilidades y son idóneos en los roles para los que se consideran.
- **Alcance:** La presente política establece que todos los Funcionarios, Contratistas, Proveedores y Terceros, deben dar cumplimiento a las Políticas de Seguridad y Privacidad del ICA.
- **Lineamientos:**
El Instituto Colombiano Agropecuario ICA, reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con personal calificado, deberá garantizar que la vinculación de los candidatos, aspirantes, contratista, proveedores y terceros cumplan con los procesos de verificación necesarios, el cual estará orientado al perfil, a las funciones y/u obligaciones que deben desempeñar para desarrollar su labor.

7.1. ANTES DE LA VINCULACIÓN

Asegurar que los empleados y contratistas comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran:

- a. El Grupo de Gestión de Talento Humano y Gestión Contractual de acuerdo a su competencia, deben realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por los candidatos o aspirantes a ocupar un cargo en ICA, antes de su vinculación definitiva.
- b. El Grupo de Gestión de Talento Humano debe convocar a los Funcionarios de la Entidad, para que asistan a las charlas inducción y reintroducción donde se darán a conocer las Políticas de Seguridad de la Información.
- c. Se debe incorporar dentro de las minutas contractuales, cláusulas referentes a:

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- Estricto cumplimiento del Manual de Políticas de Seguridad y Privacidad de la Información definida por la Entidad.
 - Confidencialidad de la Información.
 - Clausulas de Tratamiento de Datos Personales.
- d. El Grupo de Gestión de Talento Humano y Gestión Contractual de acuerdo a su competencia, debe realizar verificaciones de los antecedentes de todos los candidatos o aspirantes, se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes y deben ser proporcionales a los requisitos de la entidad, a la clasificación de la información a que va a tener acceso, y a los riesgos percibidos.
- e. El personal provisto por terceros, debe garantizar el cumplimiento de los acuerdos y/o Cláusulas de Confidencialidad y de aceptación de las Políticas de Seguridad de la Información de la Entidad antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica de la misma.
- a. En el Manual de Funciones de la Entidad, se deberá incluir un capítulo del estricto cumplimiento a las Políticas de Seguridad y Privacidad de la Entidad por parte de los Funcionarios.
- **Excepciones:**
Las excepciones establecidas por Ley cuando aplique el caso, previa notificación de las mismas a la Oficina de Tecnologia de Información y/o Líder de Seguridad de la Información.

7.2. DURANTE DE LA VINCULACIÓN

Asegurar que todos los Funcionarios, Contratistas, Proveedores y/o Terceros, tomen conciencia de sus responsabilidades de Seguridad y Privacidad de la información, considerando el cumplimiento de los siguientes lineamientos:

- a. El Grupo de Gestión de Talento Humano, deberá notificar cualquier novedad del personal en el que se encuentre en situaciones administrativas tales como: (licencias, vacaciones, traslado, retiro, entre otras); para que la OTI y las áreas que administran los aplicativos de la entidad, procedan para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados.
- b. El Grupo de Gestión Contractual, deberá notificar cualquier novedad del contratista Proveedores y Tercero tales como: (ceder contrato, terminación bilateral, terminación unilateral, entre otras), referente a su vinculación o relación comercial con la entidad para que la OTI y las áreas que administran los aplicativos de la entidad, procedan para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados.
- c. La Oficina de Tecnologia de Información – OTI, deberá diseñar y ejecutar de manera periódica (minimo una vez la año) un Plan de Cultura y Sensibilización de la Información a todos los Funcionarios, Contratistas, Proveedores y Terceros, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.
- d. Se debe contar con un proceso formal y comunicado para emprender acciones contra Funcionarios, Contratistas, Proveedores y/o Terceros que hayan cometido una violación a la Seguridad de la Información de la Entidad.

- e. Si se realizan cambios en las funciones y/o actividades en los Funcionarios, Contratistas, Proveedores y/o Terceros, estos deberán ser notificados la Oficina de Tecnología de Información y/o Líder de Seguridad de la Información.
- f. Política de Cultura y Sensibilización en Seguridad de la Información:
 - **Dominio:** A.7.2.2 Toma de conciencia, educación y formación en la Seguridad de la Información.
 - **Objetivo:** Asegurarse de que los Funcionarios, Contratistas, Proveedores, Terceros, tomen conciencia de sus responsabilidades de Seguridad de la Información y las cumplan.
 - **Alcance:** La presente política aplica para todos los Funcionarios, Contratistas, Proveedores, Terceros, los cuales deben participar activamente en los programas de sensibilización que realiza la entidad para SGSI.
 - **Lineamientos:**
Se debe dar cumplimiento de los siguientes lineamientos:
 - a. Se debe sensibilizar y divulgar a través de los medios establecidos por la entidad sobre la Seguridad de la Información, en donde a cada uno de los Funcionarios, Contratistas, Proveedores, Terceros, deben participar activamente en los Programas o Planes de Cultura y Sensibilización en Seguridad de la Información desarrollados por la Oficina de Tecnología de Información, y de acuerdo al contenido debe ser interiorizado y aplicado según corresponda su rol y responsabilidad dentro de la Entidad.
 - b. Para realizar el contenido de los Programas o Planes de Cultura y Sensibilización de Seguridad de la Información deben enmarcarse en tres (3) fases:
 - **Diseño.** Deben ser diseñados teniendo en cuenta la misión de la Entidad, identificación de las necesidades y prioridades (verificación de Incidentes de Seguridad), elaboración de indicadores o métricas de desempeño que permitan generar resultados.
 - **Desarrollo.** Elaborar material de entrenamiento en el que se pueda emplear una buena pedagogía para la difusión de los temas de Seguridad y este debe ser sometido a aprobación por la Alta Dirección, antes de la puesta en marcha.
 - **Implementación.** Socializar el programa o Plan de Cultura Sensibilización de Seguridad de la Información de la Entidad que fue diseñado y desarrollado al igual que emplear los indicadores o métricas para evaluar el desempeño del Programa o Plan.
 - **Excepciones:**
Las excepciones establecidas por Ley cuando aplique el caso, previa notificación de las mismas a la Oficina de Tecnología de Información y/o Líder de Seguridad de la Información.

7.3. DESPUES DE LA VINCULACIÓN

- a. El Funcionarios, Contratistas, Proveedores y/o Terceros, deberá mantener la confidencialidad de la información después de su vinculo laboral o relación comercial con la entidad, de acuerdo a lo establecido en el manual de funciones y/o obligaciones contractuales.
 - b. La Oficina de Tecnologia de Información – OTI y las áreas que administren las aplicaciones, deberá suspender los Servicios de TI a los Funcionarios, Contratistas, Proveedores y/o Terceros que no tengan ningún tipo de vinculación con la Entidad, siempre y cuando este sea informado por el Grupo de Gestión de Talento Humano y el Grupo de Gestión Contractual por le canal que estime el ICA.
 - c. El Funcionarios, Contratistas, Proveedores y/o Terceros, deberá entrega los elementos tales como: (computador, GPS, archivo físico y digital, entre otros) para que la entidad le genere el paz y salvo.
- **Excepciones:**
Las excepciones establecidas por Ley cuando aplique el caso, previa notificación de las mismas a la Oficina de Tecnologia de Información y/o Líder de Seguridad de la Información.

8. POLÍTICA DE GESTIÓN DE ACTIVOS

- **Dominio:** A.8 Gestión de Activos.
- **Objetivo:** Establecer los lineamientos para identificar los activos Institucionales y definir las responsabilidades de protección apropiadas.
- **Alcance:** La presente política aplica para todos los Funcionarios, Contratistas, Proveedores y/o Terceros o que por su rol, tengan bajo su propiedad o custodia, activos de información.
- **Lineamientos:**
Se debe dar dar cumplimiento a los siguientes lineamientos:

8.1. RESPONSABILIDAD POR LOS ACTIVOS

8.1.1. Inventario de Activos

El Líder u Oficial de Seguridad de la Información o quien haga sus veces, es el encargado de llevar a cabo funciones de orientación y apoyo en cada uno de los Procesos Institucionales a través de las actividades para la identificación de activos de información, con el objeto de contribuir a que los inventarios de activos de cada una de las dependencias del ICA, deben encontrarse con las Tablas de Retención Documental como con los criterios establecidos en el procedimiento de Identificación, Valoración y Clasificación de Activos de Información, asegurando que:

- a. Toda la información deberá ser clasificada por:
 - Su nivel criticidad.
 - Su valor.
 - Disposiciones de normativad legal.
 - Las indicaciones de los propietarios de la información como por la Entidad.
- b. La Matriz de identificación y clasificación de activos de información debe permanecer en un repositorio seguro con acceso restringido.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- c. La Matriz de identificación y clasificación de activos de información se debe actualizar por lo menos una vez al año y/o cuando se presenten:
 - Cambios en la tabla de retención documental.
 - Retiro de activos de información.
 - Adquisiciones de nuevos activos de información.
- d. Mantener actualizado el inventario de los activos de información tecnológicos de la entidad tales como (redes, servidores, aplicaciones, dispositivos de red, estaciones de trabajo, teléfonos IP, impresoras, portátiles y licencias de software), así como aires acondicionados, generadores de energía, unidades de potencia (UPS).
- e. Los activos de información deberá estar publicados de acuerdo a la legislación actual vigente.
- f. Los activos de información tanto físico como digitales deberán estar rotulados de acuerdo a la Guía de Clasificación de información definida por la Entidad.

8.1.2. Propiedad de los Activos de Información

Quien ejerza las funciones de propietario de activos de información en el Instituto deberá:

- a) Procurar que todos los activos de información bajo su propiedad se encuentren debidamente inventariados.
- b) La Entidad, deberá identificar cuales son los propietarios de la información y asignar repsonsabilidades para:
 - Definición de controles para la protección de los activos de Información.
 - Mantenimiento de los controles definidos para la protección de los activos de Información.
 - Seguimiento y/o monitoreo de los custodios de los activos de Información para la verificación de la aplicación de los controles definidos.
- c) Velar porque los activos de información bajo su propiedad se encuentren debidamente inventariados.
- d) Verificar que los activos de información sean clasificados y protegidos de acuerdo al:
 - Su nivel criticidad.
 - Su valor.
 - Disposiciones de normativad legal.
- e) Revisar al menos una vez al año o cuando ocurra un cambio significativo, las restricciones y clasificaciones de acceso a los activos de información.
- f) Verificar que los procesos de eliminación o destrucción no permitan la exposición de los activos de información a terceros.
- g) Cuando se realicen actividades de archivo, estas no pueden ser realizadas fuera de las oficinas o dependencias responsable de estos activos de infromación, ni pueden ser alojadas en lugares de transito de personal como pasillos, salas de reunión, comedor,

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

baños y cocina; dado que se está incumpliendo con la Confidencialidad, Integridad y Disponibilidad de la Información.

8.1.3. Uso Aceptable de los Activos de Información

- Todos los Funcionarios, Contratistas, Proveedores y/o Terceros o que por su rol, tengan bajo su propiedad o custodia, activos de información de la Entidad, deben acatar y dar estricto cumplimiento a lo prescrito en la Guía de Uso Aceptable de los Activos de Información.¹³.
- Todos los Funcionarios, Contratistas, Proveedores y/o Terceros; no deben usar imágenes o fotos en la herramientas colaborativas que no sean institucionales y avalas por el Manual de Imagen Corporativa definida por la Entidad.

8.1.4. Devolución de los Activos de Información

- Todos los Funcionarios, Contratistas, Proveedores y/o Terceros, debe hacer devolución del activo de información bajo su responsabilidad, una vez finalizado el vínculo con la Entidad.
- Una vez finalizado el vínculo con la Entidad, el Jefe de Área o Supervisor del Contrato (según sea el caso) deberá solicitar a la Mesa de Ayuda, la aplicación de las herramientas de borrado seguro sobre la información Institucional alojada en los equipos asignados ejecución para la ejecución de sus funciones u obligaciones contractuales, previo a la generación del backup de la Información que allí se aloje.
- El Jefe de Área o Supervisor del Contrato (según sea el caso), debe asegurarse que los equipos que se encuentren bajo su custodia y estos sean:
 - Devueltos al almacén de la Entidad.
 - Reasignado a un Servidor Público, Contratista, Proveedor o Tercero de la Entidad.
 - Traspasados a otra Área, Dependencia o Seccional de la Entidad.
 - Destruídos o dar de baja.
 - Donados a Terceros.

Se les genere el borrado seguro a los equipos de la entidad, previo a la generación del backup de la Información que allí se aloje.

8.2. POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

8.2.1. Clasificación de la Información

- Los únicos niveles de clasificación de información establecidos en el ICA son: Pública, Uso Interno, Confidencial (Sensible) y Reservada¹⁴, por tanto, el dueño del proceso está obligado

¹³ Ver Guía de uso aceptable de activos

¹⁴ Ver Procedimiento Identificación y Clasificación de Activos del ICA

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

a clasificar y dar el tratamiento adecuado a la información de acuerdo a estos niveles y siguiendo los lineamientos de la Guía de Clasificación y Rotulado de Información del ICA¹⁵.

- b. Los propietarios de los activos de información, están obligados a clasificar y dar tratamiento adecuado a la misma, de acuerdo a los niveles definidos en la Guía de Clasificación y Rotulación de la Entidad.

8.2.2. Etiquetado de la Información

- a. Cada activo debe poseer un etiquetado en donde se identifique el nivel de clasificación asignado. El etiquetado debe ser utilizado para aquella información que se encuentre contenida tanto en medio físico, electrónico y digital.

8.2.3. Manejo de Activos de Información

- a. Para el manejo, procesamiento, almacenamiento y comunicación de la información se debe considerar los niveles de clasificación definidos en la Guía de Clasificación y Rotulación de la Entidad.
- b. La eliminación y destrucción de la información debe realizarse de acuerdo a su nivel de clasificación y siguiendo los lineamientos de la Guía de Clasificación y Rotulado de Información del ICA¹⁶.
- c. Política de Integridad:
 - En lo que respecta a todas las aplicaciones de la Entidad, se deben implementar mecanismos cuyo objeto sea el de propender por la Integridad del Activo de información con base en el nivel de clasificación y el nivel de evaluación de Riesgo identificado.
 - La Oficina de Tecnología de Información de la Entidad, será la única dependencia autorizada para realizar copia de Seguridad del Software Original.
 - El software proporcionado por la Entidad, no pueden ser copiados o suministrados a terceros.

- **Excepciones:**

Cualquier excepción debe ser autorizada por La Oficina de Tecnología de Información y/o el Líder u Oficial de Seguridad de la información de la Entidad.

8.3. POLÍTICA DE MANEJO DE MEDIOS

8.3.1. Gestión de Medios Removibles

- a. Cualquier dispositivo de almacenamiento de información de propiedad de la Entidad, se constituye en un activo de información, por tanto, el ingreso, uso, movilización y salida, debe ser previamente autorizado por la (s) dependencia (s) competente (s).

¹⁵ Ver Guía de Clasificación y Rotulado de Información del ICA

¹⁶ Ver Guía de Clasificación y Rotulado de Información del ICA

- b. Se debe mantener un inventario actualizado de los dispositivos de almacenamiento de información removible de la entidad como (Cintas de Backup, Discos Duros, USB, GPS, entre otros) y de sus propietarios.
- c. Los propietarios y custodios de los medios removibles, deben asegurarse que éstos no queden desatendidos debido a que pueden ser susceptibles a pérdida o robo.
- d. La protección a los medios debe hacerse de acuerdo al nivel de clasificación definidos por la entidad para la información contenida en los mismos.
- e. El uso de dispositivos de almacenamiento personales o de la Entidad como (USB, DISCO DUROS EXTERNOS, ENTRE OTROS) estan prohibidos y en caso de ser requerido no puede contener información de la Entidad.
- f. Todos los medios de almacenamiento removibles, deben ser almacenados en un ambiente seguro de acuerdo a las especificaciones de los fabricantes.
- g. Si ya no se requiere de la información contenida en los medios removibles de la Entidad, se deberá aplicar el procedimiento de borrado Seguro definido para que estos puedan ser reutilizados.

8.3.2. Disposición de los Medios

- a. Una vez terminado el ciclo de vida útil de un determinado medio de almacenamiento, la información allí contenida, debe ser eliminada de manera segura de acuerdo con los procedimientos formales previamente establecidos por la Entidad, previo a la generación de backup de la información que allí se contenga.
- b. Se debe tener en cuenta el procedimiento para la disposición de dispositivos tecnológicos RAES para los equipos y medios de almacenamiento que se den de baja.
- c. La Entidad debe asegurarse que se implemente los controles establecidos en el Procedimiento de Disposición Segura de Medios definidos por la Entidad, cuando se vayan a:
 - Destruídos o dar de baja.
 - Donados a Terceros.
- d. Para la eliminación de medios de almacenamiento se debe generar un registro mediante acta con el fin de mantener registros para efectos de auditorias.

8.3.3. Transferencia de Medios Físicos

- a. El transporte de los medios de almacenamiento de la Entidad, debe darse de acuerdo a la clasificación de la información contenida en éstos, para ello se deben:
 - Utilizar servicios de mensajería confiables.
 - Verificarlos tipos de monitoreo para la transferencia de medios físicos.
 - Verificar si se realizan técnicas de embalaje.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- Llevar un registro correspondiente de los medios físicos que son transportados.

- **Excepciones:**

Cualquier excepción debe ser autorizada por la Oficina de Tecnología de Información y el Líder u Oficial de Seguridad de la Información.

9. POLÍTICA DE CONTROL DE ACCESO

- **Dominio:** A.9 Control de Acceso

- **Objetivo:** Establecer los lineamientos para evitar el acceso no autorizado a la información y a las instalaciones de procesamiento de información del ICA.

- **Alcance:** La presente Política aplica para todos los Funcionarios, Contratistas, Proveedores y/o Terceros o que por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información del ICA.

- **Lineamientos:**

Se debe dar cumplimiento a los siguientes lineamientos:

9.1. POLÍTICA REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO

- Los Sistemas de Información de la Entidad, debe contar con mecanismos para el control de acceso lógico.
- Establecer medidas de control de acceso para los Funcionarios, Contratistas, Proveedores y/o Terceros, a través de mecanismos de identificación, autenticación y autorización de acceso, a nivel de Red, Sistemas de Información, Bases de Datos y Servicios de TI de acuerdo con los perfiles y cargos establecidos en la Entidad.
- La Entidad, proporcionará a los Funcionarios, Contratistas, Proveedores y/o Terceros, los recursos tecnológicos necesarios para que puedan desempeñar las funciones de una manera eficaz.
- No se permite conectar o instalar, de manera cableada o inalámbrica a la red LAN de la Entidad, cualquier dispositivo fijo o móvil como: (impresoras personales, computadores de escritorio, portátiles, Tablet, enrutadores, switches, agendas electrónicas, Smartphone, Access point, amplificadores de señal, entre otros) que no sean autorizados por la Oficina de Tecnología de Información y Líder de Seguridad de la Información.
- El acceso a la red interna por parte de un proveedor, debe estar autorizada por parte de la Oficina de Tecnología de Información y el Líder de Seguridad de la Información mediante los mecanismos definidos por la Entidad.
- El tiempo de inactividad de una sesión de usuario, debe activarse de acuerdo a la Política del Directorio activo.
- Todas las contraseñas de usuarios privilegiados o super usuarios (Administrador), se deben cambiar de acuerdo al análisis previo realizado por la Oficina de Tecnología de Información y el Oficial de Seguridad de la Información; y para ello se debe convocar a Comité de Cambios donde se aprobara y se programará el cambio.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- h) Todas las contraseñas de usuarios privilegiados o super usuarios (Administrador), se deben proteger y almacenar bajo la custodia del Jefe de la Oficina de Tecnología de Información.
- i) El Grupo de Gestión de Talento Humano y Gestión Contractual, deberán informar a los Administradores de los Sistemas de Información y/o Aplicaciones de la Entidad, lo referente a novedades que surjan para los Funcionarios, Contratistas, Proveedores y Terceros, con el objeto de que dichos usuarios sean deshabilitados o suspendidos oportunamente, según fuere el caso.
- j) Los controles de autenticación deben ser confiables, para lo cual la entidad adelantarán los mecanismos o procedimientos que ello amerite.
- d. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n):
 - Tendrá la responsabilidad de custodiar dichos programas y por virtud de su función no deberá pertenecer al equipo de desarrollo.
 - Llevar un registro actualizado de todos los programas fuentes en uso, indicando entre otros, el nombre del programa, programador, analista responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
 - Restringir el acceso a los códigos fuente de los programas, asegurándose de que solamente los ingenieros desarrolladores tengan acceso.
 - Mantener los códigos fuente de los programas en el servidor o repositorio de fuentes.
 - Asegurarse de que el código y las bibliotecas fuentes del programa sean manejadas con los procedimientos establecidos.
 - Actualizar las bibliotecas de fuentes del programa, así como la emisión de las fuentes para los programadores sólo se deben realizar después de haber recibido la autorización del Profesional encargado del Equipo de Desarrollo.
 - Mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa.
 - Realizar el mantenimiento y copiado de las bibliotecas fuentes del programa está sujeto a procedimientos estrictos de control de cambios.
 - Asegurarse que los desarrolladores deben aplicar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
 - Asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada, conforme a lo estipulado en el procedimiento de backup.

9.2. POLÍTICA DE GESTIÓN DE ACCESO A USUARIOS

- a) Quien(es) ejecute (n) el rol de Lider de Servicios Tic's o quien haga de sus veces, debe (n):
 - Dar cumplimiento a la aprobación o rechazo de los permisos de conexión remota o VPN, previamente otorgado por el Jefe de Tecnologías de la Información de la Entidad o quien haga

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

sus veces, En lo que respecta a la solicitud de acceso lógico que efectúen los Funcionarios, Contratistas, Proveedores y/o Terceros, esta debe ir respaldada, soportada y avalada por el Jefe inmediato o Supervisor del contrato según sea el caso.

- Asegurar que las redes inalámbricas cuenten con métodos de autenticación que eviten accesos no autorizados.
 - Velar por el cumplimiento del procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red.
 - Realizar una verificación de los controles de acceso de los Funcionarios, Contratistas, Proveedores y/o Terceros en la periodicidad que se establezca para ello, a fin de cerciorarse que dichos usuarios acceden solamente a los recursos autorizados para la realización de sus tareas, funciones u obligaciones; así mismo debe realizar la des habilitación o suspensión de aquellos usuarios que contando con acceso activo, presenten cualquier tipo de novedad que así lo amerite.
 - Asignar los privilegios a los usuarios de acuerdo con los roles y responsabilidades, estos privilegios se extenderán solo cuando sea necesario y deben contar con autorización del Jefe o Supervisor del Contrato y visto bueno de la Oficina de Tecnología de Información y el Líder u Oficial de Seguridad de Información.
 - Cancelar los derechos de acceso a la información a todos los Funcionarios, Contratistas, Proveedores y/o Terceros que no tengan vinculación con la Entidad.
- b. El acceso a los recursos de red, serán controlados por medio de la creación de usuarios y password correspondientes, con el fin de prevenir el acceso no autorizado.
 - c. Los Funcionarios, Contratistas, Proveedores y/o Terceros de la Entidad, tenderán solamente acceso a los servicios de red y Sistemas de Información para los cuales fueron autorizados y que son vezarios para realizar sus funciones.
 - d. Los Funcionarios, Contratistas, Proveedores y/o Terceros de la Entidad, deben reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece en la herramienta de Mesa de Ayuda como incidente de Seguridad de Información.
 - e. Asignación de los permisos de uso de VPN para Funcionarios, Contratistas, Proveedores y/p Terceros de la Entidad, deben ser solicitados mediante el diligenciamiento del Formato de solicitud de VPN, y previo aprobación del Oficial de Seguridad de la Información y Jefe de Oficina de Tecnología de Información – OTI. El uso de la VPN es únicamente a los servicios solicitados y autorizados y no se pueden asignar premisos sin previa validación.
 - f. Para asignar permisos a un Proveedor sobre la Plataforma Tecnológica y/o Servicios de red, debe ser solicitados al Oficial de Seguridad de Información y Jefe de la Ofician de Tecnología de Información – OTI, con el fin de evaluar de riesgos y la pertinencia de autorizar o rechazar la solicitud; no se pueden asignar premisos sin previa validación.
 - g. Cuando un Proveedor requiere creación de usuario de dominio para realizar consultas propias de la actividad definida en el Contrato, debe ser solicitados al Oficial de Seguridad de Información y Jefe de la Ofician de Tecnología de Información – OTI, con el fin de evaluar de riesgos y la pertinencia de autorizar o rechazar la solicitud; no se pueden asignar premisos sin previa validación.

- h. Se requiere hacer monitoreo permanente a los usuarios que tiene permisos de VPN, por parte del administrador de la Plataforma Tecnológica, este debe reportar de forma periódica el comportamiento de las mismas, y si se llega a evidenciar un mal uso, debe notificarse de forma inmediata.
- i. Cuando un Funcionarios, Contratista, Proveedor y/o Tercero de la Entidad; genera un Incidente de Seguridad por el mal uso de la de los recursos compartidos, usuario de dominio, VPN, entre otros; se debe suspender de forma inmediata el servicio de TI.

9.3. POLÍTICA DE RESPONSABILIDAD DE LOS USUARIOS

- a) Todos los Funcionarios Contratistas, Proveedores y Terceros, debe bloquear el equipo en caso de ausentarse del puesto de trabajo, con el fin evitar el acceso no autorizado a cualquier aplicación de la Entidad.
- b) Todos los Funcionarios Contratistas, Proveedores y Terceros, debe apagar el equipo en caso de ausentarse de las instalaciones, con el fin evitar el acceso no autorizado a cualquier aplicación de la Entidad.
- c) Todos los Funcionarios Contratistas, Proveedores y Terceros bajo ningún motivo deberá prestar su usuario y contraseña para acceder al equipo y/o aplicaciones de la Entidad.
- d) Es responsabilidad de los Funcionarios Contratistas, Proveedores y Terceros, el buen manejo y uso de los recursos de la Entidad, así como de las claves que le han sido asignadas.
- e) Todo Funcionarios, Contratistas, Proveedores y/o Terceros, que con ocasión a sus tareas u obligaciones con la Entidad, tengan acceso a los Sistemas de Información, deben utilizar un nombre de usuario de dominio ICA, asignándole para ello una contraseña que cumpla con las políticas de seguridad adoptadas por la entidad, la cual deberá ser personal e intransferible.
- f) Para la creación de contraseñas seguras, los Funcionarios, Contratistas, Proveedores y/o Terceros, deben:
 - Escoger contraseñas que sean difíciles de descifrar y que no contengan información relacionada con su trabajo o vida personal, por lo cual no se debe utilizar la siguiente información: Números de identificación personal, números de teléfono, nombres de los conyugues, direcciones postales, nombres propios, lugares conocidos o términos técnicos.
 - Combinar palabras (Mayúsculas o minúsculas), puntuación y números, de tal modo que arroje como resultado una contraseña alfanumérica con símbolos especiales.
 - Transformar una palabra común utilizando un método específico.
 - Crear acrónimos (siglas que forman una palabra).
 - Crear contraseñas que contengan como mínimo 8 dígitos y cambiarla en intervalos de 60 días.
 - Los Intentos no exitosos de ingreso de la contraseña, después de un número veces determinadas y previamente establecidas por la entidad, traerá consigo el bloqueo del usuario

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

de manera inmediata para lo cual se deberá solicitar el desbloqueo a quien ejecute el rol de Administrador de control de acceso lógico.

- g. Las contraseñas que sean suministradas a través de correo electrónico por quien ejecute el rol de administrador de un determinado Sistema, deben ser cambiadas de manera inmediata tan pronto como la misma sea recibida por parte de la persona a quien se le han asignado los permisos, siguiendo para ello con los protocolos de seguridad de la información y las buenas prácticas de uso de contraseña aludidas.
- h. Las contraseñas no deben ser almacenadas en formato legible, papeles, agendas de trabajo, computadores sin sistemas de control de acceso o cualquier otro lugar donde las personas no autorizadas puedan encontrarlas.
- i. Si algún Funcionarios, Contratistas, Proveedores y/o Terceros, sospecha (n) de la pérdida de confidencialidad de alguna de sus claves, debe (n) notificar de manera escrita el evento o incidente de seguridad de la información (según sea el caso) a la mesa de ayuda del instituto, a fin de tomar las medidas pertinentes de cuidado de la información y supervisar la generación de nuevas credenciales siguiendo los lineamientos del Procedimiento Gestión de Incidentes de Seguridad de la Información de la Entidad.

9.4. POLÍTICA CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

El instituto Colombiano Agropecuario – ICA, deberá asegurar, preservar y garantizar el control de acceso a los Sistemas y/o Aplicaciones Institucionales, para lo cual deberá dar cumplimiento a los siguientes parámetros de Seguridad:

- a. El acceso a los Sistemas de Información y Servicios Tecnológicos de la Entidad, a través del uso de usuario de dominio ICA, debe estar restringido y delimitado a las tareas, funciones, responsabilidades u obligaciones que ejecuten los Funcionarios, Contratistas, Proveedores y/o Terceros de la Entidad.
- b. El propietario de la aplicación y de la información, deberá identificar y documentar explícitamente la Sensibilidad o Confidencialidad de la Información contenida en los Sistemas Información y/o Aplicaciones de la Entidad.
- c. Los propietarios de los activos de Información, deben autorizar los accesos a sus Sistemas de Información y/o Aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la Clasificación de la Información
- e. No está permitido para ningún Funcionarios, Contratistas, Proveedores y/o Terceros, acceder a los Sistemas de Información y/o Aplicaciones para el cual no haya sido autorizado.
- f. Quien(es) ejecute (n) el rol de Líder de Servicios Tic's o quien haga de sus veces, debe (n):
 - Asegurar que los grupos de servicios de información, usuarios y Sistemas de Información sean segmentados en redes.
 - Asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.
 - Establecer los controles de acceso a los ambientes de producción de los Sistemas de Información.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- Asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción de la Entidad.
 - Restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
 - Asegurar que en lo que respecta a los Sistemas Operativos, Sistemas de Información y/o Aplicaciones de la Entidad, se bloquee la sesión automáticamente, después de determinados minutos de inactividad, previamente establecidos.
 - Garantizar que los Sistemas de Información y/o Aplicaciones de la Entidad, tenga establecidos "Time Out" después de determinados minutos de inactividad previamente establecidos. Esto debe estar tanto para las Aplicaciones locales y web.
- g. En lo que respecta a la autorización y continuidad en el uso de los usuarios de los aplicativos, deberá ser responsabilidad de cada una de las Áreas, Dependencias y/o Procesos de la Entidad.
- h. Se debe dar cumplimiento a la Metodología de desarrollo de Software definida por la Entidad.
- **Excepciones:**
Cualquier excepción a los lineamientos, debe ser justificada por quien ejecute el rol de Líder de Servicios Tic's y/o quien ejecute el rol de Administrador de programas fuentes debe, según aplique el caso; debidamente validada y aprobada por el Jefe de la Oficina de Tecnología de Información y el Líder u Oficial de Seguridad de la Información de la Entidad.

10. POLÍTICA DE CRIPTOGRAFIA

- **Dominio:** A.10.1 Controles Criptográficos.
- **Objetivo:** Establecer los lineamientos para asegurar el uso apropiado y eficaz de la criptografía a fin de proteger la confidencialidad, la autenticidad y/o la integridad de la información.
- **Alcance:** La presente política aplica para todos los Funcionarios o contratistas del ICA que hagan uso de controles criptográficos, cuando se requiera.
- **Lineamientos:**
 - a. Quien(es) ejecute (n) el rol de Lider de Servicios Tic's o quien haga de sus veces, debe (n):
 - Identificar los Sistemas de Información y/o Aplicaciones en los que se considere necesario hacer uso de controles criptográficos para proteger la información. El uso de controles criptográficos quedará determinado por el análisis de riesgos de los Sistemas de Información, así como el nivel o fortaleza de los mecanismos de cifrado a utilizar (algoritmos, longitudes de clave mínimas, etc.).
 - Documentar los pasos necesarios para el registro, generación, distribución, almacenamiento, recuperación, renovación, revocación y destrucción de las claves criptográficas y debe mantener un registro de actividad que evidencie su cumplimiento y permita su posterior revisión o auditoría.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- b. Los aspectos importantes que se deben tener en cuenta para el uso de los controles criptográficos son:
- Para la Información Sensible y/o Confidencial de la Entidad.
 - Para las líneas de comunicación por donde se almacena, procesa y transmite la información Confidencial.
 - Las herramientas y mecanismos de cifrado definidas por la Entidad.
 - Para cumplimiento de los Requisitos legales¹⁷.
- c. Se debe realizar una gestión segura de todas las claves criptográficas, por parte de quienes requieran su uso, con el objeto de garantizar la eficacia de los controles criptográficos.
- d. Cuando se utilicen mecanismos de cifrado simétrico o de clave privada (compartida), se debe garantizar la confidencialidad en el intercambio de las claves (por un canal seguro o cifradas mediante mecanismos de cifrado asimétrico).
- e. Cuando se utilicen mecanismos de cifrado asimétricos o de clave pública/privada, se debe:
- En el intercambio de claves públicas, la autenticidad e integridad de las mismas deben quedar avaladas por una autoridad de certificación de confianza, bien sea interna (PKI interna) o externa.
 - En el caso de uso de servicios criptográficos de terceros, los acuerdos de prestación de servicios deben cubrir aspectos de responsabilidad civil, fiabilidad y seguridad del servicio y tiempos de provisión.
- f. Los tokens de Seguridad suministrados a los Funcionarios y/o Contratistas, para realizar consulta, modificación, transmisión de información, pagos, entre otros fines, por lo tanto:
- Se debe guardar en un lugar seguro bajo llave, libre de acceso al mismo por personal no autorizado.
 - No se debe dejar desatendido cuando el usuario se encuentre ausente del puesto de trabajo.
 - No se puede prestar el token ni suministrar la clave bajo ninguna circunstancia.
 - No se debe utilizar fuera de las Instalaciones de la Entidad.
 - No se debe utilizar en horario no laboral sin previa autorización escrita del Jefe o Supervisor de Contrato.
 - Si el token se bloquea por intentos fallidos por el uso del mismo se debe solicitar el desbloqueo a la Entidad "Administradora" del mismo, previo a solicitud en la Mesa de Ayuda de la Oficina de Tecnología de Información, para autorizar el Servicio remoto mediante aprobación del Líder u Oficial de Seguridad de la Información.

¹⁷ Ver Ley 527 de 1999

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- g. Se debe contar con un algoritmo criptográfico para el cifrado de datos sensibles, siempre que se garanticen los tres pilares de la Seguridad de la Información.
- h. Se debe contar con mecanismos de autenticación por usuario y contraseña siguiendo la Política de control de acceso a la información de la Entidad.

- **Excepciones:**

Cualquier excepción debe ser autorizada por la Oficina de Tecnologías de la Información y el Líder u oficial de Seguridad de la Información de la Entidad.

11. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

- **Dominio/ Control:** A.11.1 Áreas Seguras
- **Objetivo:** Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información del ICA.
- **Alcance:** La presente política aplica para todos los Funcionarios, Contratistas, Proveedores y/o Terceros o que por su rol tengan acceso físico a las instalaciones y áreas seguras del ICA.
- **Lineamientos:**
Se debe dar cumplimiento a los siguientes lineamientos:

11.1. ÁREAS SEGURAS

11.1.1. Perímetros de Seguridad Física

Las áreas y dependencias del Instituto Colombiano Agropecuario – ICA, deben encontrarse protegidas por barreras y controles físicos para lo cual deben estar monitoreadas y supervisadas con circuito cerrado de cámaras. Para la Entidad se definen las siguientes áreas seguras:

- a. **Datacenter:** corresponde al centro de procesamiento de datos en donde se albergan los sistemas de información (aplicaciones, bases de datos), los componentes de telecomunicaciones y los sistemas de almacenamiento (servidores físicos y virtuales).
- b. **Centros de Cableado:** áreas de unión central que se usan para conectar los dispositivos de la red del área local (LAN) el cual alberga paneles de conexión, Hubs de cableado, Switches, Router, Puentes, Rack, Access Point, entre otros.

Cuartos de Suministro: áreas en donde se ubican los servicios de suministro como: las UPS y la planta eléctrica.
- c. **Archivo Físico Central:** áreas en donde se administran, custodian y conservan los documentos físicos con valor administrativo, legal, permanente, histórico entre otros, para el Instituto que son transferidos por las diferentes oficinas.
- d. **Archivo Físico de Gestión:** Hace referencia a aquella documentación todavía en trámite que conservan las oficinas así como a aquella que aun después de finalizado el procedimiento administrativo, está sometida a uso continuo y consulta administrativa por las mismas oficinas, aplicando para ello lo dispuesto en las tablas de retención documental.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

e. **Oficinas:** todas aquellas dependencias y áreas de la Entidad, que por sus competencias funcionales manejan información Sensible y/o Confidencial, serán consideradas “Áreas Seguras”, para lo cual deben adoptarse los mecanismos tendientes para asegurar dicha información. Por todo lo expuesto, se deben adoptar por lo menos los controles definidos en el “*Numeral 11.1.2. Controles de Acceso Físico*”.

- **Excepciones:**

Cualquier excepción debe ser autorizada por el Líder u Oficial de Seguridad de la información.

11.1.2. Controles de Acceso Físico

- a. Impedir que aquellas áreas cuyas ventanas den al exterior por su ubicación, permitan de alguna manera (al menos mínima) la visibilidad hacia el interior de la Entidad, para lo cual es necesario que las mismas deban estar cerradas con llave.
- b. Implementar el uso de chapas de seguridad en las puertas de las áreas seguras con el objeto de que permanezcan cerradas.
- c. Los privilegios de acceso a las áreas seguras del ICA, deben ser definidos y otorgados por el profesional u oficina encargada del área segura, para ello debe tener en cuenta los siguientes tipos de usuario:
 - Profesionales que trabajan regularmente en las áreas seguras.
 - Profesional de soporte que requiere acceso periódico.
 - Visitantes (Funcionarios, Contratistas, Proveedores y/o Terceros) que requieren acceder muy rara vez.
- d. Teniendo en cuenta lo anterior, los únicos que deben tener privilegios de acceso permanente a las áreas seguras son los profesionales que trabajan regularmente en ellas. Los demás usuarios deben solicitar autorización para el acceso y portar un documento que demuestre y en todo caso acredite la calidad en la que actúa para efectuar dicho ingreso. En este tipo de casos, se debe asignar por parte del área responsable del área segura un profesional que acompañe y supervise la labor de dicho visitante, hasta su salida.
 - El acceso al Datacenter está restringido y su ingreso es únicamente por medio biométrico. Esto debe aplicarse para el personal como: (Funcionarios, Contratistas, Proveedores y Terceros) de la Entidad.
 - El acceso a los Centros de Cableados, se debe diligenciar la bitácora de ingreso y salida. Esto debe aplicarse para los Funcionarios, Contratistas, Proveedores y Terceros de la Entidad.
 - Para el ingreso de los visitantes, en las áreas seguras se debe llevar un registro de la fecha y la hora de entrada y salida, profesional que autoriza, dependencia o entidad a la que pertenece y actividad realizada, entre otros que sean requeridos para cada caso en particular.

- Las actualizaciones a los derechos de acceso, pueden ser efectuadas cuando ello así se requiera por parte de cada profesional u oficina encargada del área segura, para lo cual si es del caso, se revocarán aquellos permisos que ya no sean necesarios.

- **Excepciones:**

Cualquier excepción debe ser autorizada por el Líder u Oficial de Seguridad de la información.

11.1.3. Seguridad de Oficinas, Recintos e Instalaciones

Con el propósito de mantener la Confidencialidad, Integridad y Disponibilidad de la Información en las Oficinas, recintos e instalaciones, es necesario establecer y dar cumplimiento a las siguientes directrices de Seguridad:

- Todos los Funcionarios, Contratistas, Proveedores y/o Terceros deben presentar su carnet o documento de identificación, según sea el caso, para el ingreso a las instalaciones de la Entidad.
- Todos los Funcionarios, Contratistas, Proveedores, Terceros y visitantes deben portar visiblemente la escarapela, carnet o documento que los acredite como tal, mientras se encuentren en las instalaciones de la Entidad.
- Todo el personal que ingrese o salga de las instalaciones de la Entidad independientemente de su calidad, deberá registraren la bitácora de vigilancia, el ingreso y salida de los dispositivos tecnológicos institucionales o personales.
- Todo visitante debe notificar y registrarse en la recepción, la oficina o área a la que se dirige y su ingreso debe estar previamente autorizado.
- Todas las oficinas del Instituto que procesen, almacenen y/o gestionen información reservada o sensible deben implementar y adoptar las medidas tendientes a asegurar dicha información.
- Para aquellas oficinas cuyo acceso físico, se de a través de puertas, es deber del Jefe de Oficina correspondiente, salvaguardar las llaves de esta y asegurar una copia en un lugar diferente y seguro.
- Los materiales o combustibles, deben ser almacenados de manera segura a una distancia prudentes de las áreas de procesamiento y almacenamiento de Información.
- Los suministros de papelería no deben almacenarse en Áreas Seguras como: (Datacenter, Centros de Cableado, Cuarto de Suministro, Archivo Físico Central y Archivo Físico de Gestión).
- En las Áreas Seguras como: (Datacenter, Centros de Cableado, Cuarto de Suministro, Archivo Físico Central y Archivo Físico de Gestión), no se debe utilizar como bodega.
- Las salidas de emergencia deben tener alarma.

- **Excepciones:**

Cualquier excepción debe ser autorizada por el Líder u Oficial de Seguridad de la información.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

11.1.4. Protección Contra Amenazas Externas y Ambientales

El Instituto Colombiano Agropecuario - ICA, debe proveer las condiciones físicas y mediambientales necesarias para brindar la protección de las personas y a la Seguridad de la Información de la Entidad, ante posibles eventos como incendios, inundaciones, terremotos, explosiones, ataques maliciosos, entre otros. Por lo anterior se debe dar cumplimiento a los siguientes lineamientos:

- La Oficina de Tecnología de Información, debe propender por la Seguridad del (Datacenter y Centros de Cableado) que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- El propietario del activo de información debe propender porque la Información se almacene en un ambiente protegido y seguro.

- **Excepciones:**

Cualquier excepción debe ser autorizada por el Líder u Oficial de Seguridad de la información.

11.1.5. Trabajo en Áreas Seguras

- En el Datacenter y Centros de Cableado, deben existir sistemas de control ambiental de temperatura, 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 Tecnología de Información, debe velar porque los Recursos de la Plataforma Tecnológica de la Entidad, estén ubicados en el Datacenter (Interno o Externo) con protecciones contra fallas o interrupciones eléctricas.
- La Oficina de Tecnología de 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 Tecnología de Información, debe tener control de: (cualquier cambio, modificación, actualización, ajuste o soporte) que se realice sobre los procesos, Áreas Seguras y Sistemas de Procesamiento de Información, que puedan afectar uno o más de los "Pilares de Seguridad de Información (Confidencialidad Integridad y Disponibilidad)"; para ello deben pasar por la aprobación del Comité de Cambios TI antes de su ejecución.
- En las áreas seguras no está permitido el registro fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con una autorización del profesional o área encargada del área segura, para ello.

- **Excepciones:**

Cualquier excepción debe ser autorizada por el Líder u Oficial de Seguridad de la información.

11.1.6. Áreas de Despacho y Carga

El Instituto Colombiano Agropecuario – ICA, no cuenta con estas áreas definidas, dado que la Administración del Edificio no cuenta con dicha ubicación para tal fin.

11.2. EQUIPOS

- **Objetivo:** Establecer los lineamientos para prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la entidad.
- **Alcance:** La presente Política aplica para todos los Funcionarios, Contratistas, Proveedores y/o Terceros que tengan acceso a la información, en medio digital o físico, del ICA.
- **Lineamientos:**
La seguridad de los Equipos y Activos de la entidad, permite prevenir pérdidas, daño o compromiso de los activos y la interrupción de las actividades del negocio. Se debe dar cumplimiento de los siguientes lineamientos:

11.2.1. Ubicación y Protección de Equipos

- a. La Infraestructura Tecnológica de la Entidad, tales como: Servidores, Equipos activos y otro tipo de hardware que no resida típicamente en escritorios de usuario estar ubicados físicamente en un área segura, se deben implementar los controles necesarios que puedan afectar la disponibilidad de los datos.
- b. Los computadores portátiles y de escritorio tipo “todo en uno” asignados a los Funcionarios, Contratistas, Proveedores y/o Terceros de la entidad, deben ser entregados con guaya de Seguridad, para permitir su anclaje en el puesto de trabajo con el fin de mitigar el riesgo de pérdida o robo del mismo.

11.2.2. Servicio de Suministro

- a. La infraestructura tecnológica de la entidad, debe estar protegido contra problemas eléctricos que puedan causar una falla o mal funcionamiento de los mismos.

11.2.3. Seguridad de Cableado

- a. Gestión de Recursos Físicos, debe garantizar que dentro de la infraestructura física del ICA, el cableado de energía eléctrica y de telecomunicaciones que transporta los datos o soporta los Servicios de Información de la entidad, deben estar protegidos para evitar daño o mala manipulación.
- b. Las áreas de distribución de redes deben estar físicamente aseguradas para prevenir la modificación o el acceso no autorizado a las mismas.

11.2.4. Mantenimiento de Equipos

- a. La instalación de cualquier tipo de software en los equipos de la entidad, es responsabilidad de la Oficina de Tecnología de Información y por tanto son los únicos autorizados para realizar y/o autorizar esta labor, que se realizara con usuario administrador del equipo local.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- b. El mantenimiento de los equipos, se deben realizar a intervalos planificados teniendo en cuenta las especificaciones y recomendaciones de los fabricantes; por lo que es necesario llevar un registro de las fallas presentadas.
- c. El Mesa de ayuda de la Entidad, no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración) a equipos personales.
- d. Los usuarios no deben realizar cambios en los equipos de la Entidad; referente a: la configuración del equipo, conexiones de red, papel tapiz y protector de pantalla definido por el ICA, fotografía personal en el usuario de correo institucional. Estos cambios pueden ser realizados únicamente por el personal de la Mesa de Ayuda designado para tal labor por parte de la Oficina de Tecnología de Información, a través de una solicitud de ticket previamente autorizada.

11.2.5. Retiro de Activos

- a. El retiro de equipos de la entidad, deberá estar justificado y autorizado por el jefe de área donde está ubicado el equipo, y visto bueno del Jefe de Oficina de Tecnología de Información y Líder Oficial de Seguridad de Información.

11.2.6. Seguridad de Equipos y Activos Fuera de las Instalaciones

- a. Se deben asegurar los equipos de la entidad, fuera de las instalaciones y su salida debe estar autorizada por el responsable del área a la cual esté asignada la máquina.

11.2.7. Disposición Segura o Reutilización de Equipos

- a. Toda la información de la entidad, tendrá que ser removida del equipo antes de su disposición o reutilización, previa generación de backup de la información allí almacenada.
- b. Antes de cualquier venta o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación de información que adopte la entidad, previa generación de backup de la información allí almacenada.

11.2.8. Equipos de Usuarios Desatendidos

Los usuarios deben asegurar que el equipo desatendido tiene una adecuada protección y están obligados a:

- a. No dejar la sesión abierta, cuando se ausente del puesto de trabajo.
- b. En el momento de dejar desatendido el computador o portátil en el puesto de trabajo, el usuario debe bloquear su equipo usando las teclas: "Botón de windows + la tecla L" o "Ctrl + ALT+ SUPR + ENTER".
- c. Bloquee la sesión y/o cierre la sesión de usuario, cuando finalice la tarea (no es correcto apagar la pantalla o el equipo sin salir de la sesión de usuario).
- d. Los equipos que se encuentren bloqueados deberá contar con protector de pantalla definido por la entidad, de acuerdo al tiempo límite de inactividad definida por el Administrador.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- e. Los equipos portátiles y los equipos de escritorios tipo “todo en uno”, deberán contar con el uso de guaya como mecanismo de Seguridad Física.

11.2.9. Política de Escritorio Limpio y Pantalla Limpia

a. Escritorio limpio

La Política de escritorio limpio aplica para toda los equipos de propiedad de la entidad y personales, por lo que se debe dar cumplimiento de los siguientes lineamientos:

- Proteja la información siempre que abandone su puesto de trabajo.
- No se deben dejar documentos con información Sensible o Confidencial, al alcance de personal no autorizado, en caso de tener este tipo de información en físico ésta debe ser guardada bajo llave en archivadores.
- No se debe dejar documento que se encuentre en tránsito al alcance de personal no autorizado, independiente de su clasificación que contiene información institucional.
- No se debe consumir líquidos en el puesto de trabajo.

b. Pantalla Limpia

- El escritorio virtual del equipo de cómputo debe permanecer libre de documentos digitales, independiente de su clasificación de información.

- **Excepciones:**

Cualquier Excepción debe ser justificada, validado y aprobada por el Jefe de Oficina de Tecnología de Información y el Líder u Oficial de Seguridad de la de la Entidad.

12. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

- **Dominio/ Control:** A.12 Seguridad en las Operaciones.
- **Objetivo:** Establecer los lineamientos para las operaciones de la Entidad, de forma correcta y seguras de las Instalaciones de procesamiento de información.
- **Alcance:** La presente Política aplica para todas las operaciones que se desarrollen en la Entidad, a través de Funcionarios, Contratistas, Proveedores y/o Terceros, con los que interactúa el ICA.
- **Lineamientos:**
Se debe dar dar cumplimiento a los siguientes lineamientos:

12.1. PROCEDIMIENTOS DE OPERACIONES Y RESPONSABLES

12.1.1. Procedimientos de Operación Documentado

- a. Los Procedimientos Operativos se deben documentar y poner a disposición de los Funcionarios, Contratistas, Proveedores y/o Terceros que los necesitan para la ejecución de sus funciones.
- b. Los Procedimientos Operativos específicos de la Entidad, deben ser tratados como documentos formales y los cambios que se generen deben ser autoizados.

- c. Se debe mantener un diagrama actualizado de la red de la Entidad.
- d. La Oficina de Tecnología de Información, debe mantener una lista documentada y actualizada de los Servicios, Protocolos y Puertos Utilizados, incluyendo la justificación pertinente en los casos que se estén utilizando protocolos no seguros. En el caso de detectar protocolos inseguros, se debe contar con contramedidas para cerrar las vulnerabilidades encontradas.

12.1.2. Gestión de Cambio

- a. La Oficina de Tecnología de Información, se debe implementar un proceso documentado para la Gestión de Cambios, el cual debe ser implementado para todo el ICA, en las instalaciones, los Sistemas de Información e Infraestructura de TI donde se afectan la Seguridad de la Información.
- b. Solo se deben habilitar los Servicios y Protocolos necesarios y seguros según lo requiera la función del Sistema solicitado.

12.1.3. Gestión de Capacidad

- a. La Oficina de Tecnología de Información, se debe realizar un análisis de capacidades y proyecciones para el procesamiento y almacenamiento disponible de la información. Estas proyecciones deben tener en cuenta:
 - Los nuevos requerimientos de Sistemas de Información de los Procesos.
 - Cambios Tecnológicos.
 - El crecimiento de los Sistemas actuales de Procesamiento de la Información.

12.1.4. Separación de los Ambientes, de Desarrollo, Pruebas y Operación

- a. La Oficina de Tecnología de Información, debe separar los ambientes de Desarrollo, Pruebas y Producción para reducir los Riesgos de accesos o cambios no autorizados a los Sistemas en Producción, así como posibles inconvenientes en la operación de los mismos.

12.2. PROTECCIÓN CONTRA CODIGO MALICIOSO

12.2.1. Controles Contra Código Malicioso

- a. Se deben implementar controles de detección y prevención para proteger contra código malicioso, así mismo se deben realizar Procedimientos de concientización para el usuario.
- b. Todos los equipos personales y de propiedad de la Entidad, deben tener instalados los parches de Seguridad más recientes proporcionados por los fabricantes. La aplicación de los parches debe realizarse dentro de un periodo máximo de un mes a partir de su liberación, esta tarea se debe realizar de forma automática o en caso manual cuando se requiera.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

12.3. COPIAS DE RESPALDO

12.3.1. Respaldo de la Información

- La Oficina de Tecnología de la Información, debe definir un Procedimiento para las actividades de backup de la Información de la Entidad, teniendo en cuenta la criticidad y las necesidades de disponibilidad de los datos. Este procedimiento debe estar debidamente documentado para seguimiento y control.
- Es responsabilidad de quien (es) ejecute (n) el rol de administrador de cada Sistema de información, realizar la solicitud de copia a quien (es) ejecute (n) el rol de administrador de backup, validar y asegurar que su Sistema de Información se encuentre contemplado en el cronograma de copias de seguridad, además de hacer seguimientos regulares a su ejecución.
- Quien (es) ejecute (n) el rol de Administrador de backup debe validar el resultado de la ejecución de las copias de Seguridad y registrar las novedades en la bitácora establecida para ello como lo debe indicar el procedimiento.
- Es responsabilidad de quien (es) ejecute (n) el rol de Administrador de backup realizar pruebas de restauración de copias de seguridad de manera trimestral siguiendo los lineamientos del Procedimiento Backup y Recuperación de la Información.
- Cada copia de seguridad debe quedar registrada en la máquina donde son realizados (logs de servidor) o en un archivo externo (texto, planilla, etc.) que permita mantenerla disponible para controles o auditoría.
- Los medios de respaldo removibles deben ser trasladados a un lugar externo que garantice el catálogo, la fiabilidad, Seguridad y disponibilidad de estos. Para ello se debe asegurar un transporte o un servicio de mensajería fiable que cuente con todas las medidas de seguridad.

12.4. REGISTRO Y SEGUIMIENTO

12.4.1. Registro de Eventos

- Se deben generar y mantener registros de auditoría sobre las actividades de los usuarios, excepciones y eventos de Seguridad de Información para soportar futuras investigaciones y monitoreo del control de acceso.

12.4.2. Protección de la Información de Registros

- Los registros de información se deben proteger contra intentos de alteración y acceso no autorizado.

12.4.3. Registros de Administrador de Operador

- Todas las evidencias que se recolecten como resultado de las auditorías practicadas, deben contar con un lugar para el almacenamiento de los registros y monitoreo de los eventos de Seguridad.
- Todo acceso administrativo a sistemas críticos de la Entidad que no sea por consola debe ser cifrado (SSH, HTTPS).

12.4.4. Sincronización de Relojes

- a. Se debe tener como referencia la Hora Legal Colombiana, no está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora.

12.5. CONTROL DE SOFTWARE OPERACIONAL

12.5.1. Instalación de Software en Sistemas Operativos

- a. La Oficina de Tecnología de Información, debe implementar Procedimientos para controlar la instalación de software sin autorización, para minimizar vulnerabilidades de Seguridad.
- b. Los usuarios no podrán realizar instalaciones de software no autorizado en los equipos de la Entidad, esta solicitud debe estar avalada por el Oficial de seguridad de la Información.

12.6. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

12.6.1. Gestión de las Vulnerabilidades Técnicas

- a. La Oficina de Tecnología de Información, debe implementar Procedimientos para la Gestión de Vulnerabilidades Técnicas y Remediaciones de las mismas.
- b. Está totalmente prohibida la instalación de software no autorizado en los equipos de la Entidad.
- c. La ejecución del análisis de vulnerabilidades tiene como fin, identificar las brechas de Seguridad con las que cuenta un Sistema de Información y la Infraestructura Tecnológica, por lo tanto, la Entidad debe ejecutar análisis de vulnerabilidades a los Activos de información. Se debe:
 - Documentar los resultados.
 - Priorizar las vulnerabilidades.
 - Documentar el Plan de remediación para corregir o mitigar (según sea el caso) las brechas identificadas.
 - Entregar los resultados de las pruebas realizadas a cada uno de los responsables de los Sistemas de Información e Infraestructura Tecnológica del ICA, quién es el encargado de definir y aplicar el debido plan de remediación.

12.7. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN

12.7.1. Controles de Auditoría de Sistemas de Información

- a. Los registros y auditorías, debe garantizar la evaluación de los controles, la eficiencia de los Sistemas y el cumplimiento de los Lineamientos establecidos por la Entidad, así como las recomendaciones de las deficiencias o hallazgos detectados.
- b. Las herramientas de auditoría deben estar separadas de los ambientes de desarrollo y producción, y no deben estar en bibliotecas de cintas y/o áreas de usuarios; a menos que se le dé un nivel adecuado de protección adicional.

- **Excepciones:**

Cualquier excepción debe ser autorizada por la Dirección de Tecnologías de la Información y el Líder u oficial de Seguridad de la información de la entidad.

13. POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES

- **Dominio/ Control:** A.13 Seguridad de las Comunicaciones

- **Objetivo:** Establecer los lineamientos para la gestión segura de las redes y sus instalaciones de procesamiento de Información de la Entidad.

- **Alcance:** La presente Política aplica para todos los Funcionarios, Contratistas, Proveedores y/o Terceros o que por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información del ICA.

- **Lineamientos:**

Se debe dar cumplimiento a los siguientes lineamientos:

13.1. GESTIÓN DE LA SEGURIDAD LAS REDES

13.1.1. Controles de Redes

- a. Se deben controlar los accesos a servicios internos y externos conectados en red.
- b. Funcionarios, Contratistas, Proveedores y/o Terceros, antes de contar con acceso lógico por primera vez a la red de datos del ICA, deben contar con la autorización previa por parte de su Jefe inmediato y/o supervisor del Contrato, para proceder a la creación, activación de la cuentas de usuario, esta solicitud se debe hacer a la Oficina de Tecnología de Información por el canal definido por la Entidad.
- c. Se deben identificar e incluir en los acuerdos de niveles de Servicio (ANS) (SLA) como mecanismos de Seguridad. Los niveles de Servicio y los requisitos de administración de todos los Servicios de Red, independientemente de si estos servicios se entregan de manera interna o están tercerizados.

13.1.2. Seguridad de los Servicios de Red

- a. La Oficina de Tecnología de Información de la Entidad, como responsable de las redes de datos y los recursos de red del ICA (internos y externos), debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

13.1.3. Separación en las Redes

- a. La Oficina de Tecnología de Información de la Entidad, debe asegurar que las redes inalámbricas del ICA, cuenten con procedimientos de autenticación para evitar el acceso no autorizados. Estos procedimientos deben estar soportados en técnicas de segmentación de redes y restricción de uso de las redes inalámbricas solo a funcionarios autorizados.
- b. Se deben segmentar las redes en función de los grupos de Servicios, usuarios y sistemas de información de la Entidad.

- c. La Entidad, debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su Plataforma Tecnológica y Sistemas de Información, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados sobre los Sistemas Operacionales.
- d. No deben realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción de la Entidad.

- **Excepciones:**

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador de redes, según aplique; debidamente validada por el Líder u Oficial de Seguridad de la Información de la Entidad y aprobada por el Jefe de la Oficina de Tecnologías de la Información o quien haga sus veces.

13.2. TRANSFERENCIA DE INFORMACIÓN

- **Dominio/Control:** A13.2 Transferencia de Información.

- **Objetivo:** Establecer los lineamientos para mantener la Seguridad de la Información transferida dentro de la Entidad y con cualquier Entidad externa.

- **Alcance:** La presente política aplica para Funcionarios, Contratistas, Proveedores y/o Terceros, o quien por su rol, transfieran información dentro de la entidad y con cualquier entidad externa.

- **Lineamientos:**

La transferencia de Información por cualquier medio debe realizarse protegiendo la confidencialidad e integridad de los datos con los mecanismos que se encuentren establecidos en el Modelo de Seguridad y Privacidad de la Información- MSPI de acuerdo con la clasificación del activo de información involucrado.

13.2.1. Política y Procesamiento de Transferencia de Información

- a. La Entidad, debe establecer una Política, Procedimientos y controles formales para proteger la transferencia de información, soportada en su Infraestructura Tecnológica.

13.2.2. Acuerdos Sobre Transferencia de Información

- a. Cuando se trate de intercambios periódicos, se debe privilegiar la transmisión de datos a través de vías seguras, con los cuales se establecen convenios o nexos de diferente naturaleza, y que involucran de alguna forma el intercambio de información.
- b. Para el acceso a sitios web, se debe implementar herramientas de Seguridad perimetral seguros (firewalls) y el uso de protocolos y/o certificados SSL seguros, ofuscamiento, entre otras herramientas, plugins y/o técnicas con la finalidad de protección.

13.2.3. Mensajería Electrónica

- a. Todos los mensajes enviados desde la cuenta Institucional de la Entidad, deben respetar el estándar de formato e imagen Corporativa del ICA.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- b. El uso del correo electrónico en cadenas o mensajes enviados a un número de destinatarios y estos a su vez son reenviados a otros, sin un propósito relacionado con la misión del ICA, degradan el desempeño del Servicio de Correo y consumen recursos de TI valiosos. El usuario debe abstenerse de reenviarlos a otras personas.
- c. El envío de archivos que contengan extensiones como .mp3, wav, .exe, .com, .dll, .bat. o cualquier otro archivo ejecutable; en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Oficina de Tecnología de Información de la Entidad.
- d. No Enviar o recibir cadenas de correo, mensajes con contenido religioso, juegos, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos. Si un usuario encuentra este tipo de material deberá reportarlo mediante ticket a la Mesa de Ayuda de la Entidad.
- e. La Entidad, asignar una cuenta de correo electrónico como herramienta de trabajo para cada uno de los Funcionarios, Contratistas o quien por su rol, lo requieran para el desempeño de sus Funciones y/o Obligaciones y en algunos casos a terceros previa autorización; su uso se encuentra sujeto a lo establecido en la presente Política.
- f. Los mensajes y la información contenida en los buzones de correo son de propiedad de ICA, y cada usuario es responsable de su buzón, por lo que debe mantener solamente los mensajes relacionados con el desarrollo de sus Funciones y /o Obligaciones.
- g. El correo electrónico, deberá tener al final del mensaje el siguiente texto:
 - “Aviso Legal: Este mensaje es de interés exclusivo para la persona o personas a la(s) que va dirigido. Puede contener información confidencial o legalmente protegida. No hay renuncia a la confidencialidad o privilegio por cualquier transmisión mala y/o errónea. Si usted lo ha recibido este mensaje por error, este, todas sus copias y archivos adjuntos, deben ser eliminados de sus sistemas y disco duro inmediatamente y notifique al remitente. Si usted no es el destinatario final, no debe, directa o indirectamente, usar, revelar, distribuir, imprimir o copiar ninguna de las partes de este mensaje”.
 - “This message is intended exclusively for the named person or people. It may contain confidential, proprietary or legally privileged information. No confidentiality or privilege is waived or lost by any mistransmission. If you receive this message in error, please immediately delete it, all copies and included files of it from your system, destroy any hard copies of it and notify the sender. You must not, directly or indirectly, use, disclose, distribute, print, or copy any part of this message if you are not the intended recipient. Any views expressed in this message are those of the individual sender”.

13.2.4. Acuerdos de Confidencialidad o de No Divulgación

- a. La presente Política de Confidencialidad, tiene por objeto informarles a todos los Funcionarios, Contratistas, Proveedores y/o Terceros o quien por su rol estén vinculados con el ICA, sobre el compromiso frente a la no divulgación de la información relacionada

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

con las funciones y/o obligaciones contractuales que desempeña en la Entidad, a personal interno o externo de la misma. Concluyendo que en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcial sin contar con previa autorización.

- b. Todos los Funcionarios, Contratistas, Proveedores y/o Terceros o quien por su rol estén vinculados con el ICA, deben firmar la cláusula y/o acuerdos de confidencialidad definidos, y este deberá ser parte integral de cada uno de los contratos. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la Entidad a personas o entidades externas.
 - c. El ICA, firmará acuerdos de Confidencialidad con los Clientes y Terceros o Contratistas, que por diferentes razones requieran conocer o intercambiar información Reservada o Confidencial de la Entidad. En estos los acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.
 - d. El acuerdo de Confidencialidad deberá formalizarse en cada uno de los contratos celebrados con Terceros y que en la Prestación del Servicio puedan tener acceso a la información Reservada o Confidencial de la Entidad.
 - e. Todos los Funcionarios, Contratistas, Proveedores y/o Terceros del ICA, deben guardar absoluta reserva en relación con la Información a la que tenga acceso con ocasión de la ejecución del Funciones y/o Obligaciones, aun después de finalizada su ejecución, por el tiempo establecido por la normatividad legal vigente y aplicable para cada caso en particular.
 - f. El acuerdo de Confidencialidad deberá formalizarse en cada uno de los casos en los que se requiere suministrar información de la Entidad a un tercero con el que la Entidad no tiene ningún vínculo directo o indirecto para estimación de proyectos futuros.
 - g. El acuerdo de Confidencialidad se firmara por un lado entre la parte RECEPTOR de la información y por otro lado como REVELADOR de la información de propiedad de la Instituto Colombiano Agropecuario – ICA será el Jefe de Oficina.
 - h. Se debe firmar un acuerdo de confidencialidad con los Proveedores y/o Terceros con los que no se cuente con un vinculación vigente; cuando estos requieran información de la Entidad.
- **Excepciones:**
Las excepciones establecidas por Ley en caso de aplicar.

14. POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- **Dominio/ Control:** A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas.
- **Objetivo:** Asegurar, preservar y garantizar el control de acceso a los Sistemas y Aplicaciones de la Entidad.
- **Alcance:** Para todas las Aplicaciones de la Entidad.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- **Lineamientos:**

Se debe dar cumplimiento a los siguientes lineamientos:

14.1. REQUISITOS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

14.1.1. Análisis y Especificaciones de Requerimientos de Seguridad de la Información

- a. El propietario del Sistema de Información de la Entidad, deberá identificar y documentar que tipo de clasificación de la información se encuentra contenida en los mismos.
- b. Los propietarios de los Activos de Información deben autorizar los accesos a sus Sistemas de Información o Aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la clasificación de la información definida por la Entidad.
- c. No está permitido para ningún Servidor Público, Contratista, Proveedor y Tercero, acceder a la información y a las aplicaciones de un Sistema de Información para el cual no haya sido autorizado.
- d. Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Oficina de Tecnología de la Información – OTI con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
- e. Ninguna Subgerencia, Oficina y Gerencias Seccionales de la Entidad, podrá hacer adquisición de elementos tecnológicos como (computadores de escritorio, portátiles, dispositivos de red, software, cámaras de vigilancia, telefonía IP, impresoras, Tablet, equipos de comunicación, switches, router, entre otros) sin el visto bueno del Jefe de la Oficina de Tecnología de Información del Instituto Colombiano Agropecuario “ICA”.
- f. Ninguna Subgerencia, Oficina y Gerencias Seccionales de la Entidad, podrá hacer cableados de red, sin el visto bueno del Jefe de la Oficina de Tecnología de Información del Instituto Colombiano Agropecuario “ICA”.

14.1.2. Seguridad de Servicios de las Aplicaciones en Redes Públicas

- a. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico en la Entidad debe (n) asegurar que los grupos de Servicios de Información, usuarios y Sistemas de Información sean segmentados en redes.
- b. En lo que respecta a la autorización y continuidad en el uso de los usuarios de los Sistemas de Información y/o Aplicativos del ICA, será deber de cada una de las dependencias de la entidad, informar a los Administradores de las aplicaciones la novedad o novedades que surjan en Servidor Público, Contratista, Proveedor y Tercero, con el objeto de que dichos usuarios sean deshabilitados o suspendidos oportunamente, según fuere el caso.
- c. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el Sistema y los controles de las aplicaciones.
- d. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n) llevar un registro actualizado de todos los programas fuentes en uso, indicando entre otros, el nombre del programa, programador, analista responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

- e. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n) restringir el acceso a los códigos fuente de los programas, asegurándose de que solamente los ingenieros desarrolladores tengan acceso únicamente a las aplicaciones de su competencia.
- f. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n) mantener los códigos fuente de los programas en el servidor o repositorio de fuentes. El mantenimiento y copiado de las bibliotecas fuentes del programa está sujeto a procedimientos estrictos de control de cambios.

14.1.3. Protección de Transacciones de los Servicios de las Aplicaciones

- a. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.
- b. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) establecer los controles de acceso a los ambientes de producción de los sistemas de información.
- c. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- d. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurar que en lo que respecta a los sistemas operativos de la entidad, se bloquee la sesión automáticamente, después de determinados minutos de inactividad, previamente establecidos.
- e. Quien (es) ejecute (n) el rol de desarrollador de sistemas de información debe (n) garantizar que se cierre la sesión en las aplicaciones, después de determinados minutos de inactividad (Timeout) previamente establecidos.
- f. Se debe asignar el rol del Administrador de programas fuentes, quien tendrá la responsabilidad de custodiar dichos programas y por virtud de su función no deberá pertenecer al equipo de desarrollo.
- g. La actualización de las bibliotecas de fuentes del programa, así como la emisión de las fuentes para los programadores sólo se deben realizar después de haber recibido la autorización del Arquitecto de Desarrollo.
- h. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n) mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa.
- i. Los desarrolladores Interno y Externos, deben aplicar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
- j. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe(n) asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada, conforme a lo estipulado en el procedimiento de backup.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- k. No está permitido facilitar el usuario o la contraseña a otra persona para adelantar cualquier labor en los Sistemas de Información y/ Aplicaciones.

- **Excepciones:**

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador de control de acceso lógico o Administrador de programas fuentes, según aplique; debidamente validada por el Líder u Oficial de Seguridad de la Información de la Entidad y aprobada por el Jefe de la Oficina de Tecnologías de la Información o quien haga sus veces.

14.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE

- **Dominio/ Control:** A.14.2 Seguridad de los Procesos de Desarrollo Seguro.

- **Objetivo:** Propender porque se diseñe e implemente dentro del ciclo de vida de Desarrollo de los Sistemas de Información buenas Prácticas de Seguridad de Información.

- **Alcance:** La presente Política aplica para los Sistemas de Información, tanto desarrollos propios como de terceros, que integren cualquiera de los ambientes administrados por la Entidad en: (desarrollo, producción y/o pruebas).

- **Lineamientos:**

La protección de la Confidencialidad de los Activos de Información de la Entidad, se delimita el acceso a los mismos, de acuerdo a los niveles de clasificación y riesgos identificados y definidos por el propietario de los mismos, para lo cual se debe considerar la separación de los ambientes tecnológicos como son: desarrollo, pruebas y producción. Por lo anterior se debe dar cumplimiento a los siguientes lineamientos:

14.2.1. Política de Desarrollo Seguro

- a. Los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no deben ser accesibles desde los ambientes de producción cuando no se requiera.

14.2.2. Procedimientos en Control de Cambios en Sistemas

- a. Se debe implementar el Procedimiento de Control de Cambios definidos por la Entidad, cuando se realicen cambios a los Sistemas de Información; estos cambios pueden ser:
- Modificación a Sistemas de Información en Producción (campos, tablas, parámetros, entre otros).
 - Nuevos Requerimientos a Sistemas de Información en Producción (módulos, tablas, campos, entre otros).
 - Nuevos Sistemas de Información (desarrollo in house o externo).
 - Cambios reglamentarios.
 - Y demás que afecten los Sistemas de Información por necesidades puntuales de la Entidad.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- b. En el ambiente de producción se ubicarán todos los Público y aplicativos que prestarán los servicios a los usuarios finales internos y/o externos a la entidad. Luego que la etapa de pruebas llegue a su fin y se tenga un aplicativo estable en ambiente de pruebas donde se haya probado la instalación y la funcionalidad, el responsable de la aplicación desarrollada, debe hacer una solicitud de cambio al Comité de cambios para migrar de manera controlada dicho aplicativo hacia producción. Para poder recibir un software en el ambiente de Producción se debe tener en cuenta las siguientes condiciones:

- Tipo y clasificación de la información que maneja.
- Características del respaldo y restauración (cantidad de información, periodicidad, crecimiento esperado, tiempo de retención, tiempo aceptable de recuperación, desde cuándo se debe recuperar).
- Plan de contingencia (preferiblemente alineado con el plan de continuidad de la entidad).
- Documento de control de cambios o documentación de implementación.
- Resultado del plan de pruebas detallado y exhaustivo (con pruebas de desempeño y funcionales).
- Pruebas de seguridad y controles aplicados a la mitigación o respuesta al riesgo.
- Manual de diseño.

14.2.3. Revisión Técnicas de las Aplicaciones después de Cambios en la Plataforma de Operación

- a. Los cambios en los sistemas operativos y aplicaciones se deben poner a prueba en un entorno de pruebas antes de aplicarlos a los ambientes de producción.

14.2.4. Restricciones en los cambios a los paquetes de Software

- a. Se deben definir y documentar las reglas para la transferencia de software del ambiente de pruebas al ambiente de producción.

14.2.5. Principios de Construcción de los Sistemas Seguros

- a. La Entidad, debe garantizar que los criterios de Seguridad de la Información se cumplan en todas las etapas de desarrollo y durante todo el ciclo de vida de un determinado software, con el objeto de incluir los requisitos de Seguridad de la Información en la metodología utilizada para tal fin en el que se establezcan las directrices de codificación seguras para cada lenguaje de programación usado y se apliquen los siguientes pasos:

- Análisis de requerimientos.
- Análisis arquitectónico.
- Tipo de desarrollo (propio o a terceros).

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- Pruebas (funcionales, no funcionales y de Seguridad).
 - Producción.
 - Mantenimiento.
- b. El ICA, asegurará que el software adquirido y/o desarrollado al interior de la Entidad, cumplirá con los requisitos de Seguridad con Calidad.
- c. La Oficina de Tecnología de Información, incluirán requisitos de Seguridad en la definición de Requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.
- d. En caso de desarrollos propios la Entidad, debe verificar que estén:
- Que estén completamente documentados.
 - Que las diferentes versiones se preservan adecuadamente en varios medios.
 - Que se guarda copia de respaldo externa a la Entidad.
 - Que sean registrados ante la “Dirección General de Derechos de Autor”.

14.2.6. Ambiente de Desarrollo Seguro

- a. Los usuarios deben usar diferentes perfiles de usuario para los ambientes de producción y los ambientes de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error.

14.2.7. Desarrollo Contratado Externamente

- a. El software que se adquiera a través de los proyectos o programas debe quedar a nombre del Instituto Colombiano Agropecuario - ICA.

14.2.8. Pruebas de Seguridad de Sistemas

- a. Las pruebas no se deben llevar a cabo en el ambiente de producción.

14.2.9. Pruebas de Aceptación de Sistemas de Sistemas

- a. La Oficina de Tecnología de Información de la Entidad, debe aplicar los documentos relacionas con el Ciclo de vida de Desarrollo, definios en el **Numeral:14.2.5** de está Política.

14.3. DATOS DE PRUEBA

14.3.1. Protección de Datos de Prueba

- a. Los datos sensibles no se deben copiar en el ambiente de pruebas, salvo que se suministren controles equivalentes al ambiente de producción.

15. RELACION CON LOS PROVEEDORES

- **Dominio/ Control:** A.15 Relación con los Proveedores.
- **Objetivo:** Establecer los lineamientos para asegurar la protección de los activos de la Entidad que sean accesibles a los proveedores.
- **Alcance:** La presente Política aplica para todos los Proveedores o Terceros, que requieran acceso a los Activos de Información de la Entidad.
- **Lineamientos:**
Se debe dar cumplimiento a los siguientes lineamientos:

15.1. SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON LOS PROVEEDORES

15.1.1. Política de Seguridad de Información para las Relaciones con Proveedores

- a. La Entidad, durante la Etapa Precontractual, desde la construcción de los estudios previos, el Área solicitante de la contratación, debe identificar los Riesgos de Seguridad de la Información con el apoyo del Líder u Oficial de Seguridad de la Información, los cuales deben ser parte de la estimación y cobertura de los riesgos del proceso de contratación. De acuerdo con lo anterior, el análisis de riesgos de seguridad de la información debe incluir la identificación de los mismos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.
- b. La Entidad, en cabecera del Comité evaluador debe identificar si el objeto de la propuesta u oferta evaluada, requiere del acceso de los proveedores a:
 - A la información Reservada o Confidencial.
 - A los Sistemas de Información.
 - A las Áreas Seguras.
- c. El Comité evaluador debe contar con la participación del Líder u oficial de seguridad de la información a fin de determinar los requisitos mínimos de seguridad y los controles necesarios por parte del proveedor para ejecutar dicho contrato.
- d. En medio de la Etapa Contractual, se debe asegurar la inclusión de las cláusulas:
 - De Confidencialidad.
 - De Protección de Datos.
 - Derechos de Propiedad Intelectual.
 - Las Políticas de Seguridad y Privacidad de la Información definida por la Entidad.
 - Derechos de Autor.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- e. En la suscripción y perfeccionamiento del contrato que se celebre entre el ICA y aquellos Proveedores.

15.1.2. Tratamiento de Seguridad dentro de los Acuerdos con Proveedores

- a. Antes de iniciar la ejecución del contrato, el supervisor debe socializar a los Proveedores:}
- Las Políticas de Seguridad y Privacidad de la Información.
 - Los Procedimientos asociados al Sistema de Gestión de Seguridad de la Información.
- b. Durante la Etapa Post Contractual, es función del supervisor y/o interventoría asignada, monitorear y hacer seguimiento a los controles pactados para asegurar la Confidencialidad, Integridad y Disponibilidad de la Información, frente a los riesgos previamente identificados.

15.1.3. Cadena de Suministro de Tecnología de Información y Comunicaciones

- a. Para los Servicios de Tecnología y de Comunicaciones contratados externamente, se debe exigir que los Proveedores divulguen los requisitos y prácticas de Seguridad del ICA, a lo largo de la cadena de suministro.
- b. Para la contratación de servicios o componentes de la Infraestructura de TI y/o Áreas Seguras, se debe exigir a los Proveedores la presentación de los Planes de Contingencia que aseguren la Disponibilidad de la Información, suministrada y procesada entre las partes.

15.2. GESTIÓN DE PRESTACIÓN DE SERVICIO DE PROVEEDORES

15.2.1. Seguimiento y Revisión de los Servicios de los Proveedores

- a. Como parte de la supervisión a la ejecución del contrato, se debe contemplar procesos de auditoría a proveedores cuyo objetivo sea validar el cumplimiento de los requisitos de Seguridad de la Información estipulados en la etapa contractual, dichos resultados deben quedar consignados también en los informes presentados por el supervisor del contrato.

15.2.2. Gestión de Cambios en los Servicios de los Proveedores

- a. Toda gestión del proveedor que represente una modificación, mantenimiento, revisión al Servicio de Tecnología de la Información, Comunicaciones o Equipos de Suministros, debe pasar por el Procedimiento Gestión de Cambios y seguir las directrices del Líder u Oficial de Seguridad de la Información, antes de su ejecución.

- **Excepciones:**

Cualquier excepción a los lineamientos, debe ser justificada por el Área solicitante, el comité evaluador o el supervisor del contrato, según aplique; y aprobada por el Líder u oficial de seguridad de la información de la entidad.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- **Dominio/ Control:** A.16 Gestión de Incidentes de Seguridad de la Información.
- **Objetivo:** Asegurar un enfoque coherente y eficaz para la Gestión de Incidentes de Seguridad de la Información, incluida la comunicación sobre eventos de seguridad y debilidades.

- **Alcance:** La presente Política aplica para todos los Funcionarios, Contratistas, Proveedores y/o Terceros, los cuales deben reportar todo Evento o Incidente de Seguridad de la Información a la mesa de ayuda, a través de los canales oficiales establecidos por la Entidad, y estos a su vez, deben ser gestionados por los responsables de acuerdo con el procedimiento establecido para tal fin.

- **Lineamientos:**
Se debe dar cumplimiento a los siguientes lineamientos:

16.1. GESTIÓN DE INCIDENTES Y MEJORA EN LA SEGURIDAD DE LA INFORMACIÓN

16.1.1. Responsabilidades y Procedimientos

- a. Los Propietarios de los Activos de Información, deben informar a la Oficina de Tecnología de Información del ICA, a través de la mesa de ayuda los Eventos e Incidentes de Seguridad que identifiquen o que reconozcan ante su posibilidad de materialización.
- b. La Oficina de Tecnología de Información, son los únicos autorizados para reportar Incidentes de Seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos Oficiales ante Entidades Externas.

16.1.2. Reporte de Eventos de Seguridad de Información

- a. El ICA, promoverá entre los Funcionarios, Contratista, Proveedores y Terceros, ante la existencia de una anomalía, Evento de Seguridad de la Información (informáticos y no informáticos) en el cual se comprometan:

- Los Recursos Tecnológicos.
- Los Sistemas de Información.
- La Información física.
- Las personas.
- Demás medios en el que se encuentre Información de la Entidad.

Y que afecte uno (1) o más de los Pilares Fundamentales de Seguridad como son: Confidencialidad, Integridad y Disponibilidad de la información; ellos deberá reportar dicha novedad de manera inmediata, a través de los canales de comunicación oficiales definidos por la Entidad.

16.1.3. Reporte de Debilidades de Seguridad de Información

- a. El ICA, promoverá entre los Funcionarios, Contratista, Proveedores y Terceros, ante la existencia de una anomalía, Incidentes de Seguridad de la Información (informáticos y no informáticos) en el cual se comprometan:

- Los Recursos Tecnológicos.
- Los Sistemas de Información.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- La Información física.
- Las personas.
- Demás medios en el que se encuentre Información de la Entidad.

Y que afecte uno (1) o más de los Pilares Fundamentales de Seguridad como son: Confidencialidad, Integridad y Disponibilidad de la información; ellos deberá reportar dicha novedad de manera inmediata, a través de los canales de comunicación oficiales definidos por la Entidad.

16.1.4. Evaluación de los Eventos de Seguridad de la Información y Decisiones Sobre Ellos

- Los Incidentes deben ser atendidos a través de una serie de normas, reglamentos, procedimientos y/o protocolos a seguir, donde se definen las distintas medidas a tomar para identificar, prevenir, priorizar los Incidentes identificados los cuales se les debe documentar, solucionar, realizar seguimiento y posterior cierre por las responsables del equipo de manejo de Incidentes al interior del ICA o Entidades externas según sea el caso; al igual se debe tener en cuenta los aspectos Legales a los cuales se debe dar cumplimiento.

16.1.5. Respuesta a Incidentes de Seguridad de la Información

- El ICA, 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 re-ocurrencia.

16.1.6. Aprendizaje Obtenido de los Incidentes de Seguridad de la Información

- El ICA, Se debe crear bases de conocimiento para los Eventos o Incidentes de Seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los mismos a futuros, partiendo de dichas bases de conocimiento.

16.1.7. Recolección de Evidencia

- El ICA, en caso de conocer la pérdida o divulgación no autorizada de información, los Funcionarios, Contratistas, Proveedores y/o Terceros, deben notificarlo a la Oficina de Tecnología de Información para que se registre y se le dé el trámite necesario.

- Excepciones:

Toda excepción debe ser validada y aprobada por el Jefe de Oficina de Tecnología de Información y el Líder u Oficial de Seguridad de Información o quien haga de sus veces.

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

- **Dominio/ Control:** A.17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio.
- **Objetivo:** La Continuidad de Seguridad de la Información se debería incluir en los Sistemas de Gestión de la Continuidad de Negocio de la Entidad, para que proporcionen los recursos suficientes para dar

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

una respuesta efectiva a los procesos en caso de contingencia o eventos catastróficos que se presenten y que afecten la Continuidad de su Operación.

- **Alcance:** La presente Política establece que el ICA, debe determinar sus requisitos para la Continuidad del Negocio, basados en la planificación, implementación y verificación de los mismos, para todos los procesos de la Entidad.
- **Lineamientos:**
Se debe dar cumplimiento a los siguientes lineamientos:

17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

17.1.1. Planificación de la Continuidad de la Seguridad de la Información

- a. El ICA, debe determinar sus requisitos para la Seguridad de la Información y la Continuidad de la Gestión de la Información en situaciones adversas durante una crisis o desastres.
- b. El ICA a través de la Oficina Asesora de Planeación; debe liderar el Plan de Continuidad del Negocio.
- c. El ICA, debe establecer, documentar y mantener procesos, procedimientos para asegurar el nivel de Continuidad requerido para la Seguridad de la Información durante una situación adversa.

17.1.2. Implementación de la Continuidad de la Seguridad de la Información

- a. La Oficina de Tecnología de Información, debe elaborar el Plan de Recuperación Ante Desastres (DRP) y retorno a la normalidad, para cada uno de los Servicios y Sistemas de Información que tengan un impacto alto en los Procesos del ICA.

17.1.3. Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información

- a. El ICA, debe asegurar la realización de pruebas periódicas del Plan de Recuperación Ante Desastres (DRP) y/o Continuidad de Negocio, verificando la Seguridad de la Información durante su realización y la documentación de dichas pruebas.
- b. El ICA, debe verificar a intervalos regulares los controles de Continuidad de la Seguridad de la Información, implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

17.2. REDUNDANCIA

17.2.1. Disponibilidad de las Instalaciones de Procesamiento de Información

- a. La Oficina de Tecnología de Información, debe asegurar la disponibilidad de instalaciones de Procesamiento de Información del ICA y propender por la existencia de una Plataforma Tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la Entidad.
- b. La Oficina de Tecnología de Información, debe analizar y establecer los requerimientos de redundancia para los Sistemas de Información Críticos para la Entidad y la Plataforma Tecnológica que los apoya.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- c. La Oficina de Tecnología de Información, , debe evaluar y probar soluciones de redundancia Tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Entidad.
- d. La Oficina de Tecnología de Información, a través de sus colaboradores como: Funcionarios, Contratistas y Proveedores, los cuales deben administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Entidad.

- **Excepciones:**

Toda excepción debe ser validada y aprobada por el Jefe de Oficina de Tecnología de Información y el Líder u Oficial de Seguridad de Información o quien haga de sus veces.

18. CUMPLIMIENTO

- **Dominio/ Control:** A.18 Cumplimiento.

- **Objetivo:** Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con Seguridad de la Información y de cualquier requisito de Seguridad.

- **Alcance:** La presente Política establece que se debe dar cumplimiento a los requisitos estatutarios, reglamentarios y contractuales pertinentes, establecidos por la Entidad a través de las Políticas de Seguridad y Privacidad de la Información.

- **Lineamientos:**

Se debe dar dar cumplimiento a los siguientes lineamientos:

18.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

18.1.1. Identificación de la Legislación Aplicable y de los Requisitos Contractuales

- a. La Entidad, identifica y elabora una Matriz de Requisitos Legales vigentes referentes al cumplimiento de Seguridad de la Información.

18.1.2. Derecho de Propiedad Intelectual

- a. La Entidad, implementará los procedimientos a que haya lugar para asegurar el cumplimiento de ley y requerimientos regulatorios y contractuales acerca de la propiedad intelectual, patentes, entre otras.

18.1.3. Protección de Registros

- a. La Entidad, deberá proteger los registros contra pérdida, destrucción, falsificación y acceso no autorizado; para dar cumplimiento a los Requisitos Legales.

18.1.4. Privacidad y Protección de Información de Datos Personales

- **Dominio:** A.18.1.4 Privacidad y Protección de Información de Datos Personales.
- **Objetivo:** Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con Seguridad de la Información, y de cualquier requisito de seguridad.

- **Alcance:** La presente Política aplica para todos los Funcionarios, Contratistas, Proveedores y/o Terceros o que por su rol, tengan bajo su responsabilidad o suministren datos personales a la Entidad. Acional es de libre consulta para los **TITULARES** de dichos datos.
- **Lineamientos:**
Se debe dar cumplimiento de los siguientes lineamientos:
 - a. El ICA en cumplimiento de lo establecido en la normatividad legal vigente aplicable a la privacidad y protección de datos personales en Colombia, actúa como Responsable de los datos personales que por virtud de sus funciones y competencias legalmente establecidas, le han sido suministradas y se encuentran en sus bases de datos siendo cada de una de las dependencias del Instituto él o la Encargado (a) del tratamiento.
 - b. Por tanto, el ICA podrá dar tratamiento a los datos personales de **TITULARES** con los cuales tiene, ha tenido o espera tener algún tipo de relación, cualquiera sea su naturaleza (civil, comercial y/o laboral, etc.) y entre los cuales se incluyen, pero sin limitarse, los grupos de interés (usuarios directos, usuarios indirectos, terceros relacionados y entidades externas).
 - c. Salvo en los casos exceptuados por la ley, el ICA solicitará a más tardar en la recolección de la información, autorización del **TITULAR** para capturar, almacenar, procesar, usar, circular, suprimir y en todo caso tratar los datos personales que hayan sido suministrados a la entidad por cualquier medio, bien sea digital o físico, y en desarrollo de su objeto social o con ocasión de cualquier tipo de relación civil o comercial que llegue a surgir en virtud de sus actividades conexas o propias de su naturaleza; dicha autorización deberá estar contenida en un documento físico o electrónico.
 - d. Para todos los efectos, se entiende que la autorización por parte de los **TITULARES** a favor del ICA para el suministro y/o tratamiento de sus datos personales, realizada a través de los canales físicos o electrónicos, o por escrito o mediante conductas inequívocas, es:
 - **Expresa y voluntaria**, lo que implica que **EL TITULAR** y/o sus representantes, según sea el caso, acepta todo el contenido de la presente y le concede(n) al ICA su autorización para que utilice dicha información personal conforme a las estipulaciones de la presente política, la cual también está publicada en la página web www.ica.gov.co, obligándose a leerla, conocerla y consultarla en desarrollo del derecho que le asiste como **TITULAR** de datos personales.
 - En el evento en que desee manifestar su negativa frente a la mentada autorización o solicitar la supresión de la información, podrá ejercer su derecho a través del correo: contactenos@ica.gov.co, o en cualquiera de los puntos de atención al ciudadano, dentro de los 30 días hábiles siguientes a la implementación y publicación de la Política de Privacidad y Protección de Datos Personales del ICA.
 - Una vez vencido el periodo señalado anteriormente, el Instituto podrá mantener un tratamiento sobre los datos suministrados con anterioridad a esta legislación, en atención a lo consagrado en el numeral cuarto del artículo 10° del Decreto 1377 de 2013, sin perjuicio de la facultad que el **TITULAR** de la Información de ejercer en cualquier momento su derecho a pedir la eliminación del dato.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- No obstante se hace la salvedad que de conformidad al artículo 9 del decreto 1377 del año 2013, la solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el **TITULAR** de esta, tenga un deber legal o contractual de permanecer en la base de datos de la entidad.
- e. Por su parte, el ICA asegura un manejo adecuado de los datos personales recolectados en sus bases de datos, registros de Ingreso a las instalaciones, registro fotográfico, firmas de asistencia, y de más medios de recolección, con el fin de proteger la privacidad de la misma y conservarla bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como el respeto de los derechos del **TITULAR**, según lo estipulado en la ley. De esta manera la entidad manifiesta que garantiza los derechos de privacidad e intimidad en el tratamiento de los datos personales, en consecuencia todas sus actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
- f. Todas las personas que en desarrollo de diferentes actividades, contractuales, laborales, entre otras, sean permanentes u ocasionales, llegaran a suministrar al ICA cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla.
- g. En efecto, el ICA:
- Garantiza al **TITULAR**, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
 - Conserva la información bajo las condiciones de Seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
 - Realiza oportunamente la actualización, rectificación o supresión de los datos en los términos que estipula la ley.
 - Actualiza la información reportada por los Encargados del Tratamiento en los términos que estipula ley.
 - Tramita las consultas y los reclamos formulados por los **TITULARES** en los términos señalados en la ley.
 - Se abstiene de circular información que esté siendo controvertida por el **TITULAR** y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
 - Permite el acceso a la información únicamente a las personas que pueden tener acceso a ello.
 - Informa a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los **TITULARES**.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO GIT-PTI-POL-001 V3
MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	

- Cumple las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

h. Cualquier consulta, reclamo o requisito debe ser dirigido a través de los diferentes sitios y canales de atención dispuestos por el ICA para tal fin, los cuales se pueden consultar en la página web www.ica.gov.co.

- **Excepciones:**

Las excepciones establecidas por Ley.

18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

18.2.1. Revisión Independiente de la Seguridad de la Información

- a. La Entidad, deberá realizar auditoria al Sistema de Gestión de Seguridad de la Información, con el fin de llevar a cabo la mejora continua.

18.2.2. Cumplimiento con las Políticas y Normas de Seguridad

- a. El incumplimiento a la Política de Seguridad y Privacidad de la información de la Entidad, traerá consigo, las consecuencias legales que aplique a la normativa vigente.

18.2.3. Revisión de Cumplimiento Técnico

- a. La Oficina de Tecnología de Información, deberá gestionar y revisar de forma periódica el cumplimiento de las Políticas de Seguridad de Información definidas por la Entidad en los Sistemas de Información.

- **Excepciones:**

Las excepciones establecidas por Ley en caso de aplicar.

19. VIGENCIA DE LAS POLÍTICAS

Las políticas descritas en este documento regirán a partir de la fecha de aprobación y publicación de la misma.