MANUAL DE SEGURIDAD DE LA INFORMACIÓN

PROCESO

Gestión Estratégica de Tecnologías de la Información

Versión 2

08/08/2019

Contenido

1. INTRODUCCION

Con el aumento en el número de incidentes de seguridad de la información en las entidades, los cuales generan pérdidas financieras, de imagen, de información y datos así como la generación de reprocesos administrativos, se crea la necesidad de implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información (SGSI) donde se diseñen, documenten, implementen y monitoreen controles basados en una gestión de riesgos que minimice el impacto o la probabilidad de ocurrencia, a fin de mantenerlos en niveles aceptables para la entidad.

El Ministerio de Ambiente y Desarrollo Sostenible decide establecer, implementar, hacer seguimiento, mantener y mejorar un SGSI; por ello es necesario construir un manual de seguridad de la información que consolida la normatividad, alcance, política, grupo operativo y la metodología de gestión de riesgo del SGSI.

2. OBJETIVO DEL DOCUMENTO

Proporcionar un panorama general del Sistema de Gestión de Seguridad de la Información del Ministerio de Ambiente y Desarrollo Sostenible.

3. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Protección de los activos de información del Ministerio de Ambiente y Desarrollo Sostenible ubicado en la sede de Bogotá, Calle 37 No. 8 – 40, de acuerdo con la versión vigente de la declaración de aplicabilidad.

4. NORMATIVIDAD

La norma internacional ISO 27001 contiene los estándares para implementar la gestión de la seguridad de la información permitiendo el aseguramiento, la confidencialidad e integridad de los datos, así como de los sistemas que la procesan basándose en la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

En este sentido el marco de referencia normativo lo estipulan las leyes: 1753 de 2015 por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”. En su art.159 que modifica el art.227 de la ley 1450 del 2011 “Obligatoriedad de suministro de información. Para el desarrollo de los planes, programas y proyectos incluidos en el Plan Nacional de Desarrollo y en general para el ejercicio de las funciones públicas, las entidades públicas y los particulares que ejerzan funciones públicas, pondrán a disposición de las entidades públicas que así lo soliciten, la información que generen, obtengan, adquieran o controlen y administren, en cumplimiento y ejercicio de su objeto misional. El uso y reutilización de esta información deberá garantizar la observancia de los principios, normas de conformidad con lo dispuesto en las Leyes 1581 del 2012 Protección de datos personales y la ley 1712 del 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, así como las demás normas que regulan la materia. Además el suministro de la información será gratuito, y Las entidades públicas propenderán por la integración de los sistemas de información para el ejercicio eficiente y adecuado de la función pública.

También los decretos 1078 del 2015 por medio del cual se expide "El Decreto Único Reglamentario del Sector de Tecnologías de la información y las comunicaciones" en su título 9 "Políticas y Lineamientos de Tecnologías de la Información", el Decreto 1499 del 2017 por medio del cual se modifica el Decreto 1083 del 2015 Decreto único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la ley 1753 del 2015" en su capítulo 2 "Políticas de Gestión y Desempeño institucional en su art. 2.2.22.2.1 que hace referencia a las "Políticas de Gestión y Desempeño Institucional" dentro de las cuales se encuentran numeral "11. Gobierno Digital, antes Gobierno en línea, 12. Seguridad Digital". Y los últimos el Decreto 1413 del 2017 en su título 17 establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales y el Decreto 612 del 2018 en su numeral "2.2.22.3.14 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado que deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:

- Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información

Adicionalmente, el documento CONPES 3701 del 2011 brinda los lineamientos de política para ciberseguridad y ciberdefensa, que busca fortalecer las capacidades del estado para afrontar las diferentes amenazas y mitigar el impacto de las mismas, y el documento CONPES 3854 del 2017 de la Política de seguridad digital, establece nuevos lineamientos y directrices sobre el tema teniendo en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.

5. TERMINOS Y DEFINICIONES

Establecer las normas que se deben cumplir en cuanto a la clasificación, manejo y etiquetado de la información, con el fin de asegurar que reciba el nivel de protección adecuado de la información de MINAMBIENTE.

Aceptación del Riesgo	Decisión informada de asumir un riesgo en particular. [ISO/IEC 27000:2018]
Activo	Cualquier cosa que tenga valor para la organización. [ISO/IEC 13335-1:2004].
Activo de Información	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, hardware, software, sistemas de información, edificios, personas, imagen, etc.) que tenga valor para el Ministerio de Ambiente y Desarrollo Sostenible.
Amenazas	Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. [ISO/IEC 27000:2018]
Análisis del riesgo	Proceso de comprender la naturaleza del riesgo y determina el nivel de riesgo. [ISO/IEC 27000:2018]. Busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias,

	calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.
Comunicación y consulta del riesgo	Conjunto de procesos continuos e iterativos que una organización realiza para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas sobre la gestión del riesgo. [ISO/IEC 27000:2018].
Confidencialidad	Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000:2018].
Control	Medida que modifica el riesgo. [ISO/IEC 27000:2018]. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
Disponibilidad	Propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000:2018].
Estimación del riesgo	Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
Evaluación del riesgo	Proceso de comparar los resultados del análisis de riesgo con criterios de riesgo para determinar si el nivel de riesgo o magnitud es aceptable o tolerable. [ISO/IEC 27000:2018].
Evento	Aparición o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000:2018].
Eventos en seguridad de la información	Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser la pertinente a seguridad. [ISO/IEC 27000:2018].
Gestión de Incidentes de Seguridad de la Información	Procesos para detectar, informar, evaluar, responder, tratar, y aprender de los incidentes de seguridad de la información. [ISO/IEC 27000:2018].
Gestión del riesgo	Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. [ISO/IEC 27000:2018].
Identificación del riesgo	Proceso para encontrar, reconocer y describir los riesgos. [ISO/IEC 27000:2018].
Impacto	Cambio adverso en el nivel de los objetivos del negocio logrado.
Incidente en seguridad de la información	Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información. [ISO/IEC 27000:2018].
Integridad	Propiedad de exactitud y completitud. [ISO/IEC 27000:2018].
Nivel de Riesgo	Magnitud del riesgo expresada en términos de la combinación del impacto y la probabilidad. [ISO/IEC 27000:2018].
Política	Intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000:2018].
Probabilidad	Posibilidad de que algo suceda. [ISO/IEC 27000:2018].
Propietario del riesgo	Persona o entidad con la responsabilidad y autoridad para gestionar un riesgo. [ISO/IEC 27000:2018].
Riesgo	Efecto en la incertidumbre de los objetivos [ISO/IEC 27000:2018].

Riesgo residual	Riesgo restante después del tratamiento del riesgo. [ISO/IEC 27000:2018].
Tratamiento del riesgo	Proceso de modificar el riesgo. [ISO/IEC 27000:2018].
Valoración del riesgo	Proceso general de identificación, análisis y evaluación de riesgos. [ISO/IEC 27000:2018].
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas. [ISO/IEC 27000:2018].

6. GRUPO OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN

El grupo operativo de seguridad de la información se encarga de definir el alcance, gestionar, planificar, controlar y verificar los procesos del SGSI. El grupo operativo es primordial en la implementación del SGSI ya que es el ente que regula cualquier cambio dentro del sistema de gestión, siempre apuntando a una mejora continua.

Las funciones del grupo operativo son las siguientes:

- Revisar periódicamente el estado general de la seguridad de la información, mínimo una vez al año.
- Revisar y monitorear los incidentes de seguridad de la información.
- Revisar, actualizar y escalar a la Alta Dirección las políticas de seguridad de la información del SGSI.
- Realizar otras actividades de alto nivel (p. ej. Estrategias, planes, proyectos, entre otros) relacionadas con la seguridad de la información.
- Establecer proyectos especiales para la identificación de amenazas potenciales.
- Evaluar la eficacia de las medidas tomadas.
- Elaborar un plan de formación y sensibilización en seguridad de la información.
- Presupuestar los recursos necesarios.
- Planificar auditorías internas periódicas del SGSI.
- Concertar las medidas o controles de seguridad en el procesamiento de la información.
- Validar jurídicamente las medidas o controles a implantar.
- Reportar al Comité Institucional de Gestión y Desempeño sobre eventos e incidentes de seguridad y el estado general de seguridad de la información.

En el anexo 1 se muestra la matriz de roles y responsabilidades de los integrantes del grupo operativo de la seguridad de la información.

7. POLÍTICAS DEL SGSI

7.1. Política General del SGSI

En cumplimiento de su objeto misional, la normativa vigente y con criterios técnicos, el Ministerio de Ambiente y Desarrollo Sostenible, como rector del Sistema Nacional Ambiental, se compromete a garantizar la satisfacción de las partes interesadas, hacer un uso eficiente de sus recursos y preservar la confidencialidad, integridad y disponibilidad de la información, bajo un enfoque de prevención de riesgos, mejora continua y autocontrol en los procesos y en la prestación de los servicios, con el apoyo de un equipo humano competente y comprometido.

Como objetivos específicos para el cumplimiento de la Política y del objetivo estratégico del SGSI se tiene:

- Sensibilizar al personal del Ministerio de Ambiente y Desarrollo Sostenible en seguridad de la información.
- Gestionar los incidentes de seguridad de la información que atenten contra la confidencialidad, integridad y disponibilidad de los activos de información del Ministerio de Ambiente y Desarrollo Sostenible.

Las revisiones de la Política de Seguridad de la Información del Ministerio de Ambiente y Desarrollo Sostenible, al considerarse una política integrada, será revisada bajo la periodicidad definida por el Sistema Integrado de Gestión o cuando se presenten cambios significativos en el Ministerio tales como:

- Objetivos tanto del Sistema de Gestión de Seguridad de la información, como en el cumplimento de los objetivos misionales de MINAMBIENTE o cambios en los procesos relacionados.
- Cambios en la tecnología.
- Condiciones contractuales, regulatorias o legales.

7.2. Políticas Específicas del SGSI

Frente a formulación e implementación de las políticas del Sistema de Gestión de Seguridad de la Información es importante tener en cuenta las siguientes responsabilidades:

- El Comité Institucional de Gestión y Desempeño debe aprobar las Políticas de Seguridad de la Información, demostrando así su compromiso con el SGSI en el Ministerio del Ambiente y Desarrollo Sostenible. Una vez aprobadas las políticas de seguridad de la información, éste comité debe velar por su divulgación y cumplimiento al interior de la entidad.
- Así mismo, debe revisar periódicamente la aplicabilidad y vigencia de las políticas específicas de seguridad de la información y efectuar los ajustes necesarios sobre ellas, para que sean funcionales y se pueda seguir exigiendo su cumplimiento por parte de todos los funcionarios, contratistas y proveedores de la Entidad.
- Todos los Integrantes del Comité Institucional de Gestión y Desempeño, Funcionarios de Carrera, Funcionarios Provisionales, Contratistas, Servidores públicos en general o Terceros/Proveedores relacionados, son responsables de la implementación de las Políticas de Seguridad de la Información.
- Las Políticas de Seguridad de la Información son de carácter obligatorio para todo el personal de la entidad, cualquiera sea su situación laboral, el proceso al que pertenece y cualquiera que sea el nivel organizacional en el que se encuentre y es responsabilidad de la Alta Dirección velar por su divulgación y cumplimiento.
- El Grupo Operativo de Seguridad de la Información deberá revisar y proponer al comité Institucional de Gestión y Desempeño para su aprobación las políticas de seguridad de la información y las funciones generales en materia de Seguridad de la Información.

- El Oficial de Seguridad de la Información (O personal asignado, encargado o quién ejerza su rol, bien sea una o varias personas), será el responsable de coordinar e impulsar los temas relacionados con la Seguridad de la Información, velando por la implementación y cumplimiento de la Políticas tanto del SGSI, como de las políticas específicas de seguridad de la información.
- Los usuarios de la Información y de los Sistemas utilizados para su procesamiento son responsables de conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente y las políticas específicas y procedimientos que de ésta se deriven.
- El proceso de Evaluación Independiente deberá de practicar auditorías sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por las políticas, procedimientos y prácticas que de ella surjan.
- El seguimiento al tratamiento de riesgos y a la gestión de los mismos, lo realiza la Oficina de Control Interno bajo los criterios aplicados y definidos por el Departamento Administrativo de la Función Pública.
- El seguimiento a planes de Mejoramiento se controlará teniendo en cuenta los lineamientos establecidos en el SIG. Se realizarán de igual manera auditorías externas y para el control técnico.
- El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

7.2.1. Organización de la Seguridad de la Información

El Ministerio de Ambiente y Desarrollo Sostenible debe definir responsabilidades y deberes con respecto a la seguridad de la información, y asegurar la concientización de servidores públicos, contratistas y terceros/proveedores con respecto a la importancia y el cumplimiento de los lineamientos internos y la normatividad legal vigente.

Toda tarea o actividad en la cual los servidores públicos o contratistas tengan acceso a la infraestructura tecnológica o a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la entidad. Los sistemas de información del Ministerio deben contar y permitir gestionar roles y permisos y en la medida de lo posible sincronizar el acceso con el Directorio Activo.

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios o actualizaciones a los sistemas existentes en MINAMBIENTE, (Nuevos proyectos o mejoras a los actuales) deben contar con la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor se debe ser realizar con las partes interesadas, incluyendo seguridad de la información mediante la metodología de cambios de acuerdo con el alcance.

El uso de dispositivos móviles para trasmitir, recibir, procesar o almacenar información es responsabilidad de cada servidor público y deberá velar por la seguridad de la información, en caso de incurrir en un incidente de seguridad debe informar a la entidad, si existen consecuencias que

afecten el cumplimiento normativo, organizacional o legal, se aplicará el proceso disciplinario vigente de la entidad.

Es obligación del usuario de tecnología móvil con información sensible del Ministerio informar a través de Aranda o mediante comunicación formal, la pérdida o extravío del dispositivo de la forma más rápida posible, para que se realice un análisis de riesgos y tomar acciones para mitigar cualquier impacto no deseado.

Las comunicaciones externas a la infraestructura de la entidad deben realizarse por canales seguros que garanticen la confidencialidad de los datos de acceso y la comunicación que se transfiere y deberá ser aprobada por el líder del proceso de gestión de información y comunicaciones.

El uso remoto de los activos de información y la Computación móvil será realizado a través de VPN, bajo una autorización previa del Coordinador del Grupo de Sistemas y será creada por el personal de apoyo de tecnología designado para tal función.

7.2.2. Seguridad en Recursos Humanos

Selección de Personal

El Ministerio establece controles para asegurar que todos los servidores públicos se les aplique los controles de seguridad de la información definidos en el proceso de ingreso y se les presente las responsabilidades en seguridad de la información durante el proceso de inducción.

Los servidores públicos que se vinculen al Ministerio son seleccionados de acuerdo con los requisitos del manual específico de funciones de la organización y según los requerimientos específicos para la seguridad de la información definidos.

Al momento de la vinculación, el proceso de gestión humana también realizará la inducción a los empleados y contratistas en los siguientes temas:

- Políticas de seguridad de la información
- Objetivos de seguridad de la información
- Lineamientos de seguridad de la información

Durante la ejecución

Se deben implementar capacitaciones y divulgaciones del SGSI. Los servidores públicos deben conocer la normativa relacionada con la seguridad de la información del Ministerio de Ambiente y Desarrollo Sostenible ya que el desconocimiento de la misma no los exonerará de los procesos disciplinarios definidos ante violaciones de las políticas de seguridad.

El proceso de Gestión Humana, con el apoyo del responsable de seguridad de la Información, incluirá lo pertinente del tema de seguridad de la información en el plan de capacitación anual y será divulgado a los empleados y contratistas de la organización.

Los incidentes de seguridad deben ser reportados al oficial o líder de seguridad de la información. Cuando en un incidente de seguridad de la información se determine un grado de culpabilidad o responsabilidad por parte de los empleados y contratistas, la organización tomará las acciones pertinentes.

Terminación y cambio de empleo

El Ministerio establece los controles para proteger los intereses de la entidad como parte del proceso de cambio de cargo, perfil o en la terminación laboral.

Los cambios de funciones en los servidores públicos deben estar guiados por procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, y la posterior entrega de los mismos (activos) de acuerdo con su nuevo rol.

El líder del proceso de gestión humana del Ministerio informará al proceso de Gestión de Servicios de Información y Soporte Tecnológico GTI, mediante el diligenciamiento del respectivo formato y la aplicación Aranda, los retiros del personal y las novedades administrativas, para el bloqueo o eliminación de datos de acceso y cuentas de correo.

En casos de desvinculación inmediata, el aviso de retiro por parte de gestión humana o del jefe del funcionario debe ser inmediato a través del medio más ágil para ello.

7.2.3. Gestión de activos de información

El Ministerio tiene identificados y clasificados los activos de información y asigna los respectivos responsables para su protección y custodia.

Todos los servidores públicos serán responsables de proteger la información a la cual accedan o procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

Los líderes de proceso son los responsables de identificar, actualizar e informar al oficial o líder de seguridad o quién haga sus veces en la entidad, sobre nuevos activos de información en el proceso o comunicar cambios que se presenten en los actuales.

Cada usuario es responsable de dar uso adecuado y en ningún momento el activo puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros.

Cualquier servidor público que intente inhabilitar, vencer o sobrepasar los controles de seguridad de la información en forma no autorizada será sujeto de las acciones legales correspondientes y al proceso disciplinario de la entidad.

Las cuentas de correo electrónico serán creadas únicamente por el proceso de Gestión de servicios de Información y Soporte Tecnológico GTI, previa justificación de la necesidad por parte de los usuarios, a través del aplicativo Aranda y con el procedimiento correspondiente.

Se debe promover el buen uso de los activos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data, y la protección de los datos de sus propietarios o custodios.

Uso adecuado del Software

Los usuarios no deben efectuar ninguna de las siguientes actividades:

- Copiar software licenciado del Ministerio para utilizar en sus computadores personales o en cualquier tipo de dispositivo diferente a los autorizados por el Ministerio, cualquiera sea su ubicación.
- Intentar instalar software no autorizado por el Ministerio, en cualquier computador o servidor de la organización, sin autorización expresa del Coordinador del Grupo de Sistemas o a quién haga de líder del proceso de gestión hardware, software y canales de comunicaciones de datos.
- Introducir programas maliciosos en las redes o a los servidores (ejemplo: virus informáticos, gusanos, troyanos, spyware, adware, puertas traseras, spam, phishing, pharming, ataques DDOS, keyloggers o cualquier otro tipo de malware).

Uso de recursos tecnológicos

- Los servidores públicos o contratistas bien sean directos o por Outsourcing, no deben realizar soporte técnico a activos tecnológicos que no hagan parte de la entidad.
- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, fondo de pantalla y protector de pantalla institucional.
- Los servidores públicos o contratistas previamente autorizados por la coordinación del grupo de sistemas, que tengan acceso controlado mediante usuario y contraseña o registro de IP/MAC a las comunicaciones inalámbricas, deberán dar uso adecuado en los términos legales y en concordancia con las políticas del presente manual, de este activo tecnológico.
- Los usuarios deben cerrar la sesión activa en el equipo de cómputo al dejar el puesto de trabajo o bloquearla mediante las teclas Windows + L para un bloqueo manual, el bloqueo se debe realizar incluso para periodos de ausencia cortos.
- Todos los escritorios de los servidores públicos del Ministerio de Ambiente y Desarrollo Sostenible se deben mantener despejados y libres de información pública reservada o pública clasificada en ausencia de este.
- El escritorio virtual de cada equipo de cómputo independiente del sistema operativo que use debe mantenerte despejado, no debe contener archivos de ningún tipo salvo los accesos directos a aplicaciones necesarias en la labor del servidor público o contratista.
- El Grupo de Sistemas implementa el bloqueo automático de la sesión de usuario a través del directorio activo (LDAP) al transcurrir 10 minutos de inactividad en el equipo de cómputo.

Uso de Correo electrónico

- El proceso para solicitar acceso a los buzones de correo de servidores públicos que ya no pertenecen a la organización será por medio de autorización o solicitud expresa y escrita del líder de proceso interesado, quién enviará un ticket mediante Aranda o mediante correo electrónico al Coordinador del Grupo de Sistemas, solicitando el acceso.

- Es responsabilidad del usuario realizar constantemente la depuración de su correo electrónico, tanto a los correos enviados como los recibidos y los que se encuentran en la papelera de reciclaje.
- Ningún usuario debe permitir a otro usuario enviar correos electrónicos utilizando su cuenta. Las cuentas asignadas son únicas e intransferibles. Cada servidor público o contratista es responsable del alcance de las acciones o uso de cada una de ellas.
- El mantenimiento del buzón de correo electrónico y la lista personal de direcciones de correo en cada computador, será responsabilidad del usuario.
- La cuenta de correo electrónico institucional asignada al usuario, sólo podrá ser utilizada para el desempeño de las funciones en la entidad en el marco del cumplimiento de los objetivos institucionales.
- Los mensajes y la información contenida en los buzones de correo electrónico, así como los archivos adjuntos, son propiedad del Ministerio de Ambiente y Desarrollo Sostenible y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones laborales.
- No se debe utilizar la dirección de correo electrónico de la organización, como punto de contacto en redes sociales, comerciales o cualquier otro sitio que no esté directamente relacionado con las actividades laborales.
- No está permitido crear o enviar cadenas de correo electrónico, mensajes con contenido religioso, político, racista, pornográfico, publicitario no institucional, o que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, organizaciones sociales, de derechos humanos o que promuevan cualquier partido político, así como los datos relativos a la salud, a la vida sexual y los datos biométricos, sin que los mismos estén autorizados a ser tratados, por los titulares de la información de conformidad con Ley 1581 de 2012, y demás normas que las adicionen, aclaren y modifiquen.
- No está permitido el envío de archivos que contengan extensiones ejecutables.
- No está permitido el envío de archivos de música y videos exceptuando la necesidad de suplir comunicaciones institucionales. En caso de requerir hacer un envío de este tipo de archivos, deberá ser autorizado por el líder del proceso al que pertenece y la coordinación del grupo de sistemas.
- El Ministerio sólo permitirá la radicación de correos electrónicos sobre el sistema de gestión documental implementado (SIGDMA), con archivos de acuerdo con las extensiones permitidas en el Anexo 1. Formatos de archivos de uso común, del documento: Gestión de Documentos y Expedientes Electrónicos – Guía Técnica numeral A13.2.3 de la norma ISO 27001

Clasificación de los activos

- Los líderes de proceso deben realizar la clasificación y calificación en términos de seguridad de los activos de información a su cargo con la ayuda de oficial de seguridad o quien haga sus veces en la entidad.
- Los niveles de clasificación de la información en el Ministerio, atendiendo a lo estipulado en la Ley de transparencia y del derecho de acceso a la información Pública Nacional, Ley 1712 del 6 de marzo de 2014, donde se establece el Principio de máxima publicidad para titular universal, artículo 2: “Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o

legal, de conformidad con la presente ley" y el cumplimiento del artículo 5, literal a), de la misma ley, "Toda entidad pública, incluyendo las pertenecientes a todas las Ramas del poder público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en orden nacional, departamental, municipal y distrital".

- Los niveles de clasificación de la información del Ministerio permiten identificar las características de protección, manejo y tratamiento de la información en cuanto a: niveles de acceso, métodos de distribución, restricciones en la distribución, almacenamiento, archivado, disposición y destrucción.
- Se establecen los siguientes niveles de clasificación en el Ministerio:

Información Pública: Se permite cualquier medio de divulgación o trasmisión que normalmente utilice el MINAMBIENTE, Se almacena en cualquier medio físico o magnético sin ningún tipo de protección. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o samiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014. Solo deben tener acceso los funcionarios explícitamente autorizados.

Información Pública Reservada: Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley (1712 de 2014). Para su transmisión por medios electrónicos es obligatorio solicitar acuse de recibo al destinatario. Se debe mantener guardar en un medio protegido con controles de acceso o si se encuentra en medio físico debe estar bajo llave de manera que solo esté para el acceso al propietario.

Manejo de Medios

El Ministerio mantendrá controles para prevenir o monitorear la divulgación, modificación, retiro o destrucción no autorizada de la información que se encuentra almacenada en los medios removibles que pertenecen a la organización.

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura tecnológica del Ministerio, está autorizada únicamente para servidores públicos o contratistas que por su perfil de cargo y funciones lo requiera.

El Ministerio de Ambiente y Desarrollo Sostenible, se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente.

Los líderes de proceso mediante requerimiento formal podrán solicitar al Grupo de Sistemas el back up de la información contenida en medios removibles.

7.2.4. Control de Acceso

Deben establecerse medidas de control de acceso al sistema operativo, para garantizar la autenticación de los servidores públicos o contratistas.

Los servidores públicos no deben utilizar ninguna estructura o característica de contraseña que pueda dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.

La longitud mínima de las contraseñas será igual o superior a ocho caracteres y estarán constituidas por combinación de caracteres numéricos, especiales y alfabéticos (letras mayúsculas y minúsculas).

Todos los usuarios con acceso a un sistema de información o a la red informática de la entidad dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña, serán responsables de las acciones realizadas por el usuario que les ha sido asignado.

El acceso a la información del Ministerio deberá ser otorgado sólo a Usuarios autorizados, los permisos y niveles de acceso deben estar basados en concordancia a lo que sea requerido de acuerdo con la necesidad expresa para la realización de las tareas relacionadas bajo su responsabilidad. El Ministerio de ambiente y Desarrollo Sostenible asignara en primera instancia acceso basado en mínimo privilegio.

El acceso a la información en producción del Ministerio debe hacerse únicamente por los aplicativos y sistemas autorizados. En ningún caso la información puede ser accedida directamente o por facilidades en los ambientes de desarrollo o pruebas.

La asignación de privilegios a las aplicaciones informáticas presentes en el Ministerio de Ambiente y Desarrollo Sostenible debe ser solicitada por el Líder de Proceso o jefe inmediato del área solicitante al Grupo de Sistemas para que se realicen las asignaciones necesarias.

El oficial o líder de seguridad de la información con el apoyo del grupo de infraestructura revisará los privilegios de acceso de los empleados a los sistemas de información al menos una vez al año.

Si entes externos (Exceptuando entes de control y vigilancia) requieren acceso a información crítica del Ministerio, se deben suscribir acuerdos de confidencialidad o de no divulgación para la salvaguarda de la información.

El Ministerio de Ambiente y Desarrollo Sostenible debe garantizar la eliminación de los permisos de acceso tanto físicos como lógicos de los servidores públicos, contratistas o terceros que de alguna manera terminan la vinculación laboral.

Los servidores públicos son responsables por el buen uso de las credenciales de acceso asignadas.

Los servidores públicos no deben compartir sus credenciales o contraseñas con ninguna persona o hacerla pública por cualquier medio.

Las acciones que se realicen con un usuario en los sistemas de información serán total responsabilidad de éste.

Después de (3) tres intentos fallidos al ingresar los datos de acceso, la cuenta debe quedar bloqueada, y sólo podrá ser desbloqueada por el personal asignado por el Coordinador del Grupo de Sistemas.

Criptografía

Todo servidor público del Ministerio que deba transportar o enviar información clasificada como confidencial deberá utilizar software o programas de cifrado de archivos para mitigar riesgos de fuga o pérdida de la información.

La asignación de firmas digitales se realiza de acuerdo con las necesidades institucionales y será expedida en un tiempo mínimo de acuerdo con la disponibilidad de asignación del proveedor. El cifrado de la misma estará directamente ligado a las necesidades de procesamiento, software y necesidad de autenticidad requerida.

Los sitios y micro sitios del Ministerio de Ambiente y Desarrollo Sostenible que recojan información de ciudadanos o que por su naturaleza requieran comunicar la autenticidad del sitio, deberán contar con certificados SSL.

El uso de Tokens y controles criptográficos bancarios, serán gestionados de acuerdo con las políticas y directrices emitidas por el Ministerio de Hacienda Nacional y de acuerdo con los requisitos de cada banco y deben ser coordinados en los líderes de proceso quienes requieran su uso y el Grupo de Sistemas para garantizar la buena operación de los mismos.

7.2.5. Seguridad física y del entorno

Áreas Seguras

Se establecen como áreas seguras:

- Centro de cómputo y centro de cableado
- Archivo de Gestión Talento Humano
- Archivo de Gestión grupo de contratación
- Archivo de Gestión Grupo de control interno disciplinario
- Archivo Central
- Cuartos eléctricos
- Cuarto de Monitoreo
- Piso 4 – Despacho
- Las que el grupo Administrativo determine de acuerdo con los estudios de seguridad.

Identificar y salvaguardar las áreas seguras para la gestión, almacenamiento y procesamiento de información en el Ministerio de Ambiente y Desarrollo Sostenible. Las áreas deben contar con

protecciones físicas y ambientales acordes con el valor y la necesidad de aseguramiento de los activos que se protegen, incluyendo la definición de perímetros de seguridad, controles de acceso físicos, seguridad para protección de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales adecuadas de operación y sistemas de contención, detección y extinción de incendios.

El ingreso de terceros a los Centros de Cómputo y Centros de Cableado debe estar debidamente registrado mediante una bitácora custodiada por el personal de vigilancia contratado en la entidad.

Los privilegios de acceso físico a los Centros de Cómputo deben ser descontinuados o modificados oportunamente a la terminación, transferencia o cambio en las labores del personal previamente autorizado.

El Centro de Cómputo debe contar con mecanismos de control de acceso tales como puertas de seguridad, sistema de alarmas o controles biométricos, estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.

Los accesos a áreas seguras deberán tener un control de acceso físico, y no se debe permitir ingresar equipos fotográficos, de filmación, grabación de audio u otras formas de registro salvo con autorización especial del responsable del área segura.

Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizadas por quienes se encuentren debidamente autorizados y, salvo situaciones de emergencia, estos no deben ser transferidos a otros servidores públicos de la entidad.

Los servidores públicos o terceros que presten sus servicios al Ministerio no deben intentar ingresar a áreas a las cuales no tengan la debida autorización.

Todos los visitantes que ingresan a la entidad deben ser recibidos o autorizados para el ingreso y estar acompañados por la persona a quien visitan durante su permanencia en las instalaciones de la misma. El personal visitante, debe cumplir con los protocolos de seguridad definidos e implementados por la entidad.

Los trabajos de mantenimiento de redes eléctricas, cableado de datos y voz, deben ser realizados por personal especialista, el cual debe estar debidamente autorizado e identificado.

El Ministerio de Ambiente y Desarrollo Sostenible se reserva el derecho de monitorear el espacio físico mediante un circuito cerrado de televisión (CCTV) con el fin de brindar mayor seguridad en el recinto ministerial.

Los contratistas y servidores públicos deberán ingresar usando el sistema biométrico dispuesto para tal fin de acuerdo con los procesos establecidos por los encargados de Seguridad Física y del entorno.

Para el tratamiento y uso del Sistema de Acceso Biométrico se cita Circular número 8300-3-23415 del 15 de julio de 2015 mediante la cual se expide por Secretaria General la política de Control de Acceso Biométrico.

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MINAMBIENTE

CIRCULAR 15 JUL 2015

8300-3-23415

Bogotá, D. C. 14 de julio de 2015

PARA: SERVIDORES PÚBLICOS Y CONTRATISTAS DEL MINISTERIO

DE: SECRETARIA GENERAL

ASUNTO: Sistema de control de acceso biométrico.

Con Gran Éxito el Ministerio de Ambiente y Desarrollo Sostenible reporta las jornadas de toma de huella e implementación del sistema de control de acceso biométrico en la Entidad, lo cual demuestra la cultura de compromiso, la conciencia de seguridad y el cumplimiento de las estrategias institucionales de vanguardia operativa, cero papel y gestión ambiental, pues en adelante no será necesario el diligenciamiento de las planillas de control de horario.

Más de 700 personas de nuestra comunidad han apoyado y participado activamente en la iniciativa de la Administración de avanzar en la innovación y modernización del MADS, así como en el cumplimiento de su función legal de garantizar la seguridad de quienes laboran o prestan sus servicios en la sede, y el control del horario definido en la Resolución No. 1337 de 2012, para la consecuente oportuna prestación del servicio o función administrativa asignada constitucional y legalmente al Ministerio de Ambiente y Desarrollo Sostenible.

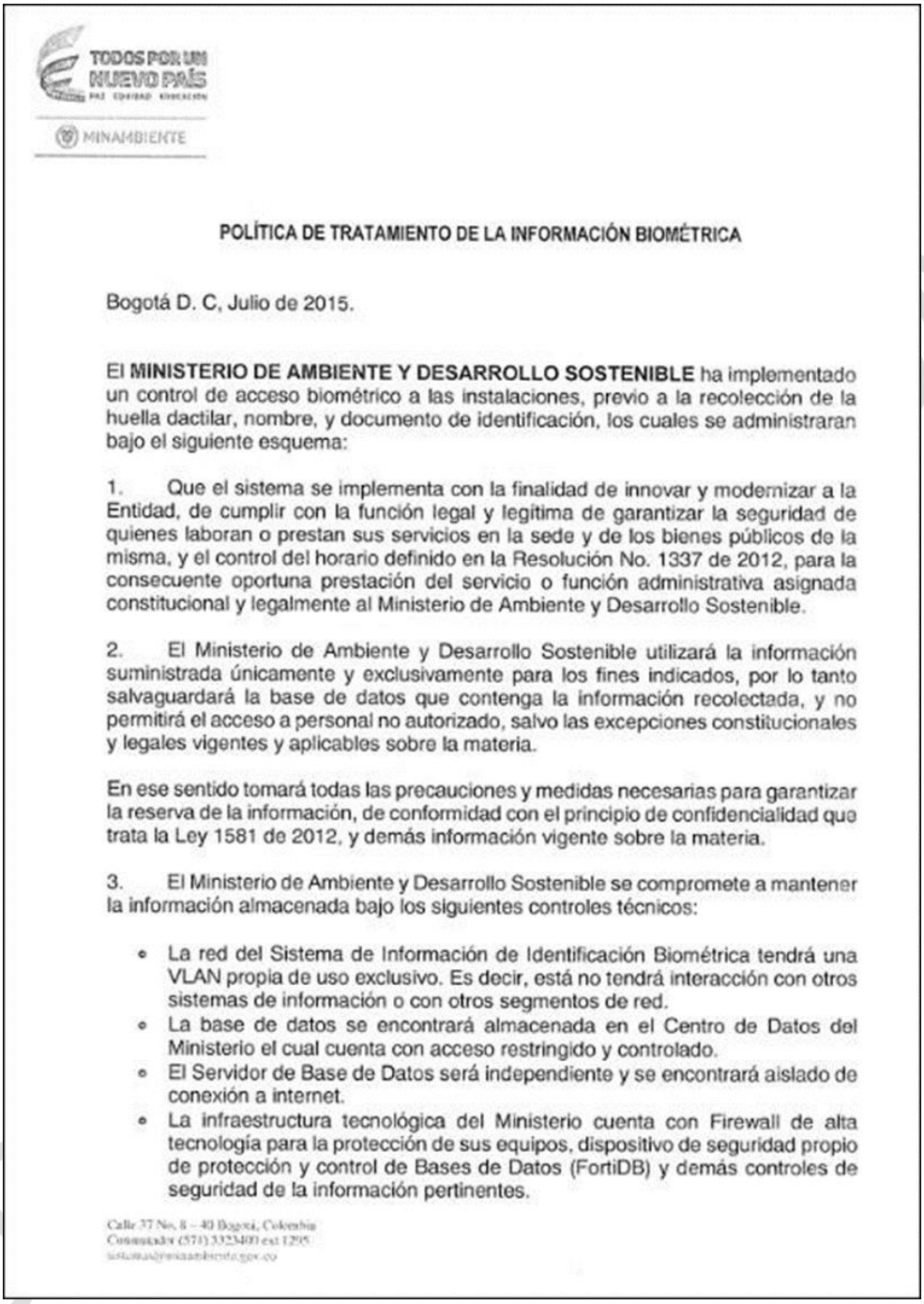
Los invitamos a seguir ingresando acorde con su calidad de funcionario o contratista, según corresponda, ya que la empresa de vigilancia y seguridad tiene instrucciones de no permitir el ingreso como visitantes a quienes en realidad no lo sean, además de aquellas impartidas en el correo electrónico enviado por este Despacho el pasado 8 de julio de 2015, en el sentido de que quienes no se encuentren registrados en el sistema de control de acceso, una vez el mismo entre en funcionamiento, no podrá ingresar a las instalaciones del MADS sin perjuicio de las consecuencias sancionatorias a que haya lugar.

Correlativamente el MADS protegerá la información de su titular, mediante los mecanismos señalados en la política de manejo de la información anexa a la presente circular.

Cordialmente,

ELIZABETH GÓMEZ SÁNCHEZ

Elaboró: Ximena Paternina De La Hoz: Contratista de la Secretaría General



TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MINAMBIENTE

POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN BIOMÉTRICA

Bogotá D. C, Julio de 2015.

El **MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE** ha implementado un control de acceso biométrico a las instalaciones, previo a la recolección de la huella dactilar, nombre, y documento de identificación, los cuales se administraran bajo el siguiente esquema:

1. Que el sistema se implementa con la finalidad de innovar y modernizar a la Entidad, de cumplir con la función legal y legítima de garantizar la seguridad de quienes laboran o prestan sus servicios en la sede y de los bienes públicos de la misma, y el control del horario definido en la Resolución No. 1337 de 2012, para la consecuente oportuna prestación del servicio o función administrativa asignada constitucional y legalmente al Ministerio de Ambiente y Desarrollo Sostenible.

2. El Ministerio de Ambiente y Desarrollo Sostenible utilizará la información suministrada únicamente y exclusivamente para los fines indicados, por lo tanto salvaguardará la base de datos que contenga la información recolectada, y no permitirá el acceso a personal no autorizado, salvo las excepciones constitucionales y legales vigentes y aplicables sobre la materia.

En ese sentido tomará todas las precauciones y medidas necesarias para garantizar la reserva de la información, de conformidad con el principio de confidencialidad que trata la Ley 1581 de 2012, y demás información vigente sobre la materia.

3. El Ministerio de Ambiente y Desarrollo Sostenible se compromete a mantener la información almacenada bajo los siguientes controles técnicos:

- La red del Sistema de Información de Identificación Biométrica tendrá una VLAN propia de uso exclusivo. Es decir, está no tendrá interacción con otros sistemas de información o con otros segmentos de red.
- La base de datos se encontrará almacenada en el Centro de Datos del Ministerio el cual cuenta con acceso restringido y controlado.
- El Servidor de Base de Datos será independiente y se encontrará aislado de conexión a internet.
- La infraestructura tecnológica del Ministerio cuenta con Firewall de alta tecnología para la protección de sus equipos, dispositivo de seguridad propio de protección y control de Bases de Datos (FortiDB) y demás controles de seguridad de la información pertinentes.

Calle 37 No. 8 – 40 Bogotá, Colombia
Conmutador (571) 3323400 ext 1295

Equipos

Se establecen controles para la prevención de pérdida, daño, robo o compromiso de activos tecnológicos, y la interrupción de las operaciones del Ministerio de Ambiente y Desarrollo Sostenible.

Los equipos que hacen parte de la infraestructura tecnológica de la organización tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento o comunicación móvil que contengan o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

La seguridad de los equipos de cómputo fuera de las instalaciones será responsabilidad de cada servidor público o contratista al que se le ha asignado, para sacar un equipo de las instalaciones se debe contar con el diligenciamiento de los respectivos formatos y autorizaciones necesarias de acuerdo con los procedimientos establecidos para tal fin.

El Ministerio recomienda a los usuarios acatar las siguientes recomendaciones, a fin de prolongar el tiempo de uso de los equipos:

- Ubicar el equipo en un área donde la conexión al suministro eléctrico sea regulada y tanto el cableado como la ubicación del mismo no represente riesgo de accidente al personal o afectación del equipo.
- No trasladar el computador sin la autorización y acompañamiento del soporte técnico dispuesto o mesa de ayuda.
- Ubicar el computador sobre escritorios y muebles estables, especialmente diseñados para ello.
- Ubicar el monitor de tal forma que, en lo posible, la luz solar no incida directamente sobre el equipo por tiempos prolongados.
- Asesorarse debidamente para garantizar una correcta conexión a la red eléctrica. La energía de corriente eléctrica regulada (110 voltios y con polo a tierra) se identifica por las tomas de color naranja.
- No conectar otros dispositivos (Radios, máquinas de escribir, calculadoras, celulares, etc.) en las tomas de corriente regulada de la organización.
- Apagar los equipos de cómputo al momento de terminar las labores diarias, incluidos los monitores, las impresoras y escáneres.
- No colocar ganchos, clips, bebidas y comida encima o cerca del computador, que puedan caer accidentalmente dentro del equipo y dañar sus partes.
- No fumar cerca a los equipos de cómputo.
- Utilizar los tamaños adecuados de papel según los requerimientos de las impresoras, no forzar las bandejas de papel o los rodillos después de un atasco. El Ministerio dispondrá del personal necesario para el mantenimiento del mismo.
- No romper los sellos de garantía para acceder y reparar los equipos por cuenta propia. Siempre solicitar el servicio a la mesa de ayuda mediante la herramienta de gestión de tickets o los canales dispuestos en la intranet para tal fin.
- No permitir el uso de los equipos a personas ajenas al proceso, salvo con autorización del superior inmediato o para actividades de soporte, mantenimiento y revisión realizadas por el Grupo de Sistemas.
- Se debe informar al Grupo de Sistemas sobre cualquier daño que sufran los activos tecnológicos que tenga a cargo.

- Apagar los activos tecnológicos asignados en las salas de reuniones al momento de finalizar su uso.
- Los servidores públicos y contratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de la organización no pueden fumar, beber o consumir ningún tipo de alimento en áreas donde se encuentren ubicados dichos equipos.

7.2.6. Seguridad de las operaciones

El Ministerio implementa controles para asegurar que las operaciones se ejecuten de manera correcta y segura en las instalaciones de procesamiento de información.

Los ambientes de desarrollo, prueba y producción de los sistemas de información del Ministerio se encuentran separados para garantizar la confidencialidad, integridad y disponibilidad de la información.

Las actividades realizadas para la gestión de tecnología tanto en el proceso de Gestión Estratégica de tecnologías de la información GET, como en el proceso de Gestión de Servicios de información y Soporte Tecnológico, deben estar debidamente documentados y actualizados.

Los procedimientos y responsabilidades de operación y administración de la plataforma tecnológica y de seguridad deben estar documentados, garantizando un adecuado control de cambios.

Todo cambio que se realice sobre la infraestructura tecnológica del Ministerio para el procesamiento de la información y comunicación debe ser controlado, gestionado y autorizado adecuadamente.

El Ministerio mantendrá un proceso continuo de medición de las variables críticas (CPU, memoria y espacio en disco) mediante monitoreo, análisis y evaluación de rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información.

Con el fin de dar respuestas oportunas y gestionar los controles implementados se realizará un monitoreo amplio y suficiente del tráfico de red, conexiones, servicios, recursos, entre otros afines a la gestión de tecnologías de la información y comunicaciones, plataformas, etc.

Protección contra códigos maliciosos

El Ministerio establece que los activos tecnológicos están protegidos mediante herramientas y software de seguridad como antivirus, antispam y otras aplicaciones y dispositivos que brindan protección contra código malicioso.

A efectos de proteger la integridad, disponibilidad y confidencialidad de los activos de información es imprescindible tener instalado, actualizado y en ejecución el programa de antivirus aprobado por la entidad, realizar mantenimiento de los equipos, administración de la red y bloqueo de puertos en la red de telecomunicaciones.

Copias de Respaldo

Se debe cumplir con el procedimiento de copias de respaldo establecido por la entidad, y realizar revisiones periódicas de la eficacia del control implementado.

Se establece un plan de restauración de copias de seguridad que serán probados a intervalos regulares (al menos una vez al año) con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado. La verificación de las copias de respaldo se realiza de acuerdo con las facilidades de la herramienta de backups Symatec del Ministerio.

La retención de Backups y tiempos de restauración a usuarios se gestiona de acuerdo con la capacidad gestionada por el Grupo de Sistemas.

Las copias de respaldo se realizan con frecuencia diaria para información que los procesos consideren relevante, para lo cual el Grupo de Sistemas dispondrá de una carpeta para dicha área en el servidor de archivos con permisos de acuerdo con la solicitud del líder de proceso. Para Backups adicionales o a equipos las áreas deben realizar una solicitud al Grupo de Sistemas.

Registro de actividades y supervisión

Los sistemas de información implementados en el Ministerio deben tener desarrollado módulos que permitan el almacenamiento y consulta de las actividades realizadas por los diferentes usuarios creados.

Los relojes de los sistemas de procesamiento de información y de los equipos de circuito cerrado de televisión deben estar sincronizados con la hora legal colombiana.

El canal de internet, uso de equipos, sistemas de respaldo de información y herramientas deben ser usadas únicamente para actividades relacionadas con el cumplimiento de las metas institucionales, por lo cual tanto los activos como la información contenida se presume de propiedad del Ministerio. Se prohíbe el uso de dichos recursos para fines personales o actividades al margen de la ley. La red del Ministerio, su tráfico, capacidad y uso será monitoreada.

Control de software operacional

Los usuarios finales no deben configurar, instalar y eliminar software de los equipos de cómputo del Ministerio de Ambiente y Desarrollo Sostenible, la interfaz del sistema operativo debe estar configurada de tal forma que tenga solo privilegios de invitado. Todas estas labores deben ser estrictamente realizadas por el proceso de Gestión de Servicios de Información y Soporte Tecnológico.

Consideraciones sobre auditorías a sistemas de información

Para las auditorías de sistemas que requieran hacer pruebas específicas que impliquen privilegios adicionales a los establecidos en las cuentas de usuario empleadas en tal área, se debe asegurar, que tales pruebas no van a afectar la seguridad de la información ni el desempeño de los servicios brindados.

Teletrabajo

En los casos que el acceso y procesamiento de la información del Ministerio de Ambiente y Desarrollo Sostenible, sea mediante la modalidad de teletrabajo, los responsables de estas actividades deberán dar cumplimiento a las condiciones y restricciones definidas entorno a la seguridad de la información, tales como:

- Seguridad física y de comunicaciones.
- Amenazas de accesos no autorizados a información o recursos.
- Acuerdos de licenciamiento para establecer responsabilidades.
- Establecer políticas acerca de derechos de propiedad intelectual desarrollada en equipos de propiedad privada.

Además, se deberán definir en los lineamientos del teletrabajo, los cuales incluirán:

- El suministro de equipo adecuado y de dispositivos de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control de la organización
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el teletrabajador está autorizado a acceder
- El suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto
- La seguridad física
- Las reglas y la orientación sobre el acceso de la familia y los visitantes a los equipos y a la información;
- El suministro de soporte y mantenimiento del hardware y el software
- El suministro de seguros
- Los procedimientos para copias de respaldo y continuidad del negocio
- Auditoría y seguimiento de la seguridad
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen

El ministerio de Ambiente y Desarrollo Sostenible asignará los permisos de acceso por medio de una Red privada Virtual (VPN), la solicitud debe ser gestionada por el aplicativo de ARANDA con previa autorización del jefe de área o líder de proceso al Grupo de Sistemas de la Entidad y previo visto bueno del Grupo de Talento Humano, deberán realizar la solicitud de permisos indicando lo que se requiere para la labor y el tiempo de vigencia del mismo.

7.2.7. Seguridad de las Comunicaciones

El Proceso Gestión de Servicios de Información y Soporte Tecnológico debe ser el encargado de bloquear el acceso a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso corporativo mediante el uso de servidor proxy, firewall o el software o control que mejor se ajuste a la necesidad.

El acceso a internet debe hacerse desde una estación debidamente registrada o autorizada.

El proceso de Gestión de Servicios de Información y Soporte Tecnológico deberá implementar y mantener la separación de las redes virtuales para garantizar la confidencialidad de la información en las redes de telecomunicaciones del Ministerio.

El acceso a la red por parte de terceros deberá ser gestionado a través de un ticket en la mesa de ayuda interpuesto por el líder de proceso.

Los contratos o acuerdos contractuales que realice el Ministerio deben incluir cláusulas que especifiquen las responsabilidades sobre el adecuado tratamiento de Información, estableciendo sanciones en caso de incumplimiento, y advirtiendo sobre la responsabilidad que en materia legal implica su desconocimiento. El alcance de los mismos puede variar dependiendo de las necesidades.

Los servidores públicos o contratistas directos del Ministerio son responsables de proteger la confidencialidad e integridad de la información y deben tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

7.2.8. Adquisición, Desarrollo Y Mantenimiento de Sistemas de Información

Desarrollo de software

Para apoyar los procesos operativos y estratégicos el Ministerio de Ambiente y Desarrollo Sostenible usará y facilitará las Tecnologías de la Información y las Comunicaciones para el mejoramiento o implementación de nuevos procesos para en consecuencia cumplir con los objetivos y cubrir las necesidades de la entidad. Los sistemas de información a usar pueden ser adquiridos a través de terceras partes bien sea en desarrollos a la medida o mediante herramientas comerciales o no comerciales que satisfagan la necesidad que se pretende subsanar. Para tal fin también se pueden implementar y mantener sistemas de información desarrollados por personal del Ministerio.

El Grupo de Sistemas y la Oficina Asesora de TIC deben elegir, elaborar, mantener y difundir el "Método de Desarrollo de Sistemas de Información" que considere apropiado o los requerimientos que apliquen de acuerdo con las funciones operativas y capacidades técnicas y de plataforma que existan al interior de MINAMBIENTE. Cuándo la necesidad de un sistema de información sea manifiesta se debe garantizar que este incluya lineamientos, procesos, buenas prácticas, plantillas, soporte y demás obligaciones que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad, así mismo se deben identificar y gestionar los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.

En la medida de lo posible y según la legislación colombiana lo permita, los sistemas de información adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

- El Ministerio de Ambiente y Desarrollo Sostenible debe asegurar que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya

controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

- El Ministerio, debe establecer controles para cifrar la información que sea considerada sensible y evitar la posibilidad de repudio de una acción por parte de un usuario del sistema. Se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.
- La información tratada por las aplicaciones aceptadas por el Ministerio debe preservar su confiabilidad desde su ingreso, transformación y entrega a las aplicaciones de la Entidad.
- La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección, por tanto, para procesos de desarrollo y pruebas, se debe evitar el uso de datos de producción y en caso de ser necesario su utilización, garantizar la eliminación segura al momento de finalización de las pruebas.
- Si los nuevos desarrollos son adquiridos a través de terceros, se deberá seguir un proceso formal de adquisición. Los contratos con los proveedores tendrán incluidos los requisitos de seguridad de la información.
- La organización debe tener un ambiente de desarrollo y de pruebas seguro o, en su defecto, exigir al proveedor mediante los contratos, que éste cuente con los controles de seguridad de la información sobre los ambientes y la posibilidad de ser auditados por parte del personal del Ministerio.
- Todos los sistemas de información del Ministerio deben pasar por un ciclo de pruebas de aceptación tanto funcionales como de seguridad antes de ser puestos en producción.

Relaciones con los Proveedores

Los proveedores relacionados con el ministerio o quienes prestan servicios al mismo, deben cumplir con las cláusulas de confidencialidad pactadas en los contratos; cumplir con los acuerdos de niveles de servicio estipulados; dar buen uso a la información de propiedad del ministerio, respetando siempre la propiedad intelectual de la misma y que sea usada para el fin al cual se destinó dicha información.

- El Ministerio identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros. Los controles que se establezcan a partir del análisis de riesgos, deben ser comunicados y aceptados por los terceros mediante la firma de acuerdos contractuales.
- La entidad debe establecer acuerdos de confidencialidad, no divulgación con los proveedores o terceros que presten sus servicios.
- Se debe hacer seguimiento a los acuerdos de niveles de servicio que se establezcan con los proveedores o terceros que presten sus servicios a la entidad.
- Cualquier actividad realizada por un proveedor en los sistemas de información del Ministerio, debe ser monitoreada por el Grupo de Sistemas, La oficina TIC o o el proceso directamente relacionado a través de la supervisión del contrato tanto con el proveedor como con el responsable del sistema de información.
- Los terceros que efectúen el Tratamiento de Información propia del Ministerio o sobre la cual la entidad sea Responsable, deben cumplir con la Política de Seguridad de la Información.
- Los contratistas directos tendrán cláusulas de confidencialidad, cumplimiento de políticas del SIG y derechos de propiedad intelectual, sin excepción.

- Para proveedores de TI se aplicarán acuerdos de confidencialidad anexos, amplios y suficientes para el cumplimiento de sus funciones.

7.2.9. Gestión de los Incidentes

- Se define y establece como responsable en el Ministerio para la atención y respuesta a eventos e incidentes de seguridad de la información al personal encargado de seguridad de la información.
- Todos los usuarios de la información del Ministerio de Ambiente y Desarrollo Sostenible deben reportar los eventos o incidentes de seguridad que se presenten, según el procedimiento de gestión de incidentes vigente en la entidad.
- El Ministerio de Ambiente y Desarrollo Sostenible debe asegurar que se establecen y ejecutan procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.
- En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicar a un ente competente para que realice el debido proceso.

7.2.10. Gestión de continuidad del negocio

- Debe evaluarse el impacto de las interrupciones que afectan la operación de los procesos críticos de la institución y definir e implementar planes de continuidad y de recuperación ante desastres para propender por la continuidad de la misma. Los planes deben considerar medidas tanto técnicas como administrativas para que se puedan recuperar oportunamente las funciones de los procesos y la tecnología que las soporta.
- Los planes de continuidad y de recuperación deben probarse y revisarse periódicamente y mantenerlos actualizados para su mejora continua y garantizar que sean efectivos.
- Se debe seguir una estrategia de recuperación alineada con los objetivos de negocio, formalmente documentada y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos del negocio, ante el evento de una contingencia.
- Se debe tener igual nivel de seguridad en los ambientes de producción y en los de contingencia.
- Para los procesos críticos del negocio, el Ministerio de Ambiente y Desarrollo Sostenible debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad del negocio aún en caso de desastre en las instalaciones de los lugares de Operación.
- En caso de no mantener acuerdos contractuales o legales vigentes que garanticen la continuidad tecnológica del Ministerio, ante una emergencia manifiesta, se deben asegurar los recursos necesarios para la recuperación.

7.2.11. Cumplimiento

El Ministerio de Ambiente y Desarrollo Sostenible, gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo entre otros los derechos de propiedad intelectual,

protección de datos personales, los tiempos de retención de registros, la privacidad, los delitos informáticos, el uso inadecuado de recursos de procesamiento, el uso de criptografía y la recolección de evidencia.

Protección de Datos Personales o la información sensible

El Ministerio de Ambiente y Desarrollo Sostenible utilizará la información suministrada única y exclusivamente para los fines indicados, por lo tanto, salvaguardará las bases de datos que contenga la información recolectada, y no permitirá el acceso a personal no autorizado, salvo las excepciones constitucionales y legales vigentes y aplicables sobre la materia.

En ese sentido tomará todas las precauciones y medidas necesarias para garantizar la reserva de la información, de conformidad con el principio de confidencialidad que trata la Ley 1581 de 2012, y demás información vigente sobre la materia. De igual manera el titular asiste los derechos que le otorga la normatividad aplicable y vigente respecto a la protección de datos y el derecho a la información.

Lo no dispuesto, se aplicará de conformidad con la normatividad vigente y aplicable sobre la materia.

Todos los productos de Software que se adquieran e instalen en los equipos de cómputo de la entidad deben contar con su respectiva licencia de uso.

Al interior del Ministerio de Ambiente y Desarrollo Sostenible se deben realizar auditorías, para verificar la eficacia de los controles y asegurar la administración de los riesgos de seguridad de la información.

La Política junto con el Sistema de Gestión de Seguridad de la Información del Ministerio de Ambiente y Desarrollo Sostenible, debe ser revisada anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.

La información de auditoría generada por el uso de los controles de seguridad de los Recursos de Tecnología debe ser evaluada por el responsable para:

- Reportar incidentes de seguridad.
- Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.
- Tomar acciones preventivas si así fuere necesario.

Los contratos de contratistas y proveedores deben contar con cláusulas referentes a la propiedad intelectual procurando que la información sea de propiedad del Ministerio de Ambiente y desarrollo sostenible, salvo contadas excepciones en el caso de acuerdos interadministrativos.

Los contratos vigentes y los futuros deben incluir dentro de sus condiciones el Derecho que tiene el Ministerio, a realizar auditorías periódicas y esporádicas a las condiciones de Seguridad de la Información que conserven sus proveedores con el fin de garantizar la protección de la información de forma integral.

Privacidad

El Ministerio de Ambiente y Desarrollo Sostenible en cumplimiento con sus actividades y objetivos institucionales y en cumplimiento con la legislación vigente es responsable de mantener la privacidad y dar un tratamiento adecuado a los datos personales y en concordancia con la ley aplicable. Así el Ministerio de Ambiente y Desarrollo Sostenible implementa la presente política en procura de la debida protección de los derechos de las diferentes partes relacionadas, en materia de privacidad y uso de los datos suministrados en los siguientes términos:

- Para los servicios web provistos por el Ministerio de Ambiente y Desarrollo Sostenible y que recojan datos, se informará explícitamente en los portales, bajo los términos de uso, que los titulares de los datos personales aceptan el uso, tratamiento o almacenamiento de los datos personales y que autorizan al Ministerio de Ambiente y Desarrollo Sostenible el tratamiento para los fines pertinentes para lo cual fueron entregados.
- La información recolectada por el Ministerio o suministrada al mismo, permanecerá de acuerdo con el término máximo definido para el uso o de acuerdo con la retención de información establecida por el Ministerio.
- En cuanto a la información suministrada al Ministerio de Ambiente y Desarrollo Sostenible a través de los diferentes portales y por entidades adscritas y vinculadas se presume su veracidad, vigencia, suficiencia, autenticidad y legitimidad de acuerdo con el principio constitucional de buena fe.
- El Ministerio cuenta e implementa controles de seguridad y políticas para mantener la privacidad de los datos, y salvaguardar y proteger la información relacionada.

Así mismo, y en cumplimiento a lo establecido en la normativa vigente se deben diligenciar los formatos F-E-GET-09 Caracterización de Bases de Datos Personales y F-E-GET-10 Reporte de Bases de Datos Personales como parte del tratamiento de las bases de datos personales, dicha información debe cargada de manera permanente, teniendo en cuenta los cambios en las mismas, en el aplicativo dispuesto para tal fin por la Superintendencia de Industria y Comercio.

8. GESTIÓN DE INCIDENTES

El Ministerio de Ambiente y Desarrollo Sostenible debe asegurar que se establecen y ejecutan procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

Todos los usuarios de la información del Ministerio de Ambiente y Desarrollo Sostenible deben reportar los incidentes de seguridad que se presenten, según el procedimiento de gestión de incidentes vigente en la entidad.

En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicar a un ente competente en el caso que se requiera y seguir el procedimiento de gestión de incidentes.

Todos los usuarios del ministerio de Ambiente y Desarrollo sostenible que detecten la ocurrencia de un evento de seguridad de la información o una debilidad (observada o sospechada) de seguridad de la información deben reportarlo en el menor tiempo posible a través de los siguientes medios:

- Aplicativo: ARANDA
- Extensión: *911

Se debe tener en cuenta que los siguientes componentes son fuentes generadoras de eventos de seguridad de la información:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Logs de servidores, aplicaciones y herramientas de seguridad

Todo evento reportado debe ser evaluado con el fin de decidir si corresponde a un incidente de seguridad de la información. Si el evento es catalogado como un incidente de seguridad de la información debe asignársele una categoría teniendo en cuenta las siguientes directrices:

Acceso no autorizado:

- **Físico:** Acceso no autorizado a las instalaciones del Ministerio de Ambiente.
- **Lógico:** Acceso no autorizado a sistemas de información, servidores, equipos de cómputo o dispositivos de red del Ministerio de Ambiente.
- **Código malicioso:** Programas utilizados por usuarios malintencionados para obtener acceso no autorizado y control de equipos de cómputo, servidores, sistemas de información; capturar contraseñas o información confidencial tecleada por el usuario; secuestrar la información de equipos de cómputo, servidores, dispositivos móviles; entre otros. Esta categoría incluye virus informáticos, gusanos informáticos, ransomware, keyloggers, entre otros.
- **Denegación de servicio:** Pérdida de disponibilidad de sistemas, redes u otros servicios.
- **Ingeniería social:** Método de ataque en el que se engaña a un usuario para obtener acceso a sistemas de información y a información del Ministerio de Ambiente, mediante técnicas tales como phishing, llamadas telefónicas fraudulentas, mensajes de texto, entre otras. Dentro de esta categoría se incluyen las subcategorías de divulgación sensible no autorizada de información oficial y no oficial y errores humanos que llevan a la fuga de información de la red.
- **Escaneo de Red o intentos de Obtención de información de la red:** Método que permite analizar y escanear todos los dispositivos de la red del Ministerio de Ambiente mediante la detección de los servicios comunes que están ofreciendo las máquinas y posibles vulnerabilidades de seguridad según los puertos abiertos esta amenaza permite el acceso a las carpetas compartidas servidores FTP, acceso remoto a los equipos y apagar dichos dispositivos.
- **Mal uso de los activos de Información:** Violaciones a las políticas de uso aceptable de los activos.
- **Datos personales:** Involucra la pérdida de confidencialidad, integridad o disponibilidad de activos relacionados con datos personales y su información asociada.

El personal de la mesa de ayuda además de clasificar el incidente debe priorizarlo, teniendo en cuenta las siguientes directrices de Priorización de incidentes.

Es frecuente que existan múltiples incidentes concurrentes, razón por la cual es necesario determinar un nivel de prioridad para la resolución de los mismos. El nivel de prioridad se basa esencialmente en dos parámetros:

- **Impacto:** Determina la importancia del incidente dependiendo de cómo este afecta los procesos de negocio o el número de usuarios afectados.
- **Urgencia:** Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente.

ESTABLECIMIENTO DEL NIVEL DE PRIORIDAD

Impacto	Urgencia Baja	Urgencia Alta	Urgencia Critico
LOW	LOW	MEDIUM	MEDIUM
HIGH	MEDIUM	HIGH	HIGH
CRITICAL	HIGH	HIGH	CRITICAL

Además, se debe tener en cuenta que el tiempo de respuesta de los incidentes de seguridad de información tiene un impacto del servicio MEDIO por tanto manejan los siguientes SLA

SLA		SLA VIP - DIRECTORES	
Tiempo Atención (mn)	Tiempo de Solución (mn)	Tiempo Atención (mn)	Tiempo de Solución (mn)
15	120	10	60

El personal de la mesa de ayuda además de clasificar el incidente debe priorizarlo, teniendo en cuenta las siguientes directrices de priorización de incidentes.
El personal de Mesa de Ayuda realizará Análisis y resolución del Incidente con ayuda de la base de conocimiento para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado.

Si la resolución del incidente se escapa de las posibilidades de la mesa de ayuda, ésta redirecciona el caso a un nivel superior para su investigación por el equipo, el líder del proceso correspondiente y el oficial de seguridad; En última instancia se escalará el incidente a terceros y el personal directivo o encargado de Dicho incidente realizará la gestión interna correspondiente. Tener en cuenta El esquema de escalamiento de incidentes y los siguientes tipos de estrategias para resolución de Incidentes:

- **Contención:** Busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura
- de TI. Algunos ejemplos de actividades de contención son: bloqueo de cuenta después de sucesivos intentos de acceso, desconexión de la red de un equipo infectado con malware.

- **Erradicación:** Busca eliminar cualquier rastro dejado por el incidente con acciones tales como: Reparación del sitio web después de un defacement, borrado seguro y restauración de un backup en un equipo infectado por malware, reinstalación del equipo y recuperación de datos cuando se detecta un rootkit.
- **Recuperación:** Restauración de los sistemas o servicios afectados el personal de la Mesa de Ayuda, a quien se le haya asignado el incidente debe restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento (hardening) del sistema que permita prevenir incidentes similares en el futuro.

Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las bases de datos correspondientes para que los implicados dispongan de información sobre el estado del mismo.
Si fuera necesario se puede emitir una solicitud de cambio, siguiendo del procedimiento correspondiente.

Antes de proceder a cerrar el caso, es necesario confirmar con el(los) usuario(s) la solución satisfactoria del mismo. Adicionalmente, se deben registrar los procedimientos aplicados para resolver el incidente.

Es necesario mantener un proceso de lecciones aprendidas después de un incidente grave, y semestralmente para analizar los incidentes menores. Se debe mantener un adecuado registro de lecciones aprendidas con el fin de conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Cuál sería la gestión de personal y qué debería hacerse la próxima vez que ocurra un incidente similar.
- Actualización de la matriz de riesgos
- Acciones correctivas para prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

8.1. Recolección de Evidencia

Para la resolución del incidente es necesaria la recolección de evidencia. Estas evidencias pueden provenir de diferentes fuentes, tales como:

- Información basada en la red: Logs de IDS o IPS, logs de monitoreo, logs de routers, logs de firewalls, información recolectada mediante Sniffers de red, información de servidores de autenticación.
- Información Basada en el Equipo:
- Live data collection: Volcado (dump) de la memoria RAM, fecha y hora del sistema, procesos activos, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red.
- Otra información: Testimonio de funcionario, contratista o tercero que reporta el evento.

En caso de que se requiera hacer denuncias penales, se debe tener en cuenta el Directorio Contacto con Autoridades y Grupos de Interés. Adicionalmente, es importante hacer una recolección y manejo

adecuado de la evidencia; para ello, la entidad puede contactar al ColCERT, contratar un experto en el tema, o en caso de que se decida que la Mesa de ayuda recolecte la evidencia se deberían tener en cuenta las directrices del procedimiento de Recolección de Evidencia. En caso de que se tipifique como un posible delito se debe contactar a la Policía Nacional y la recolección de evidencia será responsabilidad de la Unidad de Policía Judicial.

9. CONTROLES DEL MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

A fin de garantizar el mantenimiento del Sistema de Gestión de Seguridad de la Información en MINAMBIENTE se debe realizar el seguimiento semestral al cumplimiento de los requisitos de la norma ISO 27001 incluyendo los controles definidos, dicho seguimiento debe realizarse en los formatos F-E-GET-07 Seguimiento a Controles de Seguridad de la Información y F-E-GET-08 Seguimiento a Requisitos de Seguridad de la Información.

ROL	ACTIVIDADES	RESPONSABILIDADES	REQUISITOS DE COMPETENCIA				NOMBRE DEL TITULAR	COMPETENCIA	COMPETENCIA A FORTALECER	FECHA DE EJECUCIÓN
			FORMACION / ENTRENAMIENTO	EXPERIENCIA	EDUCACION	HABILIDADES				
Responsable(s) asignado para Seguridad de la Información/ Oficial de Seguridad de la información	• Apoyo al Jefe de Oficina de Tecnologías de la Información y Comunicación y Coordinador del Grupo de Sistemas liderando las acciones del grupo operativo e impulsando la implementación y cumplimiento de la presente Política. • Acompañamiento en la valoración de los activos de información con los procesos involucrados del SGSI. • Identificar, evaluar y apoyar la implementación de mejoras en seguridad de la información a los sistemas de información e infraestructura tecnológica. • Acompañamiento en la revisión y actualización de los riesgos en seguridad de la información en conjunto con los responsables de los mismos. • Liderar la planeación, implementación, pruebas y mejora del Plan de continuidad de la entidad. • Ejecutar pruebas de seguridad informática a la infraestructura tecnológica de la entidad.	Informar trimestralmente del estado de la seguridad de la información al grupo operativo de Seguridad de Información de MINAMBIENTE.	Conocimientos en ISO 27002 Auditor Interno o líder ISO 27001 Conocimientos en Gestión de Incidentes Conocimientos de Hacking Ethico	1 año	Técnico en seguridad de la información o administración tecnológica o auditoria de sistemas o auditor interno ISO 27001, o estudios en ingeniería de sistemas o afines	• Aplicar y promover metodologías actualizadas que conduzcan a la práctica de una cultura de la información; • Diseñar y administrar políticas de seguridad para los recursos informáticos del ministerio • Diseñar estrategias que puedan garantizar la seguridad de los activos de información	Designado	Cumple	• Conocimientos en ISO 27002 • Conocimientos en Gestión de Incidentes • Conocimientos en Riesgos • Conocimientos de Hacking Ethico	No aplica

ROL	ACTIVIDADES	RESPONSABILIDADES	REQUISITOS DE COMPETENCIA				NOMBRE DEL TITULAR	COMPETENCIA	COMPETENCIA A FORTALECER	FECHA DE EJECUCIÓN
			FORMACION / ENTRENAMIENTO	EXPERIENCIA	EDUCACION	HABILIDADES				
Jefe de la Oficina de Control Interno o delegado	• Notificar a todo el personal de sus obligaciones respecto a la verificación, desarrollo, planes y programas de auditoría en los tiempos establecidos tomando como insumo principal los diagnósticos y la matriz de riesgos.	Informar sobre el cumplimiento del plan de auditorías al sistema de gestión de seguridad de la información	No Aplica	No aplica	No aplica	No aplica	Designado		No aplica	No aplica
Coordinador Grupo de Sistemas	• Cumplir con los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de MINAMBIENTE.	Implementación de controles técnicos en seguridad informática.	Bases generales ISO 27001	No aplica	No aplica	No aplica	Designado	Cumple	• Conocimiento • s en ISO 27002 • Conocimiento s en Gestión de Incidentes • Conocimiento s en Riesgos • Conocimiento s de Hacking	No aplica
Jefe Oficina asesora Jurídica o delegado	• Asesorías en materia legal a MINAMBIENTE, en cuanto se refiere a la seguridad de la información.	No Aplica	Conocimientos de las leyes vigentes en Colombia referentes a seguridad de la información	No aplica	No aplica	No aplica	Delegado	No aplica	No aplica	No aplica
Coordinador Grupo Contratos o delegado	• Verificar el cumplimiento de las políticas de seguridad de la información en lo referente a la gestión de todos los contratos, acuerdos u otra documentación de MINAMBIENTE con sus empleados y con terceros.	Asegurar que en los contratos queden las cláusulas de confidencialidad de la información, derechos autor, Acuerdos de Nivel de servicio (donde aplique), Ley de trasparencia y protección de datos personales y aquellas referentes a seguridad de la información	No Aplica	No aplica	No aplica	No aplica	Designado	No aplica	No aplica	No aplica

ROL	ACTIVIDADES	RESPONSABILIDADES	REQUISITOS DE COMPETENCIA				NOMBRE DEL TITULAR	COMPETENCIA	COMPETENCIA A FORTALECER	FECHA DE EJECUCIÓN
			FORMACION / ENTRENAMIENTO	EXPERIENCIA	EDUCACION	HABILIDADES				
Coordinador Talento Humano o delegado	• Notificar a todo el personal en la Inducción o reinducción de sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.	Promover la formación y concientización en materia de seguridad de la información dentro de su ámbito de responsabilidad a través de la inducción y reinducción.	No Aplica	No aplica	No aplica	No aplica	Designado	No aplica	No aplica	No aplica
Jefe de la Oficina de Tecnología de la información y la comunicación	• Presupuestar y aprobar los recursos necesarios para implantar y soportar las políticas de seguridad. • Conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad y procedimientos del Sistema de Seguridad de la Información vigente de MINAMBIENTE.	Realizar informes trimestrales de los recursos financieros para mantener y mejorar el sistema de gestión de seguridad. Supervisión del cumplimiento según lo establecido en la política de seguridad de la Información de MINAMBIENTE por parte de su personal a cargo.	Conocimientos en Gestión de Seguridad de Información	No aplica	No aplica	No aplica	Jefe de OTIC	No aplica	No aplica	No aplica
Coordinador del Control Interno disciplinario o delegado	• Realizar las investigaciones y sanciones administrativas para los funcionarios que violen las políticas de seguridad de la información	Seguir el proceso disciplinario formal contemplado en las normas estatutarias y convencionales que rigen al personal de la Administración Pública Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad en el Ministerio	No Aplica	No aplica	No aplica	No aplica	Designado	No aplica	No aplica	No aplica

ROL	ACTIVIDADES	RESPONSABILIDADES	REQUISITOS DE COMPETENCIA				NOMBRE DEL TITULAR	COMPETENCIA	COMPETENCIA A FORTALECER	FECHA DE EJECUCIÓN
			FORMACION / ENTRENAMIENTO	EXPERIENCIA	EDUCACION	HABILIDADES				
Jefe de la oficina Asesora de Planeación o su delegado Coordinador Sistema Integrado de Gestation	• Asegurar la participación de la dirección en el SGSI • Participar en las actividades de divulgación del SGSI en cada dependencia	Garantizar la integración del subsistema de gestión de seguridad de la información al SIG	Integración de Gestión Ambiental al SIG Bases generales de ISO 27001	No aplica	Profesional especializado en Sistemas de Gestión o afines	No aplica	Coordinador grupo del SIG	No aplica	No aplica	No aplica