POLÍTICA GENERAL DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LA AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES - ANLA

BOGOTÁ, FEBRERO DE 2018

Contenido

1. GLOSARIO

Activo: Cualquier cosa que tiene valor para la organización.

Activo de Información: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo pueden ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

Administración de Riesgos: Actividades coordinadas para direccionar y controlar una organización con relación a los riesgos.

Análisis de Riesgos (RA): Actividad que permite identificar riesgos, funciones críticas para continuar la operación, controles para reducir la exposición de la organización, evaluar el costo de los controles y las probabilidades de los eventos particulares.

Anti-Virus; Aplicación cuya finalidad es la detección y eliminación de virus, troyanos y gusanos informáticos

Confidencialidad: La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados.

Disponibilidad: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Dispositivo Móvil: dispositivo que acceda a información de la ANLA, entre los que se cuentan: Teléfonos inteligentes (Smartphone), Tabletas (tablets), Computadores portátiles (laptops), Dispositivos basados en Windows Mobile, iOS o Android o Computadores de casa usados para teletrabajo.

Estrategia: Consiste en la formulación, selección e implementación de los procedimientos necesarios para mitigar riesgos, reducir los niveles de exposición y dar respuesta ante desastres.

Gestión del riesgo: Es un proceso de adopción de políticas, estrategias y prácticas orientadas a reducir los riesgos de desastres o minimizar sus efectos. Implica intervenciones sobre las causas que generan vulnerabilidades.

Incidente De Seguridad De La Información: Evento o serie de eventos adversos de seguridad de la información no deseados o inesperados que tienen una probabilidad

significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Política: Intenciones y dirección de una organización expresada formalmente por la alta dirección.

Procedimiento: Vía específica para llevar una actividad o un proceso.

Proceso: Conjunto de actividades interrelacionadas en las que se transforman entradas en salidas.

Propietario: Entendiendo por tal al responsable del activo.

Registro: Conjunto de resultados logrados o evidencia de actividades desarrolladas.

Riesgo: Efecto de un evento sobre los objetivos.

Seguridad De La Información: Adoptar mejores prácticas que permitan reducir los riesgos a los que se expone nuestra información. El propósito de la seguridad de la información es proteger la información de una amplia gama de amenazas para garantizar la continuidad del negocio, minimizar las pérdidas por daños y maximizar las oportunidades de negocios. Principalmente se ocupa de garantizar la confidencialidad, integridad y disponibilidad de la información frente a las amenazas y riesgos que afectan los sistemas de información.

2. OBJETIVOS DE LA POLÍTICA

La **Autoridad Nacional de Licencias Ambientales – ANLA** para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de seguridad de la información de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.

- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas y terceros de la ANLA.
- Garantizar la continuidad del negocio frente a incidentes.

3. ALCANCE DE LA POLÍTICA

La política de seguridad de la información se enmarca sin limitación en:

- Todos los activos de información de la ANLA a través de su ciclo de vida, incluyendo creación, distribución, almacenamiento y disposición final, priorizando su protección acorde con las evaluaciones de riesgos.
- Todos los ambientes de procesamiento de información (producción, desarrollo, pruebas y contingencia).
- Todos los empleados, contratistas y terceros que usen, tengan acceso o sean responsables de la información.
- Todo el personal que diseñe, opere o sea responsable por manejo de información en forma manual o computarizada propiedad de la Entidad o de terceros con los cuales la Entidad tenga vínculo.

4. MARCO NORMATIVO

2002 Directiva Presidencial No. 10 de 2002 Programa de renovación de la Administración Pública: hacía un Estado Comunitario
2002 Ley 790 de 2002 Programa de Reforma de la Administración Pública
2003 CONPES 3248 de 2003 Renovación de la Administración Pública
2003 Decreto 3816 de 2003 Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública
2008 Ley 1266 de 2008 Disposiciones generales de habeas data y se regula el manejo de la información
2009 Ley 1273 de 2009 protección de la Información y los datos
2010 Decreto 235 de 2010 Intercambio de información entre entidades para el cumplimiento de funciones públicas
2012 Ley Estatutaria 1581 de 2012 Protección de datos personales

2014 Decreto 2573 de 2014: Por medio del cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea

2014 Ley 1712 de 2014: Ley de trasparencia y de acceso a la información pública nacional

2015 Decreto 1078 de 2015 Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

2016 Decreto 415 de 2016, por medio del cual se establecen los lineamientos para la implementación de la figura de Director de Tecnologías y Sistemas de Información en las entidades públicas.

5. DECLARACIÓN DE LA POLÍTICA

La Autoridad Nacional de Licencias Ambientales - ANLA recibe, genera y transforma información, dándole la protección necesaria y evitando cualquier pérdida de confidencialidad, integridad o disponibilidad, como parte integral del Sistema de Gestión de Seguridad de la Información implementado al interior de la organización.

Es por ello que la ANLA ha definido e implementado la presente política de seguridad en concordancia con prácticas éticas, cumplimiento regulatorio de la nación y planeación estratégica de la organización y los lineamientos del Modelo de Privacidad y Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

6. DESARROLLO DE LA POLÍTICA

La **Política de Seguridad y Privacidad de la Información** es la declaración general que representa la posición de la **Autoridad Nacional de Licencias Ambientales - ANLA** con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

A continuación, se establecen las 12 políticas de seguridad que soportan el Sistema de Gestión de Seguridad de la Información de la Autoridad Nacional de Licencias Ambientales – ANLA:

1. La **ANLA ha decidido definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.

2. Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas y publicadas al alcance de cada uno de **los empleados, contratistas o terceros**.

3. La **ANLA protegerá la información generada, procesada o resguardada** por los procesos internos y activos de información que hacen parte de los mismos.

4. La **ANLA protegerá la información** creada, procesada, transmitida o resguardada por sus procesos internos, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. La **ANLA protegerá su información** de las amenazas originadas por parte **del personal**.

6. La **ANLA protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

7. La **ANLA controlará la operación** de sus procesos internos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. La **ANLA implementará control de acceso** a la información, sistemas y recursos de red.

9. La **ANLA garantizará que la seguridad** sea parte integral del ciclo de vida de los sistemas de información.

10. **La ANLA garantizará una mejora efectiva de su modelo de seguridad** a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información

11. La **ANLA garantizará la disponibilidad** de sus procesos de internos y la continuidad de su operación con base en el impacto que pueden generar los eventos.

12. La ANLA **garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.**

POLITICAS ISO/IEC 27001:2013

Política de la Seguridad de la Información:

- Toda persona que tenga acceso a información que sea propiedad de la ANLA, debe mantener en estricta confidencialidad e integridad dicha información y no debe compartirla ni modificarla sin la debida autorización.
- Los usuarios, contratistas y terceros deben tener acceso únicamente a los servicios de la red sobre los cuales tienen permiso y que sean necesarios para cumplir con sus actividades laborales de acuerdo a lo establecido en el procedimiento Gestión de Accesos.
- Se debe controlar la conexión remota de usuarios, contratistas y terceros únicamente a los recursos de la red necesarios para ejecutar sus labores de acuerdo a lo establecido en el procedimiento Uso de VPN.
- La Alta Dirección de la entidad dispondrá los recursos administrativos y financieros para proporcionar los elementos requeridos para mantener el Sistema de Gestión de la Seguridad de la Información.
- La Alta Dirección debe velar por el cumplimiento de los requisitos legales o reglamentarios y las obligaciones de seguridad contractuales que soportan las operaciones del negocio.
- La ANLA realizará un programa de concientización en Seguridad de la Información para los usuarios, terceros y contratistas el cual será ejecutado con base en el plan anual de capacitación.
- Los usuarios deben conocer y cumplir la política general de Seguridad de la Información y sus procedimientos.
- La ANLA debe garantizar el nivel de continuidad requerido para la seguridad de la información durante una situación de contingencia.
- La ANLA debe asegurar la privacidad y protección de datos personales como se exige en la legislación.
- La ANLA debe ejecutar la gestión de riesgos, teniendo en cuenta los criterios de valoración de riesgo establecidos.
- Cualquier violación a la política general de Seguridad de la Información y/o a sus procedimientos puede implicar una investigación pertinente.

i. Seguridad de los Recursos Humanos

- Los detalles técnicos de los sistemas de información, tales como direcciones IP, diagramas de red y software/hardware de seguridad empleado, no deben ser

revelados a los candidatos a un empleo del Proceso de Gestión de Tecnología y Seguridad de la Información hasta que no hayan firmado un acuerdo de confidencialidad y hayan sido contratados.

- Toda la información generada por terceros o contratistas para beneficio de la ANLA es propiedad de la Entidad.
- Todos los funcionarios, terceros y contratistas asociados al Proceso de Gestión de Tecnología y Seguridad de la Información deben firmar un acuerdo de confidencialidad, junto con su contrato laboral. Ver Acuerdo de Confidencialidad Área de Tecnología.
- Cuando un funcionario, contratista o tercero deja de prestar sus servicios a la ANLA, debe ser notificado por parte del Grupo de Talento Humano y/o los supervisores del contrato del Proceso de Gestión de Tecnología y Seguridad de la Información.
- El incumplimiento de la política general de seguridad de la información y sus procedimientos será motivo de investigación.
- Se consideran violaciones y objeto de procesos disciplinarios graves, el robo, daño, evasión de entrega de información de los procesos o de carácter administrativo que ponga en riesgo la ejecución normal de las operaciones de la ANLA.

ii. Gestión de Activos

- Los activos de información deben ser identificados y clasificados de acuerdo a la sensibilidad, valor y criticidad de la información que contienen o de acuerdo a la funcionalidad que cumplen.
- Se debe tener control y manejo de la información clasificada como confidencial, la cual debe ser etiquetada con anterioridad por los dueños de la misma.
- La ANLA debe garantizar el uso adecuado del correo, el internet y los recursos de red por parte de sus funcionarios, contratistas y terceros.

iii. Control de Accesos

- Los usuarios, terceros y contratistas únicamente deben tener acceso a las redes y los servicios de red a los que estén autorizados.
- La ANLA debe tener el registro de creación y cancelación de credenciales de usuario, el cual debe coincidir con el inicio y finalización de los contratos laborales.
- La asignación de privilegios sobre carpetas compartidas, recursos de red y conexión por VPN deben ser autorizados por el jefe inmediato del eventual usuario.
- Se debe velar por el uso adecuado de las credenciales asignadas a los usuarios, terceros y contratistas.
- Se debe tener un registro de los cambios realizados a los privilegios de las cuentas de usuario y debe realizarse una revisión periódica.
- Se debe garantizar la eliminación de todos los derechos de acceso a la información al finalizar el contrato laboral.

- Los usuarios, terceros y contratistas deben acogerse a los procedimientos de asignación de contraseñas para ingreso a los sistemas de información y recursos de red.
- Se debe asegurar que las credenciales de acceso a los sistemas de información estén cifradas y que se maneje una política para cambio de contraseña.
- Se deben fomentar las buenas prácticas de uso de contraseñas mediante la realización de campañas de concientización para usuarios internos y externos.
- Se debe restringir el acceso al código fuente de las aplicaciones, de tal forma que no se comprometa la confidencialidad, integridad y disponibilidad de las mismas.
- Se debe asegurar bloqueos a través de herramientas de seguridad para estaciones de trabajo en lo relacionado a accesos vía internet a cuentas bancarias, redes sociales, correos personales, etc.

iv. Criptografía

- Se deben manejar algoritmos de cifrado para comunicación a través de conexión remota a la red de la ANLA.
- Se debe garantizar la integridad de las credenciales de usuario almacenadas en las bases de datos.

v. Seguridad Física y del Entorno

- Las áreas de trabajo en donde se encuentre información sensible deben poseer controles de acceso, los cuales solo permitan acceso al personal autorizado.
- Todo maletín, maleta, bolso o equipaje debe ser revisado por el personal de vigilancia ubicado al ingreso de las instalaciones de la ANLA.
- Todo equipo portátil debe ser registrado e inspeccionado al ingreso y salida de las instalaciones de la ANLA.
- El personal de vigilancia debe asegurarse que todos los funcionarios porten el carné en un lugar visible y verificar la autenticidad del mismo.
- Se debe tener registro de todos los visitantes que se encuentren dentro de las instalaciones de la ANLA y dicho registro debe conservarse al menos por seis meses.
- Todos los funcionarios, contratistas, terceros y visitantes deben portar un carné de identificación visible mientras se encuentren en las instalaciones de la ANLA.
- Se debe tener un Circuito Cerrado de Televisión instalado en todos los ambientes que necesiten ser monitoreados para proteger los activos de información de la ANLA y tener un registro en caso de presentarse algún incidente.
- Se debe contar con un sistema de detección y extinción de incendios que proteja la infraestructura tecnológica de la ANLA, el cual debe ser probado regularmente por profesionales expertos.
- Se deben controlar las condiciones ambientales de temperatura y humedad en el Centro de Datos para no afectar el funcionamiento de la infraestructura.

- El centro de cómputo debe poseer estructuras diseñadas contra desastres naturales, disturbios y problemas relacionados.
- Se deben proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
- El cableado de energía eléctrica y de telecomunicaciones debe cumplir con la norma estándar de cableado estructurado EIA/TIA.
- Se debe realizar mantenimiento preventivo a nivel físico y lógico para los equipos al menos una vez al año.
- Se deben aplicar medidas de seguridad para el uso de equipos de cómputo por fuera de la ANLA, teniendo en cuenta los riesgos de trabajar fuera de dichas instalaciones.
- Se debe asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito antes de reusar un equipo que contenga medios de almacenamiento.
- Se debe asegurar que los equipos desatendidos se les da la protección adecuada para evitar accesos no autorizados a los mismos y robo de información.

vi. Seguridad de las Operaciones

- Se deben documentar los procedimientos de operación en el sistema de gestión de la Entidad y ser socializados a todo el personal del Proceso de Gestión de Tecnología y Seguridad de la Información.
- Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad debe ser controlado, gestionado y autorizado adecuadamente por el Líder del proceso de gestión de Tecnologías y Seguridad de la Información.
- Todo cambio sobre las plataformas críticas que administran información de los procesos núcleo (core) del negocio, debe ser sometido a una evaluación por parte del Líder del proceso de gestión de Tecnologías y Seguridad de la Información y su equipo de trabajo para identificar los riesgos, impacto y afectación de la operación de la organización, de acuerdo con el procedimiento de Control de Cambios.
- Se debe hacer seguimiento al uso de los recursos, hacer los ajustes y proyecciones de los requisitos de capacidad futura para asegurar el desempeño requerido de cada uno de los sistemas que conforman la plataforma de tecnología, de acuerdo al procedimiento Gestión de Capacidad.
- Se debe manejar ambiente de desarrollo, pruebas y producción para reducir los riesgos de cambios no autorizados.
- Se deben implementar protecciones contra códigos maliciosos, deben estar basadas en la detección de malware y reparación de software.

- Se debe prohibir el uso de software no autorizado mediante bloqueo por antivirus o control de aplicaciones y restringir el acceso a sitios web con contenido malicioso a través de perfiles de navegación.
- Se deben realizar copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba con regularidad de acuerdo a lo establecido en la Política de Generación y Restauración de Copias de Respaldo.
- Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información respaldada.
- Se deben elaborar, conservar y revisar regularmente los registros de las actividades de los usuarios y eventos de seguridad de la información.
- Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
- Las actividades de los titulares de cuentas de usuarios privilegiados (administradores y operadores) se deben registrar y los registros se deben proteger y revisar con regularidad.
- Se deben implementar reglas para controlar los privilegios otorgados para instalación de software por parte de los usuarios.

vii. Seguridad de las Comunicaciones

- Se deben implementar los controles necesarios para garantizar la seguridad de la información digital y la protección de los sistemas y aplicaciones de accesos no autorizados.
- Se deben identificar las medidas de seguridad necesarias para todos los servicios de red, como los niveles de servicio y los requisitos de gestión, ya sea que los servicios se presten internamente o se contraten externamente.
- La red debe ser segmentada en redes virtuales (VLAN) diferentes para proteger el acceso entre dominios de red.
- Los medios transportados fuera de las instalaciones de la ANLA, deberán cumplir con los controles establecidos y las normas aplicables para tal fin.
- Cualquier información solicitada telefónicamente no debe ser revelada por este medio, a menos que la persona que llama es capaz de identificarse de manera positiva a través de un secreto compartido o a través de otras medidas de identificación de llamadas aprobadas.
- Se debe proteger la seguridad de la información en la mensajería electrónica contra acceso no autorizado, modificación o denegación de servicio acorde con el sistema de clasificación adoptado por la ANLA.
- Los acuerdos de confidencialidad que se firmen entre la ANLA y sus contratistas y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la organización, deben tener 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.

viii. Adquisición, Desarrollo y Mantenimiento de Sistemas

- Los requisitos de seguridad de la información deben integrarse en las primeras etapas de los proyectos de sistemas de información o para mejoras de los mismos.
- Los servicios de las aplicaciones que estén publicados en Internet se deben proteger de actividades fraudulentas y modificación no autorizada.
- Se debe garantizar la confidencialidad, protección e integridad de la información involucrada en las transacciones de los servicios de las aplicaciones para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de los mensajes y la divulgación y reproducción no autorizada.
- Todos los sistemas de información desarrollados o adquiridos, deberán cumplir con los requisitos mínimos de seguridad. El cumplimiento de estos requisitos deberá incluirse y revisarse desde el proceso de diseño de la aplicación.
- Antes que un nuevo sistema de información sea desarrollado o adquirido, los usuarios funcionales deberán especificar con claridad los requisitos de seguridad pertinentes. Con base en estos, la Subdirección Administrativa y Financiera definirá las herramientas tecnológicas que cumplirán con estos requisitos.
- Los cambios a los sistemas deben evaluarse, valorar los riesgos, analizar los impactos y se especificar los controles de seguridad necesarios, de acuerdo al procedimiento Control de Cambios.
- Se deben manejar ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
- Se debe realizar supervisión y seguimiento a las actividades de desarrollo de sistemas contratados externamente.
- Todos los sistemas de información nuevos, las actualizaciones y las nuevas versiones deben someterse a pruebas de aceptación que se deben incluir en la prueba de los requisitos de seguridad de la información y adherencia para asegurar prácticas de desarrollo del sistema.

ix. Relaciones con los Proveedores

- La ANLA debe identificar y ordenar los controles de seguridad de la información para el acceso de terceros a los servicios de red y a la información de la organización.
- Los terceros no deben tener ningún privilegio de acceso a los sistemas de información de la ANLA a menos que el propietario de la información haya autorizado dicho acceso.

- El acceso de terceros a información interna debe ser otorgada sólo ante una necesidad demostrable, y cuando tal divulgación haya sido expresamente autorizada.
- Los accesos remotos de proveedores deben estar documentados argumentando la razón de dicho acceso y deben ser habilitados únicamente por el tiempo que sea necesario para la actividad que debe resolver el proveedor.
- La ANLA debe monitorear y revisar los servicios que prestan los terceros y contratistas y asegurarse que los términos y condiciones de los acuerdos en seguridad de la información se están cumpliendo y además que los incidentes y problemas de seguridad de la información se gestionan adecuadamente.

7. CUMPLIMIENTO

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

8. MEDICIÓN

Para garantizar la efectividad en la implementación y cumplimiento de las políticas de seguridad de la información, el Líder del proceso de gestión de Tecnologías y Seguridad de la Información realizará una verificación mediante indicadores de gestión apropiados para cada política particular.

9. RESPONSABLE

Líder del proceso de gestión de Tecnologías y Seguridad de la Información.

10. REVISIÓN, CAMBIOS Y/O ACTUALIZACIONES

La Subdirección Administrativa y Financiera, la Oficina Asesora de Planeación y el Proceso de Gestión de Tecnología y Seguridad de la Información realizará una revisión a la política enunciada dos (2) vez al año durante el último trimestre con el apoyo de las áreas que considere convenientes para determinar su conveniencia u

obsolescencia, posteriormente, se someterá a revisión de manera planeada con el fin de asegurar su idoneidad, eficiencia y efectividad.

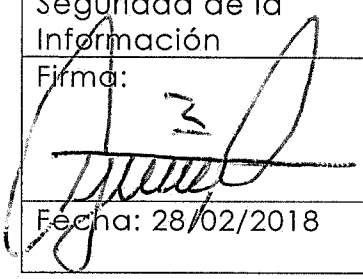
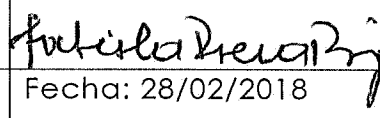
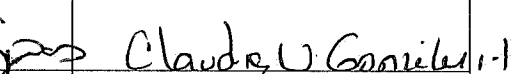
Cualquier funcionario, aliado, contratista, proveedor y otros terceros vinculados con la Entidad que considere que la información administrada se encuentra vulnerable en cuanto a su idoneidad, eficiencia y/o efectividad, podrá solicitar por medio de la mesa de ayuda al Proceso de Gestión de Tecnología y Seguridad de la Información la realización de cambios y/o actualizaciones a la política de seguridad de la información aquí enunciada.

11. CONTRAVENCIONES

Cualquier funcionario, aliado, contratista, proveedor y otros terceros vinculados con la Entidad que incurran en faltas relacionadas con la seguridad de la información y/o que contravengan la política de seguridad aquí enunciada o cualquiera de sus partes complementarias, incurrirá en falta grave, por lo cual le será retirado de manera temporal cualquier privilegio como propietario, usuario o administrador de los sistemas de información de la Entidad, así como la posibilidad de acceder a equipos y/o instalaciones de la Entidad hasta tanto sea adelantada la investigación administrativa correspondiente.

12. CONTROL DE CAMBIOS

FECHA	VERSIÓN DE LA POLÍTICA QUE MODIFICA	VERSIÓN ACTUAL DE LA POLÍTICA	MOTIVO DE LA MODIFICACIÓN
09/12/2016	1	1	Creación
23/08/2017	1	2	Actualización
16/02/2018	2	3	Actualización

Elaboró:	**Revisó:**	**Aprobó:**
Miguel José Cantillo Wandurraga	Dra. Fabiola Rivera Rojas	Dra. Claudia Gonzalez Hernández
Cargo: Líder del proceso de gestión de Tecnologías y Seguridad de la Información	**Cargo:** Subdirectora Administrativa y Financiera	**Cargo:** Directora General
Firma: 	Firma: 	Firma: 
Fecha: 28/02/2018	Fecha: 28/02/2018	Fecha: 28/02/2018