POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

OBJETIVO

Definir los lineamientos y directrices que se deben seguir por parte los colaboradores y terceros del Ministerio, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información.

ALCANCE

Aplica para todos los colaboradores y terceros del Ministerio.

DEFINICIONES

- **MSPI:** Es el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información – MINTIC.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Acceso y uso de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma, ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Carpetas Compartidas:** es básicamente igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.
- **File Server:** Es un servidor de archivos que almacena y distribuye diferentes tipos de archivos informáticos confidenciales o críticos del MEN.
- **Información confidencial o crítica:** Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en el MEN
- **MEN:** Ministerio de educación Nacional
- **Mesa de Ayuda de Tecnologia:** es el único Centro de Atención al Usuario en donde la OTSI presta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servicios TICs en el MEN.
- **Onedrive:** Sitio para almacenamiento virtual en la nube de la información pública de las áreas de la institución.
- **OTSI:** Oficina de Tecnología y Sistemas de Información**.**
- **Quota:** es un límite establecido por el administrador para la asignación de espacio en el disco duro de una manera razonable, para almacenamiento de la información de la institución.
- **SharePoint:** Sitio para almacenamiento de la información pública para uso interno de la institución.

1.1. OBJETIVO

Definir y socializar las políticas y directrices que se requieren para garantizar la protección de la información del Ministerio de Educación Nacional, velando por el cumplimiento de la integridad, disponibilidad y confidencialidad de esta.

1.2. ALCANCE

La presente política debe ser cumplida por todos los colaboradores (contratistas) y terceros de todos los procesos del Ministerio de Educación Nacional y, adicionalmente, por los ciudadanos, persona naturales o jurídicas, nacionales o extranjera que sin tener relación laboral o contractual con el MEN tengan acceso a sus instalaciones y/o servicios tecnológicos.

Propender que los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, confidencialidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso para asegurar su correcta funcionalidad, brindando un nivel de seguridad óptimo que permitan:

- Evitar la materialización de los riesgos identificados.
- Cumplimiento legal y normativo.
- Disminuir las amenazas a la seguridad de la información y los datos.
- Evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos.
- Cuidar y proteger los recursos tecnológicos del Ministerio de Educación Nacional.
- Concientizar a la comunidad sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.

1.3. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Dando cumplimiento a las actividades desarrolladas en la implementación del Modelo de Seguridad y Privacidad de la Información que se encuentra realizando el MEN, se elaboran una serie de políticas específicas que se describen a continuación:

1.3.1. *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN*

La política general del Sistema de Gestión de Seguridad de la Información se encuentra en el Manual del Sistema Integrado de Gestión.

1.3.2. *POLÍTICA DE ROLES Y RESPONSABILIDADES*

Disposiciones generales:

Hacer buen uso de la información que es generada resultado de las actividades laborales.

Se debe definir los roles, responsabilidades y competencias en seguridad de la información.

Almacenar la información resultado del ejercicio de las funciones en la carpeta local o servidor de archivos designado por la Oficina de Tecnología y Sistemas de Información – OTSI, de esta forma el Ministerio garantiza las copias de respaldo, de lo contrario no queda dentro de la presente política.

En ninguna circunstancia se podrá divulgar la información clasificada como CONFIDENCIAL o RESERVADA a personas no autorizadas o en espacios públicos o privados. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la Entidad.

Todos los activos de información del deben tener un propietario, custodio y deben estar debidamente identificados.

Los propietarios de los activos de información son los responsables de aplicar y velar por el cumplimiento de los controles que garanticen la disponibilidad, confidencialidad e integridad de la información de los activos.

Se deben definir e incluir los roles y privilegios de la plataforma tecnológica y sistemas de información, con el fin de crear el procedimiento de solicitud, modificación, eliminación y/o inactivación de usuarios privilegiados.

Se debe seguir el procedimiento de gestión de accesos definido por la Oficina de Tecnologías y Sistemas de Información.

Todas las solicitudes deben tener fecha de finalización y cuando sean roles que no se encuentren definidos se consideran como privilegios temporales.

La mesa de servicios designada para tal fin debe informar a través de los mecanismos de comunicación seleccionados, que el usuario fue creado y que fueron asignados los privilegios solicitados.

Se debe capacitar a todos los Colaboradores y terceros solicitantes de accesos a componentes tecnológicos y sistemas de información sobre el uso y la responsabilidad que tienen al ser autorizados.

Se debe definir una matriz de roles y responsabilidades en seguridad de la información, la cual debe ser actualizada periódicamente o cada vez que se requiera.

1.3.3. *POLÍTICA DE DISPOSITIVOS MÓVILES*

Se debe llevar un registro y control de todos los dispositivos móviles que posee la Entidad.

Se debe hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones laborales.

Se debe definir un procedimiento de formal de salida de dispositivos.

Los dispositivos móviles que son autorizados para salir de las instalaciones por el Ministerio deben ser protegidos mediante el uso e implementación de los controles apropiados para ello, como son: cifrado de información, políticas de restricción en la ejecución de aplicaciones, y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.

Todos los dispositivos móviles como celulares que almacenen información del MEN deben contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave.

Todos los dispositivos móviles propiedad del Ministerio pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

El Colaborador o Tercero responsable del dispositivo móvil debe hacer periódicamente copias de respaldo, en caso de los portátiles deben conectar el quipo mínimo una vez por semana a la red, con el fin de que se ejecute la copia de respaldo de la carpeta destinada para esta función.

Todos los Colaboradores y Terceros son responsables de garantizar el buen uso de los dispositivos móviles en redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

1.3.4. *SEGURIDAD DE LOS RECURSOS HUMANOS*

Objetivo: Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del personal que trabaja para el MEN, a través de mecanismos de validación y concientización del recurso humano que hará uso de esta.

Incorporación de la Seguridad en la matriz de Cargos de la entidad

Deben ser incorporadas los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.

Control y Política del Personal

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación de Colaboradores del Ministerio.

Acuerdo de Confidencialidad

Todos los Colaboradores y Terceros que ingresen a trabajar en MEN, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios o en el Acta de Posesión del funcionario. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. Este documento debe ser archivado de forma segura por el área de Talento Humano y Contractual, según sea el caso.

Dentro del mismo acuerdo el Colaborador o Tercero declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas

actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del Colaborador o Tercero.

Selección de personal

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo con la reglamentación.

Se deben aplicar los controles establecidos por el Ministerio para otorgar el acceso a la información CONFIDENCIAL o RESERVADA por parte del personal que resulte vinculado a la Entidad.

El área de Talento humano y Contratación son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación.

Términos y condiciones Laborales

Todos los Colaboradores y Terceros del Ministerio deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar.

Todos los Colaboradores y Terceros, durante el proceso de vinculación a MEN, deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

Entrenamiento, concientización y capacitación

Todos los Colaboradores y Terceros del MEN deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de la Entidad. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas y directrices de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

Formación y Capacitación en Materia de Seguridad de la Información

Todos los Colaboradores y Terceros cuando sea el caso, que trabajan para el MEN deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información. Dentro del contenido se deben contemplar los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre el uso adecuado de las instalaciones de procesamientos de información y los recursos tecnológicos informáticos que les provee la Entidad para el desempeño de sus funciones laborales y contractuales.

Procesos disciplinarios

Todos los incidentes de seguridad de la información presentados en MEN deben tener el tratamiento adecuado y establecido en el procedimiento de atención de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables.

Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

En lo pertinente a la violación de las políticas de seguridad de la información de la Entidad, a los Colaboradores y Terceros, se les aplicará lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

1.3.5. *POLÍTICA DE USO DE CORREO ELECTRÓNICO*

Objetivo: Definir las directrices generales del buen uso del correo electrónico en el MEN.

Usos aceptables del servicio

Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en el Ministerio y no se debe utilizar para otros fines.

Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de Ministerio.

Todos los Colaboradores y Terceros que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.

Todos los Colaboradores y Terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información del Ministerio.

El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con MEN. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad del Ministerio y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

Cuando un Proceso, Oficina, Grupo o Dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina de Comunicaciones del Ministerio o el medio formal autorizado para realizar esta actividad.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por MEN y deberán conservar en todos los casos el mensaje legal corporativo.

El único servicio de correo electrónico controlado en la entidad es el asignado directamente por la Oficina de Tecnologías de la Información y las Comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

El servicio de correo electrónico cuenta con respaldo de información (Back up) de diferentes procesos aplicados de manera periódica y segura.

Se realiza copia de respaldo de Información a los registros de auditoria que generan los buzones de correo.

Los demás servicios de correo electrónico son utilizados bajo responsabilidad directa y riesgo de los usuarios, siendo necesaria la aprobación y firma por parte del director, Jefe de Oficina, Subdirector, Coordinador de Grupo de Trabajo o Supervisor de contrato; de un documento de análisis de riesgos para la autorización de sistemas de correo electrónico diferentes al institucional.

Para acceder al correo electrónico desde canales externos a los del Ministerio, se debe garantizar que la información viaja cifrada.

Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Reservado o Confidencial), de acuerdo a la Clasificación y Etiquetado de la Información establecida en la entidad.

El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por la Oficina de Tecnologías de la Información y las Comunicaciones.

Todos los Colaboradores y Terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro del Ministerio, para que de esta forma la Oficina de Tecnología y Sistemas de Información realicen el ajuste de permisos requerido.

El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus a la Oficina de Tecnologías de la Información y las Comunicaciones, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y este seguro que este no es de tipo SPAM, así la Oficina de Tecnología y Sistemas de Información hacen el análisis para evaluar el origen y así tomar las medidas pertinentes.

Cuando un Colaborador se retire del Ministerio, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo corporativo, Talento Humano y Contratación

debe notificar a la Oficina de Tecnologías y Sistemas de Información la desactivación de la cuenta.

Los mensajes y la información contenida en los buzones de correo son de propiedad del Ministerio.

Cada usuario se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

Las cuentas institucionales (Ejemplo: Comunicaciones, atención al ciudadano, Soporte, control interno etc.) deben tener una persona responsable que haga depuración del buzón periódicamente.

Todo Colaborador es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Colaborador o Tercero desconfíe del remitente de un correo electrónico debe remitir la consulta a la mesa de servicios de tecnología.

Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), la Oficina de Tecnologías de la Información y Comunicaciones actuará según sea el caso.

La Oficina de Tecnología y Sistemas de Información se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no pueden ser eliminados, el mensaje será borrado.

Ningún Colaborador o Tercero debe suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.

El funcionario, Colaborar o Tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar a la Oficina de Tecnologías de la Información y las Comunicaciones, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo del Ministerio.

Las cuentas creadas en los dominios del Ministerio serán bloqueadas automáticamente después de estar inactivas en un tiempo de noventa (90) días, para el des bloqueo de la cuenta se debe hacer a través de una mesa de ayuda de tecnología.

Todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.

Todos los usuarios de correo electrónico, el tamaño máximo para recibir o enviar mensajes es de 25 MB (incluyendo la suma de todos los adjuntos).

Usos no aceptables del servicio

Envío de correos masivos que no hayan sido previamente autorizados a través del procedimiento formal de Solicitud de Cuentas de Usuario, establecido en MEN.

Envío, reenvío o intercambio del mensajes no deseados o considerados como SPAM, cadena del mensajes o publicidad.

Envío o intercambio del mensaje con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Envío o intercambio del mensaje que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

Envió del mensaje que contengan amenazas o mensajes violentos.

Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

Divulgación no autorizada de información propiedad del Ministerio.

Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

Adulterar o intentar adulterar mensajes de correo electrónico.

Enviar correos masivos, con excepción de con nivel de director o superior, quienes sean previamente autorizados por estos para ello, o de que en calidad de sus funciones amerite la excepción.

Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política.

1.3.6. *POLÍTICA DE USO DE INTERNET*

Objetivo: Definir la política de buen uso del internet, con el fin de asegurar una adecuada protección de la información del Ministerio.

Usos aceptables del servicio

Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en MEN y no debe utilizarse para ningún otro fin.

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información del Ministerio.

Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

El navegador autorizado para el uso de Internet en la red del Ministerio es el instalado por la Oficina de Tecnología y Sistemas de Información, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.

No se permite la conexión de módems externos o internos en la red del Ministerio, previa solicitud autorizada por la Oficina de Tecnologías de la Información y las Comunicaciones.

Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro del Ministerio.

Todos los usuarios son responsables del uso de sus credenciales de acceso a las cuales les fue otorgado el acceso a internet.

Para realizar intercambio de información de propiedad del Ministerio con otras entidades, se debe seguir un proceso formal de requisición de la información, el cual debe contar con la previa autorización del dueño de la información.

El Ministerio se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas

ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.

Los y Colaboradores y Tercero del Ministerio no deben asumir en nombre de la entidad, posiciones personales en encuestas de opinión, foros u otros medios similares.

Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información del Ministerio.

Usos no aceptables del servicio

Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.

Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

Todos los usuarios invitados que requieran acceso a internet dentro de las instalaciones del Ministerio deben realizarlo por medio de la red WIFI invitados y cumplir con los requerimientos que el portal solicita, una vez que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos del Ministerio y las emitidas por los entes de control.

No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

1.3.7. *POLÍTICA DE USO DE REDES SOCIALES*

Objetivo: Definir la política para el uso del servicio de Redes sociales por parte de los usuarios autorizados en MEN.

Usos aceptables del servicio

Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información del Ministerio.

El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con el Ministerio.

Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.

El Ministerio facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar por parte de los Colaboradores y Terceros, sin embargo es necesario hacer buen uso de forma correcta y moderada.

No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.

No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.

No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet del Ministerio, o aprovechar el acceso a Redes Sociales para fines ilegales.

Es claro que no se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

Todos los Colaboradores y Terceros del Ministerio, deben seguir los procedimientos y planes de comunicaciones interna y externa.

La Oficina de Tecnologías de la Información y las Comunicaciones, será el encardo de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales en MEN, previo acuerdo con el Proceso de Gestión con Grupos de Interés y Comunicaciones.

1.3.8. *POLÍTICA DE USO DE RECURSOS TECNOLÓGICOS*

Objetivo: Definir la política para el uso aceptable de los recursos tecnológicos del Ministerio

Usos aceptables del servicio

El Ministerio asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los Colaboradores y terceros de ser necesario.

El uso adecuado de estos recursos se establece bajo los siguientes criterios:

Cada equipo de cómputo está configurado con el Hardware y Software básico necesario para su funcionamiento:

- Sistema operativo: Windows, IOS o Linux
- Ofimática: Office 365 (Acces, Excel, OneNote, One Drive, Outlook, Power Point, Publisher, Word.)
- CA
- ISE
- Descomprimir Archivos: Winrar
- Antivirus
- Chat: Skype Empresarial o Lync
- Video Conferencias: Webex

La instalación de software se encuentra bajo la responsabilidad la Oficina de Tecnología y Sistemas de Información y por tanto son los únicos autorizados para realizar esta actividad y toda solicitud debe realizarse por medio de la Mesa de Ayuda de Tecnologia.

Si el Colaborador cuenta en su equipo de cómputo con aplicaciones diferentes a las antes mencionadas o con software no autorizado, se procederá a realizar la desinstalación sin previa autorización.

Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por la Oficina de Tecnologías de la Información y las Comunicaciones.

La Oficina de Tecnología y Sistemas de Información es el responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en MEN para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

Sólo el personal autorizado por la Oficina de Tecnología y Sistemas de Información podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la

infraestructura de procesamiento de información del Ministerio; las conexiones establecidas para este fin utilizan los esquemas de seguridad establecidos por la entidad.

Los Colaboradores y Terceros de la Entidad son responsables de hacer buen uso de los recursos tecnológicos del Ministerio y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros , Colaboradores y Terceros, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por MEN.

La información clasificada como personal almacenada en los equipos de cómputo, medios de almacenamiento o cuentas de correo institucionales, debe ser guardada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como “PERSONAL”.

Todo activo de propiedad del Ministerio, asignado a un Colaborador y Tercero del Ministerio, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.

Cualquier requerimiento que tenga un usuario respecto a instalación, desinstalación, o actualización de sus aplicaciones, deberá solicitarse por medio de la Mesa de Servicios Tecnológica, y estas entraran a ser evaluadas por la OTSI para su aprobación o denegación.

El software propiedad del MEN, es para uso exclusivo de usuarios de planta y contratistas con vínculo directo con el Ministerio. Proveedores y/o contratistas no pueden instalar o hacer uso de las licencias propiedad del MEN.

El Ministerio ofrece a sus usuarios planta y contratistas con vínculo directo, cinco (5) licencias de Office 365, las cuales pueden ser instaladas en sus equipos personales pero vinculadas a la cuenta del MEN. Estas licencias no pueden ser cedidas, vendidas o tener uso comercial, el MEN podrá tomar las acciones pertinentes si se evidencia el mal uso de este licenciamiento.

Si un equipo de cómputo requiere seguir algún procedimiento de formateo o reinstalación de aplicaciones, por problema de infección de virus, o por algún daño que haya sufrido, se debe realizar una solicitud a la Mesa de Servicios de Tecnología, la cual respaldará la información y documentos que se consideren de las funciones asignas a su cargo.

Cada usuario debe ser responsable de sacar el respaldo respectivo de la información que maneja en su equipo de cómputo. La OTSI sólo es responsable de respaldar y salvaguardar la información que se encuentra en los discos compartidos a través de los servidores del centro de cómputo. En caso de que algún usuario requiera ayuda con sus respaldos, deberá solicitarlo por medio de la Mesa de Servicios de Tecnología, para que este le implemente el procedimiento más adecuado y su información pueda estar asegurada.

El usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.

El usuario no deberá abrir los equipos de cómputo, como tampoco sacar o cambiar componentes de estos.

En caso de que un equipo de cómputo presente un mal funcionamiento, el usuario responsable por el equipo de cómputo deberá reportarlo de inmediato a través de la Mesa de Servicios de Tecnología. La Mesa de Servicios de Tecnología hará una evaluación del equipo para determinar el tipo de daño y la reparación que se requiere.

De la evaluación que se realice del equipo de cómputo dañado, se determinará lo siguiente:

- Si el equipo de cómputo está en garantía y el daño puede ser procesado por garantía. En este caso lo enviará al proveedor donde fue adquirido el equipo para que este haga la reposición de la parte defectuosa y devuelva el equipo lo más pronto posible.
- Si el equipo de cómputo está fuera de garantía, se determinará si el equipo puede repararse internamente en el diario o si requiere de una reparación en un servicio técnico autorizado.
- Si el daño es por falla eléctrica, se determinará la parte que debe ser reemplazada, y si la reparación puede ser realizada en el diario o debe enviarse a una empresa de servicio técnico. Adicionalmente se reportará el particular a la dependencia Administrativa para que tomen las medidas pertinentes respecto al punto eléctrico que causó el problema.
- La Mesa de Servicios de Tecnología también evaluará la causa del daño del equipo y si se determina que es por mal uso del mismo, se procederá con la reparación, pero se informará a la OTSI para que el costo de la reparación del mismo sea descontado al usuario responsable del equipo de cómputo.

El uso de dispositivos como unidades de almacenamiento USB, CD`s o cualquier otro, es de exclusiva responsabilidad de los usuarios, los cuales deberán asegurarse de que estos no contengan ningún medio de contaminación de virus.

Los equipos de cómputo suministrados por el MEN se entregarán mediante un acta de entrega/recepción en la cual se detallará todos los equipos que se entregan, sus componentes y el software que se le ha instalado (en caso de que aplique). A partir de ese momento él usuario será responsable de los equipos y accesorios que le han sido entregados, de su cuidado y su buen uso.
En caso de que un equipo tipo móvil (sea este laptop, teléfono celular o accesorios) sea hurtado o extraviado, el usuario deberá proceder de inmediato a reportarlo a la Oficina de Tecnología y Sistemas de información mediante la Mesa de Servicios de Tecnología. En el caso de robo deberá presentar también la denuncia respectiva.
Cuando un usuario se retira del MEN o cambia de función o cargo dentro de la misma debe realizar la devolución de todos los equipos de tecnología que le han sido asignado en el transcurso en que ha desempeñado su cargo. La dependencia de Gestión Humana es responsable de comunicar este particular a la OTSI. Esta devolución estará sustentada por un acta de entrega/recepción.

La devolución deber ser a la Mesa de Servicios de Tecnología, la cual se encargará de comprobar que los equipos de cómputo sean devueltos en óptimas condiciones. En caso de que algún equipo de cómputo no sea devuelto, o sea devuelto en mal estado, el MEN procederá a realizar el descuento correspondiente por la reposición de dicho equipo de cómputo, el cual será descontado de su sueldo (en el caso de cambio de cargo), o de su liquidación (en caso de salida del MEN).

Telefonía y dispositivos móviles

Se considera "usuarios de dispositivos móviles" a quienes por las características de sus funciones asignadas dentro del MEN utilizan habitualmente un portátil, Smartphone, teléfono móvil, tableta, etc. dentro y fuera de la organización.

Los teléfonos móviles se deben utilizar exclusivamente para desempeñar funciones asignadas al cargo dentro del MEN. La OTSI se reserva el derecho de revisar la utilización del dispositivo telefónico ante cualquier sospecha de un uso inapropiado del mismo

Uso del Software legal y Derechos de Autor

Los usuarios solo podrán utilizar software legalmente adquirido y/o autorizado por el MEN.

En caso de presentarse algún tipo de reclamación por software ilegal, esta recaerá sobre el usuario responsable en donde se encontrase instalado dicho software; debido a que está atentando contra los derechos de autor.

En presentaciones, documentos, informes y demás documentos que utilicen los usuarios para funciones de su cargo, debe mencionarse la fuente de donde se extrajo la información.

Los usuarios no pueden realizar copias de software que se encuentre instalado o sea desarrollado por el MEN, para su distribución.

Acceso Inalámbrico

El uso de la red inalámbrica será exclusivo para usuarios de planta y contratistas con vínculo directo con el MEN, se habilitará el servicio previa solicitud, justificación y autorización a la Mesa de Servicios de Tecnología. Para accesos a dispositivos móviles, se realizará solo previa solicitud y justificación a la Mesa de Servicios de Tecnología.

Si alguna persona externa al MEN necesita acceso a la red inalámbrica del MEN, deberá solicitarlo accediendo a la red "INVITADO" suministrando unos datos y enviado la solicitud al usuario del MEN para aprobación.

La información que se maneja dentro del MEN, es propiedad de este y no puede ser divulgada; a no ser que esté autorizado su divulgación.

1.3.9. *POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN*

Objetivo: Asegurar que la información del Ministerio es clasificada, con el fin de que sea tratada y protegida adecuadamente.

Esquema de Clasificación de la Información

Toda la información del Ministerio debe ser identificada y clasificada de acuerdo a los niveles de clasificación definidos por la entidad.

La Oficina de Tecnologías de la Información y las Comunicaciones, Gestión Documental y Gestión Jurídica son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento y manejo de la información.

De acuerdo con la clasificación establecida por la entidad y el manejo y almacenamiento de la información, se debe tener en cuenta lo siguiente:

Acceso a la información sólo de personal autorizado.
Llevar un registro formal de acceso a la información.
Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

Etiquetado y manejo de Información

Todos los Colaboradores y terceros cuando sea el caso, deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental.

Los directores, Jefes de Oficina, Coordinadores de Grupo deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

Todos los Colaboradores y Terceros cuando sea el caso del Ministerio son responsables de la organización, conservación, uso y manejo de los documentos en los medios que son dispuestos por la Entidad.

Para una óptima administración de la información, la Oficina de Tecnología y Sistemas de Información suministra a las diferentes dependencias del MEN tres (3) recursos de almacenamiento los cuales son: onedrive, sharepoint y fileserver.

Todas las dependencias del Ministerio deben enviar al Archivo Central la documentación de forma ordenada y organizada, de acuerdo con los tiempos de retención establecidos en la Tabla de Retención Documental.

El Archivo Central del Ministerio recibe las transferencias documentales de acuerdo con cronograma anual de transferencia Documentales.

Los archivos de Gestión de las oficinas del Ministerio deben custodiar sus documentos de acuerdo con lo especificado en las tablas de Retención Documental.

La plataforma tecnológica usada para salvaguardar, conservar y facilitar la información de los documentos en medios magnéticos debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.

Se debe definir procedimientos de etiquetado de la información, de acuerdo con el esquema de clasificación definido por MEN.

El etiquetado de información debe incluir la información física y electrónica.

Las etiquetas de la información se deben identificar y reconocer fácilmente.

Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

Usos no aceptables

Hacer caso omiso, retardar o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos, solicitudes y denuncias, de igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web.

Dañar o dar como perdido los expedientes, documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.

Divulgación no autorizada de los expedientes, documentos, información o archivos.

Realizar actividades tales como borrar, modificar, alterar o eliminar información del Ministerio de manera malintencionada.

1.3.10. *POLÍTICA DE GESTIÓN DE ALMACENAMIENTO*

Objetivo: Proteger la información del Ministerio velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

Se restringe el uso de carpetas compartidas desde equipos de escritorio. Si el colaborador no adopta esta política la OTSI no se hace responsable de la pérdida o infiltración de la información.

Las carpetas compartidas sobre la infraestructura ofrecida por OTSI como File server, SharePoint, OneDrive, serán administradas por las áreas quienes velarán por el buen uso de la información y de las carpetas.

Se debe documentar los permisos y accesos sobre la carpeta compartida, usando los siguientes criterios:

- Permisos de Lectura
- Permisos de Escritura y modificación
- Permisos de Control Total.

Lo cuales serán documentados por la OTSI a través de la Mesa de Ayuda de tecnología.

La información CLASIFICADA o RESERVADA, debe utilizarse en las carpetas destinadas en el file server, para que sean incluidos en las Políticas de respaldo de información a cinta (backup).

La información pública de las áreas de la institución debe utilizarse las carpetas destinadas en el OneDrive.

La información pública para uso interno de la institución debe utilizarse en las carpetas destinadas en el share point, para que sean incluidos en las Políticas de respaldo de información.

El administrador de cada carpeta deberá fijar el límite de tiempo durante el cual estará publicada la información y compartido el recurso en la infraestructura ofrecida por la OTSI.

Cada área tendrá un único administrador que será autorizado con permisos de lectura y escritura quien administrará las carpetas y será responsable a que usuarios otorgará permisos sobre esta.

Los permisos de administrador serán gestionados por la OTSI, a través de la mesa de ayuda de tecnología con el formato adjunto.

Cada administrador de las carpetas compartidas deberá realizar semestralmente una depuración de la información y notificar a la OTSI los cambios realizados.

Las carpetas compartidas tendrán una Quota de 20 Gigas en Share point, si el área requiere mayor capacidad de almacenamiento debe justificarlo a la OTSI para ajustar la Quota como se defina según acuerdo por las dos áreas.

Se prohíbe el acceso a las carpetas compartidas a Colaboradores desde equipos de cómputo que no cuenten con antivirus corporativo actualizado.

Se prohíbe el acceso a carpetas compartidas a usuarios que no tengan una vinculación directa con el Ministerio.

Se prohíbe la publicación de archivo ejecutables (.exe, bat y dll entre otros) en las carpetas compartidas de Onedrive, SharePoint, File server, si el área requiere usar alguna de las extensiones mencionadas, debe justificarlo a la OTSI para ajustar la política, como se defina según acuerdo por las dos áreas.

La OTSI realizara monitoreo y revisiones periódicas, con el fin de velar por una correcta administración de las carpetas compartidas cada semestre.

Se prohíbe el uso carpetas para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionados con el cumplimiento de la función del colaborador.

Los permisos a las carpetas compartidas administrados por la OTSI sobre los diferentes ambientes (Pruebas, Certificaciones y Producción) se autorizarán a través de una mesa de ayuda de tecnología.

La OTSI define que los nombres a los archivos y carpetas sean lo suficientemente significativo sin que sea demasiado extenso, y que no contengan nombres de los usuarios. Se establece como longitud máxima para un nombre de archivo, 256 caracteres (un carácter puede ser una letra, número o un símbolo).

El único medio de respaldo de la información para los colaboradores es OneDrive, el cual será configurado por la OTSI.

Gestión y Disposición de medios removibles

Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, dispositivos personales "USB", discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red del Ministerio y uso hasta finalización de su contrato o cese de actividades.

Toda la información clasificada como CONFIDENCIAL o RESERVADA que sea almacenada los dientes activos de información que se requiera de protección especial de acuerdo a la calificación otorgada en el levantamiento de activos de información, debe cumplir con las directrices de seguridad estipuladas para la protección de los mismo.

Se debe llevar el registro de todos los medios removibles del Ministerio y mantenerlo actualizado.

Todos los medios removibles deben ser almacenados de manera segura.

El Oficina de Tecnología y Sistemas de Información puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad del Ministerio o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.

Los medios de almacenamiento removibles que se conecten a la red de datos del Ministerio o que se encuentren bajo su custodia, están sujetos a monitoreo por parte del Oficina de Tecnologías de la Información y las Comunicaciones.

Todos los retiros de medios de almacenamiento de las instalaciones del Ministerio, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de apoyo, definidos de acuerdo al mapa de procesos del Ministerio, a través del formato orden de salida de elementos.

Todos los medios de almacenamiento removibles propiedad del Ministerio, deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc, con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

Borrado seguro

Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por MEN para su uso dentro de la red corporativa, deben contar con su respectivo soporte.

Todos los medios de almacenamiento que contengan información del Ministerio y que salgan de la Entidad y que no se les vaya a dar más uso, deben seguir el procedimiento de borrado seguro definido por MEN, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, equipos de proveedores, discos duros externos, etc.).

Los medios de almacenamiento que contengan información del Ministerio y que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido por MEN, el cual garantiza que la información no se es recuperable (Aplica para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por degaste o falla son retirados o dados de baja).

Eliminar de forma segura (destrucción o borrado) los medios de almacenamiento que no se utilicen y que contengan información del Ministerio.

Trasferencia de medios físicos

Toda la información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles y que sean transportados fuera de las instalaciones del Ministerio, debe cumplir con las disposiciones de seguridad indicadas por la Oficina de Tecnologías de la Información y las Comunicaciones, específicamente aquellas referentes al empleo de técnicas de cifrado.

El transporte de los medios físicos se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma se evitar una afectación a la integridad y disponibilidad.

Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados.

1.3.11. *POLÍTICA DE CONTROL DE ACCESO*

Objetivo: Definir las directrices generales para un acceso controlado a la información del Ministerio.

Control de Acceso a Redes y Servicios en Red

Los roles y perfiles de usuarios de Redes se encuentran definidos por la solución ISE.

El Ministerio suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Toda actividad que requiera acceder a los servidores, equipos o a las redes del Ministerio, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización la Oficina de Tecnología y Sistemas de Información.

La conexión remota a la red de área local del Ministerio debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por la Oficina de Tecnologías de la Información y las Comunicaciones, que cuenta con el monitoreo y registro de las actividades necesarias.

La autenticación de usuarios remotos deberá ser aprobada por el jefe inmediato del usuario y bajo una solicitud con su respectivo formato a la mesa de ayuda de tecnología.

Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

Gestión de Acceso a Usuarios

Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.

El sistema debe obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 90 días.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la mesa de servicios.

Se debe mantener un registro de las 3 últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.

La Oficina de Tecnología y Sistemas de Información debe garantizar que las contraseñas se almacenen de forma cifrada utilizando un algoritmo de cifrado unidireccional.

Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo apliance, impresoras, routers, switch, herramientas de seguridad, etc.).

No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, Jefes u otras personas que lo soliciten.

Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

Reportar a la Oficina de Tecnología y Sistemas de Información sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

Reportar a la Oficina de Tecnología y Sistemas de Información sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.

Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada cuatro (4) meses.

El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información debe estar autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones.

Todo equipo de cómputo que requiera acceso a la red interna del MEN deberá tener como mínimo las siguientes medidas de seguridad: solución de antimalware instalada y actualizada, parches de seguridad al día y mecanismos de autenticación habilitado para el ingreso a la red (ISE).

Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de procesamiento de información del Ministerio, debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

Retiro de los derechos de acceso

Cada uno de los procesos de la Entidad es responsable de comunicar a la Oficina de Talento Humano y Gestión Contractual, el cambio de cargo, funciones o actividades o la terminación contractual de los Colaboradores pertenecientes al proceso. La Oficina de Talento Humano y Gestión Contractual son las encargadas de comunicar a la Oficina de Tecnología y Sistemas de Información sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

1.3.12. POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información del Ministerio.

Perímetro de Seguridad Física

Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los Colaboradores y Terceros autorizados evitar que las puertas se dejen abiertas.

Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en un lugar dentro de las instalaciones del Ministerio.

Todos los Colaboradores, Terceros y visitantes cuando sea el caso, sin excepción deben portar su carnet o escarapela en un lugar visible mientras permanezcan dentro de las instalaciones del Ministerio.

Los visitantes deben permanecer acompañados de un Colaborador del Ministerio, cuando se encuentren en las oficinas o áreas donde se maneje información.

Es responsabilidad de todos los Colaboradores y Terceros del Ministerio borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

Los visitantes que requieran permanecer en las oficinas del Ministerio por periodos superiores a dos (2) días deben ser presentados al personal de oficina donde permanecerán.

El horario autorizado para recibir visitantes en las instalaciones del Ministerio es de 8:00 AM a 5:00 PM. En horarios distintos se requerirá de la autorización del Director, Jefe de Oficina o Coordinador del Grupo correspondiente.

Los dispositivos removibles, así como toda información CONFIDENCIAL del Ministerio, independientemente del medio en que se encuentre, deben permanecer bajo seguridad durante horario no hábil o en horarios en los cuales el Colaboradores o Terceros responsable no se encuentre en su sitio de trabajo.

Las instalaciones del Ministerio deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de Colaboradores y Terceros y visitantes.

Controles de Acceso Físico

Las áreas seguras dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

En las áreas seguras, en ninguna circunstancia se puede fumar, comer o beber.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un o Colaboradores del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

Se debe contar con al menos dispositivos de control de acceso físico a los Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, el cual garantice el acceso a solo el personal autorizado.

Ubicación y Protección de los equipos.

La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Seguridad de los equipos fuera de las instalaciones

Los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, deben contar con controles de seguridad que garanticen la confidencialidad de la información.

Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente al Proceso de Gestión Administrativa y la Oficina de Tecnología y Sistemas de Información y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.

Cuando los equipos portátiles se encuentren desatendidos deben estar asegurados con una guaya, dentro o fuera de las instalaciones del Ministerio.

Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.

Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones del Ministerio.

Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser

sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado del Ministerio sin una autorización formal.

Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos del Ministerio.

1.3.13. *POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA*

Objetivo: Definir los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información del Ministerio.

Todo el personal del Ministerio debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

Todo el personal del Ministerio debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.

Todos los usuarios al finalizar sus actividades diarias deben salir de todas las aplicaciones y apagar las estaciones de trabajo.

Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave.

1.3.14. *POLÍTICA DE GESTIÓN DE CAMBIOS*

Objetivo: Asegurar que los cambios a nivel de infraestructura, aplicaciones y sistemas de información realizados en MEN se realicen de forma controlada.

Se deben establecer procedimientos para el control de cambios ejecutados en la entidad.

Toda solicitud de cambio en los servicios de infraestructura y sistemas de información del Ministerio, se debe realizar siguiendo el Procedimiento de gestión de cambios, con el fin de

asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.

Se debe llevar una trazabilidad del control de cambios solicitados.

En el procedimiento de gestión de cambios se debe especificar los canales autorizados para la recepción de solicitudes de cambios, como la Mesa de servicios, correo electrónico o un oficio dirigido al Líder de Tecnología de la Información.

Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.

Se deben especificar en qué momento existen cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada.

Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los Colaboradores o Terceros que por sus funciones tienen relación con el sistema de información.

Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.

Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

1.3.15. *POLÍTICA DE SEPARACIÓN DE AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN*

Objetivo: Reducir riesgos asociados a modificaciones, alteraciones, cambios o accesos no autorizados en sistemas en producción del Ministerio.

El Ministerio debe establecer y mantener ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información de la

Entidad. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo al inventario y clasificación de activos de información.

En la Entidad se debe seguir un procedimiento formal para el paso de software, aplicaciones y sistemas de información de un ambiente a otro (desarrollo, pruebas y producción), donde se establecen las condiciones a seguir para alcanzar la puesta en producción de un sistema nuevo o la aplicación de un cambio a uno existente. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo al inventario y clasificación de activos de información.

No se deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.

En los ambientes de desarrollo y pruebas no se deben utilizar datos reales del ambiente de producción, sin antes haber pasado por un proceso de ofuscamiento.

Se debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.

Se deben utilizar controles de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.

Las interfaces de los sistemas deben ser identificadas claramente para poder determinar a qué instancia se está realizando la conexión.

Los ambientes deben estar claramente identificados, para evitar así confusiones en la aplicación de tareas o en la ejecución de procesos propios de cada uno.

Los cambios a sistemas en producción que involucren aspectos funcionales, deben ser informados y consultados con el(los) proceso (s) propietario(s) de la información.

Se debe establecer una guía para el Desarrollo seguro de Software en MEN.

1.3.16. *POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO*

Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en MEN.

Toda la infraestructura de procesamiento de información del Ministerio, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores del Ministerio.

Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación.

Todos los Colaboradores y Terceros que hacen uso de los servicios de tecnología de la información y comunicaciones del Ministerio son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

MEN cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por la Oficina de Tecnologías de la Información y las Comunicaciones.

El antivirus adquirido por MEN, sólo debe ser instalados por los responsables de la Oficina de Tecnologías de la Información y las Comunicaciones.

Los equipos de terceros que son autorizados para conectarse a la red de datos del Ministerio deben tener antivirus y contar con las medidas de seguridad apropiadas.

Todos los equipos conectados la red del Ministerio pueden ser monitoreados y supervisados por la Oficina de Tecnologías de la Información y las Comunicaciones.

Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones.

La Entidad debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

Se deben hacer campañas de sensibilización a todos los Colaboradores y Terceros de ser el caso del Ministerio, con el fin de generar una cultura de seguridad de la información entre los Colaboradores y Terceros del Ministerio.

Los Colaboradores y Terceros del Ministerio pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los Colaboradores y Terceros cuando sea necesario siempre podrán consultar a la Oficina de Tecnología y Sistemas de Información sobre el tratamiento que debe darse en caso de sospecha de malware.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por MEN, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta establecida para ello.

El único servicio de antivirus autorizado en la entidad es el asignado directamente por la Oficina de Tecnologías de la Información y las Comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones, a efectos de reforzar el control de presencia o programación de virus o código malicioso.

La Oficina de Tecnología y Sistemas de Información es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a la red del Ministerio.

La Oficina de Tecnología y Sistemas de Información se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

La Oficina de Tecnología y Sistemas de Información se reserva el derecho de filtrar los contenidos que se trasmitan en la red del Ministerio, con el fin de evitar amenazas de virus.

Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

1.3.17. *POLÍTICA DE BACKUP*

Objetivo: Proporcionar medios de respaldo de información adecuados en MEN para asegurar la información crítica y que el software asociado se pueda recuperar después de una falla.

La Oficina de Tecnologías de la Información y las Comunicaciones, debe realizar periódicamente un análisis de las necesidades del negocio para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.

La Oficina de Tecnología y Sistemas de Información y el responsable de Seguridad de la Información junto a los propietarios de la información deben determinar los requerimientos

para respaldar la información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de TI.

La Oficina de Tecnología y Sistemas de Información debe disponer y controlar la ejecución de las copias, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico del Ministerio.

Se debe definir y documentar un esquema de respaldo de la información.

El dueño de la información es responsable de definir claramente el periodo de retención de respaldos, en función de los requerimientos de las áreas funcionales.

Se debe tener en cuenta los lineamientos de la ley 594 de 2000 o cualquiera que la modifique, adicione o derogue.

Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.

Se deben definir procedimientos para el respaldo de la información, que incluyan los siguientes parámetros:

Establecer un esquema de rotulado de las copias de respaldo, que contengan toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

Definir un el procedimiento de reemplazo de los medios de almacenamiento de copias de respaldo, una vez terminada la posibilidad de ser reutilizados de acuerdo a lo indicado por el proveedor, y asegurar la destrucción de los medios de información retirados o desechados.

Almacenar en una ubicación remota o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración.

Se deben retener por lo menos por tres periodos los activos de información del Ministerio.

Para realizar las copias de respaldo en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado por la Entidad a los que se encuentre sujeta.

Se deben asignar los niveles de protección física y ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante.

Se deben extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal al sitio alterno.

La Oficina de Tecnologías de la Información y las Comunicaciones, a través del Administrador de Bases de Datos, de la Red y servidores, debe:

Actualizar periódicamente las configuraciones de los Servidores para la correcta ejecución de las copias de respaldo.

Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.

Realizar un respaldo Diferencial semanalmente de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.

Realizar un respaldo full mensual de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.

Realizar un respaldo full anual de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.

Las copias de respaldo se deben realizar en horario no hábil, lo cual será verificado a través de Procesos Automáticos.

Una vez se verifique la correcta ejecución de las copias de respaldo, se debe retirar la cinta de Backup del robot de cintas.

Los dispositivos magnéticos que contienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra almacenada.

El sitio alterno donde se almacenan las copias de respaldo debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados.

Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores.

La Oficina de Tecnologías de la Información y las Comunicaciones, cuenta con un responsable para gestionar la entrega o retiro de las cintas de Backup del sitio externo.

Las cintas de Backup con la Información actualizada, no deben permanecer más de una semana fuera del sitio externo.

Registro de Respaldo de Información

Debe existir un procedimiento formal de administración y control de copias de respaldos que permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo.

La Oficina de Tecnologías de la Información y las Comunicaciones, mediante el Administrador de Base de Datos, Red y servidores, debe aplicar la siguiente Normativa:

1. Llevar el registro de los Respaldos de Información realizada de forma Diaria.
2. Registro del retiro de las cintas de Backup del sitio externo.
3. Registro del ingreso de las cintas de Backup al sitio externo.
4. Inventario de cintas de Backup.
5. Comprobación de Integridad de la Información

La información respaldada debe ser probada como mínimo dos veces al año, asegurando que es confiable, integra y que se estará disponible en el evento que se requiera para su utilización en casos de emergencia.

Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.

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.

La Oficina de Tecnologías de la Información y las Comunicaciones, a través del Administrador de la Base de Datos, de Red y Servidores, debe aplicar los siguientes lineamientos:

Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los Servidores.

Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.

Validar la integridad y accesibilidad de las cintas magnéticas por lo menos cada cuatro meses.

Mantener siempre una copia de la información de los Servidores, por lo menos con una antigüedad no superior a 24 horas.

Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la Base de Datos para así asegurar la integridad de la información respaldada.

Respaldo de Información para Usuarios Finales

Todos los usuarios son responsables de realizar los respaldos de información personal almacenada en los equipos asignados.

Toda la información relevante a las funciones del colaborador debe ser almacenada en el Onedrive suministrado por la OTSI.

La Oficina de Tecnologías de la Información y las Comunicaciones, debe mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad, y otros.

Ningún usuario puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado fuga de información.

Todos los Colaboradores y Terceros del Ministerio deben dar estricto cumplimiento a esta política y el que haga caso omiso puede ser sujeto a acciones disciplinarias o civiles, incluyendo la terminación del respectivo contrato.

Se debe elaborar un plan de emergencia para todas las aplicaciones que manejen información crítica de la Entidad, el responsable de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

Es responsabilidad todos los Colaboradores y Terceros almacenar la información crítica asociada con su labor en el servidor de archivos establecido, para garantizar que la información está siendo respaldada.

1.3.18. *POLÍTICA DE EVENTOS DE AUDITORIA*

Objetivo: Asegurar que los registros de los eventos y las operaciones realizadas sobre los sistemas de información y plataforma tecnología del Ministerio permitan contar con evidencia necesaria para la gestión de incidentes de seguridad de la información.

Registro de eventos

Todos los accesos de usuarios a los sistemas, redes de datos y aplicaciones del Ministerio, deben ser registrados.

Se deben habilitar los log de eventos requeridos y deben ser revisados con regularidad.

Se debe hacer copia de respaldo de información de los eventos de auditoria, ya que en caso de un incidente de seguridad de la información deben estar disponibles.

Registro del administrador y del Operador

Todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información del Ministerio deben estar debidamente registradas.

Los administradores de la infraestructura tecnología y de procesamiento de información deben tener asignada una cuenta de usuario exclusiva, a través de la cual se realizarán las actividades de administración y debe ser entregada a través de un proceso formal.

Sincronización de relojes

Todos los relojes de la infraestructura de procesamiento de información del Ministerio deben estar sincronizados con la hora legal Colombiana.

1.3.19. *POLÍTICA DE GESTIÓN DE SEGURIDAD DE LAS REDES*

Objetivo: Establecer los controles necesarios para proteger la información del Ministerio transportada desde la red interna.

La Oficina de Tecnología y Sistemas de Información es la responsable de administrar y gestionar la red del Ministerio.

La Oficina de Tecnología y Sistemas de Información es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

El MEN proporciona a los Colaboradores y Terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones.

El trabajo a través de medios remotos a la red de datos del Ministerio, sólo se permitirá de acuerdo a la Política de Teletrabajo establecida por la Entidad.

Separación de las Redes

MEN debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red.

Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

1.3.20. *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES*

Objetivos: Establecer los criterios de seguridad la información para la información accedida por los proveedores.

Consideraciones de seguridad en los acuerdos con terceras partes

En todos los Contratos o Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar Acuerdos de Confidencialidad sobre el manejo de la información.

Los Acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.

Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

1.3.21. *POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*

Objetivo: Gestionar todos los incidentes de seguridad de la información reportados en MEN, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Reporte sobre los eventos y las debilidades de la seguridad de la información

Todos los Colaboradores y Terceros de la entidad y terceras partes tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

Se deben establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

Se debe definir el procedimiento de atención de incidentes de seguridad de la información del Ministerio.

Se debe llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos.

Se debe recolectar las evidencias (CCP, Fiscalía, colcert, mintic) necesarias lo más pronto posible después del reporte del incidente.

Escalar los incidentes a niveles superiores en caso de que sea requerido.

Se debe hacer evaluaciones de los incidentes presentados ya que se puede necesitar de controles adicionales.

Para el transporte de elementos, se debe llevar la cadena de custodia.

Se deben documentar todos los incidentes de seguridad reportados.

Se debe realizar sensibilización a todos los usuarios sobre incidentes de seguridad de la información.

1.3.22. *POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO*

Objetivo: Garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información del Ministerio.

MEN debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis.

El Ministerio cuenta con un centro de datos alterno, para garantizar la disponibilidad de los servicios críticos de la Entidad, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.

El Ministerio cuenta con un Plan de Recuperación de Desastres que asegura la continuidad de las operaciones tecnológicas de sus procesos críticos, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.

Para el Ministerio su recurso más importante es el Recurso Humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier evento.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan, deben estar incorporados y definidos en los Planes de contingencias.

Se debe establecer un plan de pruebas periódico del plan de Contingencia de la Plataforma Tecnológica del Ministerio.

1.4. POLITICA DE GESTIÓN DOCUMENTAL

Esta política se definió e incorporó en el Programa de Gestión Documental de la Entidad, para lo cual se tuvieron en cuenta las directrices definidas en el Decreto 2609 de 2012, Artículo 6, en el cual se establecen los componentes mínimos que debe incorporar. Dicha política fue aprobada por el Comité Institucional de Desarrollo Administrativo.

2. BIBLIOGRAFIA

Departamento Administrativo de la Función Pública, Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

Guías del modelo de seguridad y privacidad emitidas por MINTIC.

Departamento Administrativo de la Función Pública, Guía para la administración del riesgo.

Departamento Administrativo de la Función Pública, Planeación de los Recursos Humanos-Lineamientos de política, estrategias y orientaciones para la implementación.

Presidencia de la República - Secretaría de Transparencia, Documento “Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.

Presidencia de la Republica – Alta Consejería Presidencial para el Buen Gobierno y la Eficiencia Administrativa, Modelo Integrado de Planeación y Gestión.

Norma técnica ISO 27001:2013

Norma técnica ISO 27005:2013

Control de Cambios		
Versión	**Fecha de entrada en vigencia**	**Naturaleza del cambio**
01	01-06-2018	Creación del documento en el SIG, para definir los lineamientos y directrices que se deben seguir por parte los colaboradores y terceros del Ministerio, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información.

02	25-10-2018	Se actualiza el logo y los colores de este documento de acuerdo con el nuevo manual de imagen institucional generado por la Presidencia de la Republica para todas las entidades del Gobierno, lineamiento recibido de la Oficina Asesora de Comunicaciones el 31-08-2018. Al ser este un ajuste de forma y no de contenido conserva el flujo de aprobación de la versión anterior y no requiere aprobación por parte del líder del proceso.
03	El documento entra en vigencia a partir de su publicación en el SIG	Se actualiza nuevamente el logo de este documento de acuerdo con el manual vigente de imagen institucional generado por la Presidencia de la República para todas las entidades del Gobierno. Al ser este un ajuste de forma y no de contenido conserva el flujo de aprobación de la versión anterior y no requiere aprobación por parte del líder del proceso.

Ruta de Aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Yuli Andrea Parra Amaya	**Nombre**	Luis Carlos Serrano	**Nombre**	Hernán Guiovanni Ríos Linares
Cargo	Oficial de Seguridad de la Información	**Cargo**	Responsable Seguridad Informática OTSI	**Cargo**	Jefe de Tecnología y Sistemas de Información