MANUAL DE SEGURIDAD INFORMÁTICA

El Ministerio de Educación Nacional declara como única documentación válida la ubicada en el aplicativo SIG, y entra en vigencia a partir de la publicación toda copia de este se declara COPIA NO CONTROLADA

MANUAL DE SEGURIDAD INFORMATICA
Oficina Tecnología y Sistemas de Información

Tabla de contenido

1. OBJETIVOS

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

- 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 MEN.
- 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.

2. ALCANCE

Los Lineamientos del presente documento de seguridad informática de la OTSI(OTSI) del Ministerio de Educción Nacional (MEN), aplica para funcionarios, contratistas, personal de apoyo y terceros no vinculados directamente al MEN, pero que presten su servicio y utilicen tecnología de información, equipos propios del MEN o arrendados y a los equipos de personas externas que sean conectados a la red del MEN.

La revisión de estos lineamientos, así como de los objetivos del Manual de Seguridad Informática, debe realizarse con una periodicidad mínima de una vez al año, o cuando se originen cambios en la entidad que puedan afectar la operación de los servicios Tics, o durante las revisiones periódicas que desde la dirección se ejecutan para asegurar la continuidad del sistema.

3. RESPONSABILIDADES

3.1. Principios Generales

Todos los directivos y los colaboradores del MEN tienen la responsabilidad de proteger la seguridad de los activos y de los recursos de TI bajo su control, de acuerdo con las instrucciones y la capacitación recibidas. Deben definirse responsabilidades expresas para la implementación, operación y administración de los controles de seguridad informática y deben discriminarse dichas responsabilidades de aquéllas que sean incompatibles cuando esto pudiera debilitar el nivel del control interno en forma inaceptable.

3.2. Oficina de Tecnología y Sistemas de la Información

El Responsable de la Seguridad Informática del MEN, será la Oficina de Tecnología y Sistemas de la Información el cual se encargará de:

a) Desarrollar, revisar y actualizar las políticas y lineamientos.
b) Proporcionar una dirección funcional en el ámbito de seguridad informática en el MEN;
c) Acordar las prioridades de seguridad informática en el MEN;
d) Coordinar la implementación de las políticas y lineamientos dentro del MEN;
e) Monitorear e informar sobre el trabajo de seguridad informática a la Dirección;
f) Dar asesoramiento sobre la seguridad física de todas las instalaciones del MEN;
g) Garantizar que la seguridad de todos los activos de TI esté debidamente protegida;
h) que se le dé la prioridad correspondiente al trabajo de seguridad informática, de manera oportuna, en todos los proyectos de TI;
i) Definir lineamientos de gestión de acceso que permitirá únicamente el ingreso a los usuarios autorizados por la dependencia correspondiente, y en el nivel asignado, sobre los datos, la red y sistemas de información necesarios para desempeñar sus tareas habituales.
j) Definir los lineamientos de contraseñas robustas para los usuarios de las Bases de Datos, Red y Sistemas de Información.
k) Definir las herramientas, procedimientos, formatos entre otros, para la implementación de un sistema de autenticación de acceso a los usuarios internos y externos en las diferentes plataformas tecnológicas
l) Definir las herramientas, procedimientos de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad.
m) Garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica del MEN por medio de los terceros autorizados.
n) Proveer las herramientas tales como antivirus, antimalware, anti spam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica del MEN y los servicios que se ejecutan en la misma.
o) Establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en el MEN.
p) Conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
q) Validar los riesgos que genera la migración hacia nuevas versiones del software operativo.
r) Establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo del MEN.
s) Realizar el borrado seguro del contenido de medios reutilizables que contengan información reservada del MEN que se van a retirar de las instalaciones.
t) Realizar respaldo a través del proceso de gestión de copias de respaldo de la información reservada del MEN cuya duración es mayor al tiempo de vida del medio en donde se encuentra almacenada.
u) Realizar pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, a través de un tercero, que cumplan con estándares internacionales.
v) Generar y ejecutará o monitoreará planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
w) Crear y liderará el Comité de Gestión de Vulnerabilidades conformado por personal de Infraestructura, Aplicaciones, Oficial de Seguridad de la Información, Oficial de Seguridad Informática del Operador de la Red del MEN y el Oficial de Seguridad Informática de la Interventoría. El Comité de Gestión de Vulnerabilidades se reunirá cada mes (1) para realizar

seguimiento a los planes y acciones de las vulnerabilidades identificadas y en proceso de remediación.

x) Coordinar con el operador de servicios Tics las acciones en materia de Seguridad Informática que deberán llevarse a cabo en el MEN;
y) Proponer políticas y especificaciones técnicas de bienes y servicios, procedimientos, acciones y medidas específicas en materia de Seguridad Informática; que sean aplicables a cualquiera de los elementos tecnológicos que integren la plataforma de Seguridad Informática de la entidad;
z) Coordinar con el operador de servicios Tics la administración del sistema de autentificación de usuarios que permite el acceso a los recursos, servicios informáticos y comunicaciones del MEN;
aa) Coordinar la definición, la administración y las acciones técnicas en materia de Seguridad Informática con el operador de servicios Tics, lideres técnicos, lideres funcionales, los administradores de servicios y con otras áreas que realicen funciones informáticas para el MEN;
bb) Del sistema de gestión de incidentes de seguridad de la información, analizar aquellos que involucren los servicios informáticos a fin de establecer controles para detectar, corregir y prevenir incidentes posteriores.
cc) Proponer medidas específicas en materia de Seguridad Informática que deberán atender los usuarios de los bienes, de los recursos y servicios informáticos y de la información electrónica;
dd) Proponer la plataforma tecnológica para el soporte del ambiente de Seguridad Informática de la entidad;
ee) Mantener actualizado el inventario de Activos Informáticos relacionados con la Plataforma de Seguridad Informática del MEN como complemento del inventario de activos de Información e infraestructura con que esta cuenta;
ff) Realizar revisiones selectivas a los controles de los activos informáticos para asegurar que se mantenga sobre ellos la aplicación de las recomendaciones y lineamientos en materia de Seguridad Informática;
gg) Publicar en el Sistema de Gestión Documental los documentos técnicos (lineamientos, políticas, guias, procesos, procedimientos) en materia de Seguridad Informática emitidos por la OTSI
hh) Promover el cumplimiento de la Política de Seguridad de la Información del MEN;
ii) Definir controles de detección y prevención para la protección contra software malicioso;
jj) Implementar controles para la protección contra software malicioso en la infraestructura de cómputo y telecomunicaciones;
kk) Definir las cuentas de acceso para la administración de los equipos de cómputo para proteger la configuración de estos, las cuales hará del conocimiento al operador de servicios Tics dentro de la OTSI;
ll) Revisar los registros de eventos de los diferentes equipos que formen parte del ambiente de seguridad del MEN a fin de colaborar con el responsable del servicio en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad;
mm) Almacenar y administrar las contraseñas incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados;
nn) Revocar las contraseñas, cuando las claves estén comprometidas o cuando un usuario que haga uso de ellas se desvincule de la entidad;

oo) Recuperar las contraseñas perdidas o alteradas como parte de la administración para su continuidad;
pp) Coordinar, administrar y registrar todos los nombres de equipos y dominios que son accesibles a la red del MEN;
qq) Controlar y registrar todos los certificados de seguridad de los sitios de la entidad;
rr) Coordinar con el Oficial de Seguridad y con los especialistas de seguridad del operador para manejar los reportes de incidentes y anomalías de Seguridad Informática;
ss) Promover la cultura de la Seguridad Informática entre los administradores y usuarios de la información y de los recursos, bienes y servicios informáticos institucionales; y
tt) Las demás que determine la OTSI o la persona encargada de la Seguridad Informática.

3.3. Los Colaboradores

Todos los Colaboradores del MEN son responsables de:

a) cumplir con las instrucciones y los procedimientos de seguridad aprobados y aquellas responsabilidades de seguridad específicas documentadas en los objetivos personales y la descripción de tareas;
b) mantener la confidencialidad de las contraseñas personales y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados;
c) proteger la seguridad de los equipos de cómputo, así como de la información bajo su control directo;
d) informarle a la directiva inmediata o de seguridad cualquier sospecha de violaciones de la seguridad y de cualquier debilidad detectada en los controles de esta, incluyendo sospechas de divulgación de contraseñas.
e) acatar con los lineamientos establecidos dentro de este documento

3.4. Dirección de Talento Humano y Dirección de Contratación

a) Debe informar a la OTSI toda novedad de personal o contratos.

3.5. Área Administrativa

a) Responsable del inventario de equipos y su actualización, según se establezca en las normas vigentes;
b) proporcionar los suministros de los equipos de impresión que permitan la operación adecuada de los procesos de la entidad.

3.6. De la prestación de servicios por terceros.

c) Todo proveedor que proporcione servicios informáticos al MEN que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información publica y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique al MEN.
d) Todo servicio informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar que se cumplan con los términos estipulados en los acuerdos o contratos del MEN.

3.7. Implementación

A fin de implementar controles de seguridad informática que sean efectivos y eficaces, el manual de seguridad informática es:

a) implementar un conjunto coherente y equilibrado de controles de prevención, detección y recuperación;
b) implementar controles complementarios, y que se refuercen mutuamente, en todos los sistemas y actividades interrelacionadas. Debe evitarse el depender en un solo nivel de controles;
c) automatizar los controles, cuando sea posible y se justifique el costo;
d) simplificar los controles y reducir la variedad y complejidad de las herramientas de seguridad cuando sea posible y se justifique el costo. Políticas y Lineamientos de Seguridad Informática

4. LINEAMIENTOS DEL MANUAL DE SEGURIDAD INFORMATICA

Los presentes lineamientos se dictan con el objeto gestionar adecuadamente la Tecnología, los sistemas informáticos y el ambiente tecnológico del MEN.

4.1. Del buen uso

4.1.1. De los activos tecnológicos

a) Los activos tecnológicos definidos y entregados por la OTSI son:
   - PCs. de escritorio y portátiles.
   - Impresoras.
   - Escáner.
   - Teléfonos celulares.
   - Carteleras Digitales.

   Toda esta propiedad del MEN.
b) La OTSI asignara a los Colaboradores y a las áreas de acuerdo con la necesidad los activos informáticos necesarios para uso de sus funciones y estos serán los únicos responsables de su utilización, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos. En caso de requerir compartirlo o prestar el activo informático, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.
c) Los PCs de escritorio y portátiles se encuentran configurados con el Hardware y Software básico necesario para su funcionamiento y cumplimiento de las funciones:
   - 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

d) Toda movilización del activo informático dentro o fuera de las instalaciones de la entidad es responsabilidad del colaborador asignado a este.
e) Cuando exista algún incidente (robo, extravió, daño físico, etc.) que afecte de manera directa a un activo informativo del MEN, deberá ser notificado de inmediato a la OTSI mediante la Mesa de Ayuda de Tecnología, donde esta informara las acciones a tomar.
f) Solo el personal de la Mesa de Ayuda de Tecnología esta autorizada a realizar reparaciones, cambios, desarme de los activos informáticos del MEN.
g) La OTSI realizara periódicamente actualizaciones a los sistemas operativos, parches de seguridad, antivirus y de las aplicaciones instaladas en los PCs de escritorio y portátiles de los colaboradores del MEN, los cuales deben garantizar el reinicio de estos para la aplicación de estas.
h) Todos los activos tecnológicos propiedad del MEN deberán estar incluidos dentro del dominio minedu.gov.co y aplicar las políticas de seguridad definidas por la OTSI tales como: un fondo de pantalla definido por el área de Comunicaciones, acceso al activo tecnológico de acuerdo con su perfil, bloqueo a las propiedades del sistema operativos, entro otros. Todo activo tecnológico que no se encuentre dentro del dominio o no cuente con las políticas de seguridad definidas por la OTSI será solicitado al colaborador por medio de los funcionarios de la Mesa de Ayuda tecnología donde estos efectuaran las configuraciones necesarias para cumplir estos lineamientos. De negarse el Colaborador a entregar el activo tecnológico se informará al Jefe inmediato para que este tome las acciones pertinentes o comunique a la OTSI el porque la necesidad que el activo tecnológico se encuentre por fuera del dominio del MEN.
i) Los Colaboradores con activos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por La Oficina de Tecnología y Sistemas de Información; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

4.1.2. Del Internet

a) La OTSI provee el servicio de internet a todos los colaboradores del MEN para adelantar exclusivamente las funciones asignadas a su cargo utilizándose de forma austera y eficiente.
b) Abstenerse de publicar Información relevante al MEN independiente de su formato (word, excel, Power Point, PDF, avi, mp3,mp4 o cualquier otro formato actual o futuro) o su nivel de clasificación de confidencialidad en sitios de internet no licenciados por el MEN en los denominados discos, nubes, carpetas virtuales o cualquier sistema de publicación de documentos actual o futura dentro o fuera de la entidad.
c) Abstenerse de utilizar aplicaciones que permitan evadir los controles implementados por el MEN.
d) El acceso a páginas Web con contenido inapropiado se encuentra restringido. Sin embargo y si por la naturaleza del cargo se requiere el acceso a páginas de acceso contralado, se debe solicitar a la Mesa de Ayuda su acceso adjuntando la aprobación y justificación por parte del jefe inmediato.

e) Abstenerse de descargar imágenes, sonidos, música y videos, a su vez descargar archivos o instalar programas de sitios web desconocidos o gratuitos. debido a que puede saturar el canal y convertirse en
f) La OTSI se reserva el derecho de bloquear sitios que se detecten como peligrosos (con contenidos no autorizados) para la seguridad de los activos informáticos.
g) Cada colaborador es responsable del adecuado manejo de los usuarios de autenticación y contraseñá a la hora de ingresar a los diferentes sistemas de información que consulte en internet.

4.1.3. Del Correo electrónico

a) El único servicio de correo
b) El correo electrónico institucional es para uso exclusivo de los Colaboradores activos, dependencias del MEN, sistemas de información, etc., por lo cual deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.
c) Las áreas

4.1.4. Del ahorro de energía

La OTSI garantizara mediante políticas en los activos informáticos el apagado de estos en el horario establecido por el MEN.

4.2. Derechos de Autor

a) Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los colaboradores se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor y que se encuentren licenciados por parte del MEN.
b) Para asegurarse de no violar los derechos de autor, no está permitido a los colaboradores copiar ningún programa instalado en los activos informáticos de la entidad en ninguna circunstancia sin la autorización escrita de la OTSI. No está permitido instalar ningún programa en el activo informático sin dicha autorización o la clara verificación de que la entidad posee una licencia que cubre dicha instalación.
c) No está autorizada la descarga de Internet de programas informáticos no autorizados por OTSI. De ser necesario por cualquier área del MEN se debe solicitar por medio de la Mesa de Ayuda de Tecnología la validación de la OTSI del programa informático.
d) No esta permitido que los colaboradores realicen copias no autorizadas de programas informáticos, cualquier tipo de información, sistemas de información, base de datos, etc.
e) No esta permitido que los colaboradores carguen o descarguen programas informáticos no autorizados de Internet, incluidos entre otros la descarga de programas informáticos para utilizar sistemas de peer-to-peer (P2P – Ej. Kazaa) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.
f) No esta permitido que los colaboradores realicen intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución de estos.

g) Si se evidencia que algún colaborador ha realizado copia de programas informáticos o música en forma ilegal, la OTSI comunicara al jefe inmediato para que este tome las medias necesarias.
h) Si se evidencia que algún colaborador ha realizado copia de programas informáticos, sistemas de información, bases de datos, etc., propiedad del MEN en forma ilegal para dárselos a un tercero, la OTSI comunicara al jefe inmediato para que este tome las medias necesarias.
i) El MEN provee a sus colaboradores tres (3) licencia de Office 365 para su uso personal, estas asociadas a la cuenta de correo del MEN. Esta licencias no pueden ser cedidas, vendidas o alquiladas.
j) Si un usuario desea utilizar programas informáticos autorizados por el MEN en su hogar, debe consultar a la OTSI por medio de la Mesa de Ayuda Tecnología para asegurarse de que ese uso esté permitido.
k) El personal de la Mesa de Ayuda de Tecnología revisará los activos informáticos constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si los colaboradores poseen licencias para cada una de las copias de los programas informáticos instalados.
l) Si se encuentran programas informáticos sin licencias, licencias free, licencias no corporativas, etc., estas serán eliminadas y, de ser necesario, reemplazadas por programas informáticos con licencia con que cuente el MEN.
m) Los Colaboradores utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.
n) Los Colaboradores que se enteren de cualquier uso inadecuado que se haga en el MEN con los programas informáticos o la documentación vinculada a estos, deberán ser notificado por medio de la Mesa de Ayuda de Tecnología.
o) Según las leyes vigentes de derechos de autor, los Colaboradores involucrados en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.
p) Los Colaboradores que realicen, adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo con las circunstancias. Dichas sanciones pueden incluir suspensiones y despidos justificados.
q) El operador de servicios TICs del MEN deben contar con todos los programas tecnológicos necesarios para la operación licenciados y a nombre de esta.
r) El operador de servicios TICs del MEN no puede hacer uso de los programas informáticos y licencias de la entidad.

4.3. Control de Accesos

4.3.1. Gestión de Acceso de Usuarios de Correos, Bases de datos Sistemas de Información.

4.3.1.1. Creación de usuarios de Correo.

La OTSI establece como mecanismos para la creación de usuarios de correos a través de una solicitud de Mesa de ayuda de Tecnología, generada por el personal de la Subdirección de Talento Humano y todos aquellos que requieran realizar la creación, modificación y eliminación de usuarios del directorio activo en el MEN.

4.3.1.2. Creación de usuarios en Bases de Datos y Sistemas de Información.

La creación de usuarios de Bases de Datos y sistemas de Información se debe realizar a través de una solicitud de Mesa de ayuda de Tecnología, adjuntando el Formato - Configuración Usuarios Bases de Datos.

La solicitud para creación de usuarios en bases de datos debe ser aprobada por el jefe inmediato del solicitante.

4.3.1.3. Creación de usuarios de Red.

La OTSI establece como mecanismos para la creación de usuarios de red a través de una solicitud de Mesa de ayuda de Tecnología, en donde se realizará la creación, modificación y eliminación de usuarios del directorio activo en el MEN. Sistemas de Administración de Contraseñas.

El sistema de administración de contraseñas para usuarios de correo, Bases de Datos, sistemas de información y redes del MEN deben cumplir como mínimo con las siguientes especificaciones:

a) Obligar el uso de los usuarios y contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de estas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
d) No permitir mostrar las contraseñas en texto claro cuando son ingresadas.
e) La longitud mínima de la contraseña sea ocho (8) caracteres combinadas aleatoriamente entre números, letras minúsculas, letras mayúsculas y símbolos.

4.3.1.4. Uso y creación de Contraseñas de usuarios de Correo, Bases de Datos, y Redes.

El uso y creación de contraseñas para usuarios de correos, Bases de datos, Sistemas de Información y Redes deben estar alineadas con el numeral del buen uso y creación de contraseñas seguras dentro de este manual.

4.3.1.5. Uso y creación de Contraseñas de usuarios de Sistemas de Información.

La OTSI es la encargada de realizar la creación de las cuentas de usuarios de los sistemas de Información y velar por el buen uso de ellas.

La administración de usuarios en los sistemas de información del MEN, debe estar alineada a la Guía de Gestión de Usuarios que tiene por objetivo la creación, actualización e inactivación de usuarios en los diferentes sistemas de información.

4.3.1.6. Alta y baja de contraseñas de usuarios de Correo, Bases de Datos, Sistemas de Información y Redes.

La OTSI es la encargada de realizar las gestiones asociadas a la creación, edición o eliminación de contraseñas.

La administración y buen uso de contraseñas es responsabilidad de cada usuario de correo, Bases de Datos, Sistemas de Información, redes y deben estar alineadas con la política de uso y creación de contraseñas seguras.

Las contraseñas deben estar almacenadas en un sistema informático protegido mediante tecnologías diferentes a las utilizadas para la identificación y autenticación de usuarios.

4.3.1.7. Sustitución de contraseñas de usuarios de Correo, Bases de Datos, Sistemas de Información y Redes.

Para la sustitución de las contraseñas para usuarios de correo, Bases de Datos, Sistemas de Información y Redes se debe realizar bajo las siguientes premisas:

a) Cumplimiento del periodo de rotación establecido para la contraseña.
b) Cambio de contraseña decidido por el usuario o la OTSI.
c) Cambio de contraseña por olvido, pérdida o sospecha de haber sido comprometida la seguridad de la anterior.
d) Cambio de una contraseña por defecto.
e) El responsable de iniciar un procedimiento de cambio de contraseña podrá ser el dueño de la cuenta cuya contraseña ha de cambiarse, o OTSI (Responsable del Sistema) del MEN.

4.3.1.8. Control de Identificación y Autenticación de Usuarios de Correo, Bases de Datos, Sistemas de Información y Redes.

La OTSI define que todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

4.3.1.9. Sesiones Inactivas

Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que Terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

Si los sistemas de información detectan inactividad por un periodo igual o superior a cinco (5) minutos, deben automáticamente aplicar, "timeout" es decir, finalizar la sesión de usuario

4.3.1.10. Responsabilidades de los Usuarios de usuarios de Correo, Bases de Datos, Sistemas de Información y Redes.

La OTSI considera las siguientes responsabilidades de los usuarios de correo, Bases de Datos, Sistemas de Información y Redes:

a) Los usuarios de correo, Bases de Datos, Sistemas de Información y Redes son responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
b) Los colaboradores no deben compartir sus cuentas de usuario y contraseñas con otros colaboradores o con personal provisto por terceras partes.
c) A los colaboradores que les fuese asignada una cuenta y contraseña de otras entidades deberán cumplir con las políticas del MEN, así como las políticas de seguridad de la entidad que asigna dicha cuenta.
d) Los colaboradores y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información del MEN deben acogerse a lineamientos y políticas para la configuración de cuentas de usuario y contraseñas implantados por el MEN, con el fin de garantizar una gestión y administración adecuada de las cuentas de usuario y contraseñas.

Las cuentas creadas en los dominios del MEN, asignadas a las secretarias se ajustarán a los siguientes Lineamientos

a) Serán bloqueadas automáticamente después de estar inactiva en un tiempo de sesenta (60) días.
b) Serán eliminadas automáticamente después de estar inactivas en un tiempo de noventa (90) días.
c) Serán administradas por la OTSI.

4.3.2. Acceso a las Bases de Datos y Sistemas de Información.

Toda la información del MEN deberá únicamente ser operada a través de un mismo tipo de sistema manejador de base de datos y sistemas de información para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.

a) El acceso a los sistemas de información deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información del MEN. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
b) Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.

c) Los datos de los sistemas de información deben ser respaldados de acuerdo con la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados.
d) En cuanto a la información de los equipos de cómputo suministrados a los colaboradores, se recomienda a los usuarios que realicen sus propios respaldos en la aplicación de respaldo en la nube entregada por el MEN (OneDrive).
e) Todos los sistemas de información que se tengan en operación deben contar con el protocolo de paso a producción.
f) Los sistemas de información deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoria y Control).
g) Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

4.3.3. Acceso a las Redes

El acceso de los colaboradores a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

a) Se aplican mecanismos adecuados de autenticación para los usuarios y los equipos.
b) Se exige control de acceso de los usuarios a los servicios de información.
c) Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la entidad.
d) Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la entidad.
e) El acceso de las redes del MEN es de uso exclusivo y único para la infraestructura provista.

4.3.4. Roles y perfiles de usuarios (según ISE)

Los roles y perfiles de usuarios de Redes, se encuentra contenida en la matriz de roles.

4.3.4.1. Acceso a Servidores.

La OTSI, define que los servidores físicos y virtuales, deben estar bajo un solo administrador (Operador de servicios TICs).

Los servidores Físicos y Virtuales serán accesados por Consola o por escritorio remoto conservando las reglas definidas en el siguiente:

Ambiente	Consola y escritorio remoto	Reglas tráfico entrante
Pruebas	Compartido (MEN-Operador de red)	1. Todo cerrado excepto. a. Puertos documentados para su respectivo

		servicio y buen funcionamiento de aplicación. b. Permisos de acceso hacia los servidores. 2. Las reglas se depuran cada mes meses. 3. Evitar reglas provenientes de 'any'. Es preferible especificar IP o rango de IP.
Producción	Operador del Servicio	1. Todo cerrado excepto. a. Puertos documentados para su respectivo servicio y buen funcionamiento de aplicación. 2. Las reglas se depuran cada tres meses. 3. Evitar reglas provenientes de 'any'. Es preferible especificar IP o rango de IP.
Certificación	Operador del Servicio	1. Todo cerrado excepto. a. Puertos documentados para su respectivo servicio y buen funcionamiento de aplicación. 2. Las reglas se depuran cada tres meses. 3. Los permisos para servicios de administración (ssh, rdp, rpc, etc) no deben provenir de 'any', sino de IP o rango de IP.

Los accesos de los diferentes ambientes están limitados solo al tipo de ambiente requerido ya que no se debe mezclar los ambientes.

4.3.4.2. Control de acceso de los usuarios para uso de la red del MEN.

La OTSI define como control de acceso de los usuarios a las redes los siguientes lineamientos:

a) Los usuarios del MEN únicamente deben tener permiso de acceso directo a las aplicaciones y bases de datos, para cuyo uso están específicamente autorizados.
b) Todos los accesos de los usuarios remotos a sistemas y aplicaciones de información del MEN deben estar controlados por medio de autenticación.

c) Todas las conexiones remotas que se realicen a sistemas de información del MEN deben ser autenticadas.
d) Los puertos empleados para diagnóstico remoto y configuración deben estar controlados de forma segura, deben estar protegidos a través de un mecanismo de seguridad adecuado y un procedimiento para asegurar que los accesos lógicos y físicos a estos son autorizados.

4.3.4.3. Autenticación de Usuarios en la red para Conexiones Externas

La autenticación de usuarios remotos deberá ser aprobada por el jefe inmediato del colaborador y bajo una solicitud con su respectivo formato.

4.3.4.3.1. Responsabilidades del uso de las redes de MEN.

Cada uno de los colaboradores del MEN, es responsable de usar de forma adecuada los recursos de red y de seguir los procedimientos definidos para el acceso a las redes.

4.3.5. Accesos al Sistema Operativo (WINDOWS, LINUX entre otros).

Los medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos deberán contener como mínimo las siguientes características:

a) Autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;
b) Registrar intentos exitosos y fallidos de autenticación del sistema;
c) Emitir alarmas cuando se violan las políticas de seguridad del sistema;
d) Suministrar medios adecuados para la autenticación cuando sea apropiado, restringir el tiempo de conexión de los usuarios.
e)

4.3.6. Acceso a los sistemas de Información

Todos los colaboradores deben acceder a los recursos de servicios de información a través de la cuenta de usuario asignada.

El acceso lógico al software de aplicación se restringe a usuarios no autorizados.

El acceso a las aplicaciones y bases de datos debe ser independiente del acceso al sistema operativo.

4.3.6.1. Gestión de privilegios.
La asignación, modificación o revocación de privilegios en los Sistemas de Información del MEN será solicitada por los responsables del departamento o área a la que pertenezca el destinatario de dichos privilegios.

Existirán privilegios asociados a:

a) Cada usuario.
b) Cada perfil, tales como: Administrador, Operador, Usuario Externo, Usuario Interno, Usuario Temporal o Etc.
c) Cada recurso, tales como: Bases de datos, Aplicaciones. o Etc.
d) Cada permiso, tales como: Lectura, Escritura o Control total.

Los sistemas deben estar diseñados o configurados de tal forma que sólo se acceda a las funciones permitidas.

La información se creará al dar de alta a un usuario por primera vez en alguno de los sistemas afectados, y deberá mantenerse actualizada, registrándose todas aquellas modificaciones que se produzcan en los privilegios de acceso hasta el momento en que el usuario haya causado baja en todos los sistemas incluidos en el alcance.

4.3.6.2. Revisión de privilegios.

Al menos, cada año, se realizará una revisión de los privilegios de acceso de todos los usuarios.

Cuando se trate de privilegios especiales (administrador, root, etc.), tal revisión de privilegios se deberá realizar, al menos, cada 1 año, y, en cualquier caso, siempre que existan:

a) Alta de nuevos usuarios.
b) Baja de usuarios.
c) Además, los privilegios de acceso de usuarios, tanto internos como externos, deben ser revisados siempre que existan cambios en las funciones o responsabilidades. Para ambos tipos de usuarios se tendrán en cuenta, al menos, las siguientes cuestiones:
    - Necesidad de nuevos permisos.
    - Cancelación de antiguos permisos.
    - Segregación de funciones.
    - Devolución de activos y modificación o cancelación de permisos de accesos físicos.
    - Modificación de contraseñas de acceso.
    - Notificación al personal implicado de su baja o cambio.
    - Necesidad de retención de registros.

4.3.6.3. Cancelación de Privilegios.

Todos los privilegios de accesos de usuarios de correo, Bases de Datos, Sistemas de Información y Redes tanto internos como externos deben ser cancelados en el momento de la finalización de su contrato o prestación de sus servicios en el MEN.

Los accesos lógicos a los activos de información deben ser removidos por los administradores de sistemas de forma inmediata.

Las cuentas de acceso de correo, bases de datos, sistemas de Información y redes se deben colocar en modo inactiva.

4.3.6.4. Desarrolladores (INTERNOS Y EXTERNOS)

Los desarrollares deben cumplir y acatar las políticas de seguridad de la información.

Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

Los desarrolladores deben garantizar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

Los desarrolladores deben garantizar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

Los desarrolladores deben garantizar que los controles de autenticación cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

Los desarrolladores deben garantizar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

Los desarrolladores deben garantizar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.

Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

El Ministerio de Educación Nacional declara como única documentación válida la ubicada en el aplicativo SIG, y entra en vigencia a partir de la publicación toda copia de este se declara COPIA NO CONTROLADA

Los desarrolladores deben garantizar que periódicamente se re-valida la autorización de los usuarios en los aplicativos y se asegura que sus privilegios no han sido modificados.

4.3.7. Acceso Computacional Móvil y Trabajo Remoto.

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones del MEN.

4.3.7.1. Uso de equipos Móviles y dispositivos de almacenamiento móvil.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles está restringido únicamente a los provistos por la institución y contemplan las siguientes directrices:

a) Uso de usuario y contraseña para acceso al mismo.
b) Cifrado de la información.
c) Uso de software antivirus provisto por el MEN.
d) Restricción de privilegios administrativos para los usuarios.
e) Uso de software licenciado y provisto por el MEN.
f) Realización de copias de seguridad periódicas.
g) Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
h) Adquisición de pólizas que cubran el hardware y la información de los dispositivos, contra perdida o hurto.
i) Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.

4.3.7.2. Trabajo Remoto

El trabajo remoto solo es autorizado por el responsable de la unidad organizativa de la cual dependa el colaborador que solicite el permiso. Dicha autorización solo se otorgará por la OTSI, una vez se verifique las condiciones de seguridad del ambiente de trabajo.

4.3.7.3. Conexiones remotas.

Utilizar la conexión de acceso remoto solo para acceder a servicios (File server, diferentes aplicativos, infraestructura entre otros) exclusivos del MEN los cuales sean inalcanzables desde redes externas.

La OTSI permitirá las conexiones remotas a los recursos de la plataforma tecnológica; únicamente a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

La OTSI suministrará las herramientas y controles necesarios para realizar conexiones de manera segura.

La OTSI debe monitorear las conexiones remotas a los recursos de la plataforma tecnológica del Ministerio de manera permanente.

4.3.7.4. Responsabilidades de los usuarios:
Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica del Ministerio y deben acatar las condiciones de uso establecidas para dichas conexiones.

Los usuarios únicamente deben establecer conexiones remotas a través de las VPN seguras y utilizar computadores previamente identificados y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

4.3.8. Monitoreo de los Accesos.
Se deben realizar labores periódicas de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad.

El Oficial de Seguridad de la Información realizará las revisiones periódicas para la verificación del cumplimiento de los lineamientos.

A tal efecto, se tendrán en cuenta los registros de eventos y de uso de los sistemas descritos a continuación.

4.3.8.1. Registro de eventos:
La OTSI contempla que el sistema de monitoreo debe suministrar como mínimo:

a) Intentos de acceso fallidos.
b) Bloqueos de cuenta.
c) Debilidad de contraseñas.
d) Cuentas inactivas y deshabilitadas.
e) Últimos accesos a cuentas. entre otros.

4.3.8.2. Registro de uso de los sistemas:
a) Accesos no autorizados.
b) Uso de Privilegios.
c) Alertas de sistema. Entre otros.

4.4. Uso y creación de contraseñas seguras
Los Colaboradores del MEN deben proteger sus contraseñas siguiendo las siguientes recomendaciones:

a) No escribir ni reflejar la contraseña en papel o documento donde quede constancia de esta.

b) No enviar nunca la contraseña por correo electrónico, redes sociales o en un SMS.
c) Las contraseñas que se generen en las diferentes aplicaciones deben viajar cifrada por la red.
d) No se debe facilitar ni mencionar la contraseña en conversaciones o comunicaciones de cualquier tipo.
e) No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
f) No escribir las contraseñas en equipos de computo de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
g) No compartir su contraseña con terceros. El uso de la contraseña es personal e intransferible.
h) No revelar su contraseña vía telefónica.
i) No utilizar la función "Recordar Contraseña " de programas de aplicación, como Internet Explorer, Correo Electrónico, o cualquier otro programa.
j) Informar cualquier incidente de seguridad que ponga en riesgo su contraseña a la OTSI por medio de la Mesa de Ayuda de Tecnología.
k) Informar a la OTSI por medio de la Mesa de Ayuda de Tecnología si alguien dentro o fuera de la entidad le solicita su contraseña.
l) No permita que le observen al escribir su contraseña.
m) Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.
n) Luego de 5 intentos de ingreso de contraseña fallidos, se bloqueará la cuenta de usuario y este deberá solicitar por medio de la Mesa de Ayuda de Tecnología el desbloqueo de esta.
o) Los computadores deben contar con protectores de pantalla protegidos por contraseña que deben ser habilitados dentro de los 5 minutos de inactividad del usuario.
p) Los sistemas de información del MEN bloquearan automáticamente las contraseñas de los usuarios que no hayan ingresado en los últimos sesenta (60) días.
q) Cuando un usuario inicie sesión por primera vez o cuando se realice una activación del usuario, el sistema exigirá cambio de contraseña. Las contraseñas generadas por primera vez deben estar alineadas a los requisitos y recomendaciones que a continuación se contemplan.

La OTSI ha definido una serie requisitos y recomendaciones en la creación y uso de las contraseñas:

a) No utilizar información personal en la contraseña: nombre del servidor o de sus familiares, ni sus apellidos, ni su fecha de nacimiento, ni cuentas bancarias, ni tarjetas de crédito, etc.
b) Se deben utilizar al mínimo 8 caracteres para crear la clave.
c) Las contraseñas deben utilizar la combinación aleatoria de los siguientes tipos de caracteres :

    a. Minúsculas
    b. Mayúsculas
    c. Números
    d. Caracteres especiales como +*! @ # $ & % ^ -/

d) Evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”).
e) No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
f) No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
g) Las contraseñas no deben ser FECHAS.
h) La contraseña no debe basarse en dos palabras separadas por un espacio ( ), guion (-) o guion bajo (_).
i) No se deberían asignar contraseñas en blanco. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).
j) No se deben utilizar palabras que se contengan en diccionarios en ningún idioma.
k) Cuando el sistema le solicite cambio de contraseña esta no debe haber sido utilizada en los históricos del sistema.
l) Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.
m) Realizar cambio de contraseña como mínimo cada 45 días.
n) Las contraseñas deberán tener histórico de 10 claves para que puedan ser repetidas.

4.5. Medios Removibles

La OTSI para un adecuado uso de los medios removibles, recomienda tener en cuenta los siguientes lineamientos:

a) El contenido de medios reutilizables que contengan información crítica o sensible del MEN que se van a retirar de las instalaciones, se les deberá realizar un borrado seguro. Para el retiro de dichos medios se debe contar con la autorización de la OTSI.
b) La información crítica o sensible del MEN cuya duración es mayor al tiempo de vida del medio en donde se encuentra almacenada, deberá respaldarse a través del proceso de gestión de copias de respaldo para evitar la pérdida de información.
c) El colaborador debe asegurar el resguardo de la información contenida en el medio removible que le fue asignado.
d) El colaborador debe dar buen uso a los medios removibles asignados, informando en forma oportuna cualquier deterioro.
e) Se debe de garantizar la integridad y disponibilidad de la información almacenada en medios removibles, cambiando de contenedor cuando culmine el tiempo de vida.
f) Es de exclusiva responsabilidad de cada funcionario tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles. Evitando accesos no autorizados, daños, pérdida de información o extravío del medio.
g) En caso de ocurrir perdida, modificación o daño de la información o del medio, se debe informar al Oficial de seguridad o quien haga sus veces.

4.5.1. Uso de Medios Removibles.

El uso seguro de medios de almacenamiento de información es responsabilidad de los colaboradores, los cuales deben contemplar las restricciones de no divulgar, no modificar y no retirar o destruir la información de manera no autorizada sobre los siguientes dispositivos:

a. Memorias tipo USB,

b. Discos duros,
c. CD-ROM, DVD,
d. Cintas.
e. Tarjetas de memorias de impresoras.

4.5.2. Eliminación de Medios Removibles

Para la eliminación de la información resguardada en los medios removibles se hará de forma segura, garantizando que se elimine toda la información de manera total.

Los medios que contengan información sensible o confidencial se eliminarán mediante técnicas de borrado seguro de datos, dejando registro de las acciones realizadas durante el proceso de eliminación, para facilitar la trazabilidad de eventos.

4.6. Seguridad

4.6.1. Antivirus

4.6.1.1. Colaboradores del MEN

f. Los funcionarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
g. Los funcionarios deben garantizar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
h. Los funcionarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda de Tecnología, para que, a través de ella, La OTSItome las medidas de control correspondientes.
i. Realizar copias de la información reservada del MEN, mediante el uso de los puertos de los computadores, a cualquier dispositivo de almacenamiento externo (CD's, DVD's, discos duros externos, memorias USB, etc.).
j. A generar contraseñas robustas para las Bases de Datos, Red y Sistemas de Información.
k. A utilizar las herramientas, procedimientos, formatos entre otros, para la implementación de un sistema de autenticación de acceso a los usuarios internos y externos en las diferentes plataformas tecnológicas
l. A utilizar la Mesa de ayuda de Tecnología para el restablecimiento de privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información del Ministerio.
m. Velar porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y garantizará que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.
n. A utilizar las herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software

malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica del Ministerio y los servicios que se ejecutan en la misma.

o. A permitir las actualizaciones de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica del MEN.
p. A solicitar borrado seguro del contenido de medios reutilizables que contengan información reservada del MEN que se van a retirar de las instalaciones.
q. A realizar copias periódicas de la información correspondiente a sus funciones dentro del MEN, que contengan sus equipos de cómputo, apoyándose con la Mesa de Ayuda de Tecnología.
r. Comunicar por medio de la Mesa de Ayuda de Tecnología cualquier caso de vulnerabilidad dentro de los sistemas de información del MEN.

4.6.2. Red

a. Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro del MEN entre los Colaboradores, departamentos, oficinas y hacia afuera a través de conexiones con otras redes o otras entidades de orden territorial.
b. La OTSI no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el Colaborador que los genere o solicite.
c. Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
d. No se permite el uso de los servicios de la red cuando no cumplan con las labores propias dentro del MEN.
e. Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad del MEN y se usarán exclusivamente para actividades relacionadas con la labor asignada.
f. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
g. La OTSI es el único que cuenta con permisos para el uso de analizadores de red los cuales son usados para monitorear la funcionalidad de las redes.
h. No se permitirá el uso de analizadores para monitorear o censar redes ajenas a el MEN y no se deberán realizar análisis de la Red desde equipos externos a la entidad.
i. Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al Colaborador o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

4.6.3. Servidores

4.6.3.1. Configuración e instalación

a. La OTSI tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

b. La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de la OTSI por medio del Operador de servicios TICs.
c. Durante la configuración de los servidores la OTSI deben garantizar que las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios sean aplicadas.
d. Los servidores que proporcionen servicios a través de la red e Internet deberán:
    a. Funcionar 24 horas del día los 365 días del año.
    b. Recibir mantenimiento preventivo mínimo dos veces al año
    c. Recibir mantenimiento semestral que incluya depuración de logs.
    d. Recibir mantenimiento anual que incluya la revisión de su configuración.
    e. Ser monitoreados por el Operador de Servicios TICs.
e. La información de los servidores deberá ser respaldada de acuerdo con politicas establecidas por la OTSI.
f. Los servicios hacia Internet sólo podrán proveerse a través de los servidores autorizados por la OTSI.

4.6.4. Seguridad Perimetral

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

a) La OTSI implementará soluciones lógicas y físicas que garanticen la protección de la información del MEN de posibles ataques internos o externos.
b) Rechazar conexiones a servicios comprometidos.
c) Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
d) Proporcionar un único punto de interconexión con el exterior.
e) Redirigir el tráfico entrante a los dispositivos de seguridad con que cuenta el MEN.
f) Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
g) Auditar el tráfico entre el exterior y el interior.
h) Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

4.6.5. Sistemas de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

a) La OTSI implementará soluciones lógicas o físicas que impidan el acceso no autorizado a la red del MEN.
b) Detección de ataques en el momento que están ocurriendo o poco después.
c) Automatización de la búsqueda de nuevos patrones de ataque, con herramientas estadísticas de búsqueda y al análisis de tráfico anómalo.
d) Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.
e) Auditoría de configuraciones y vulnerabilidades de los sistemas de IDS.

f) Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.
g) Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto.
h) Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos.
i) La Red del MEN sólo podrá acceder a los parámetros que el Firewall tenga permitido o posibilite mediante su configuración.

4.6.6. Redes Privadas Virtuales (VPN)

Los usuarios móviles y remotos del MEN podrán tener acceso al a red interna privada cuando se encuentren fuera de esta con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por la OTSI.

a) La OTSI será el encargado de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.
b) El Colaborador que solicite una VPN es responsable del acceso remoto y del uso de este.
c) Para que un Colaborador o proveedor del MEN pueda acceder a los equipos, ya sean servidores u otros equipos de la red interna del MEN desde una conexión externa con la tecnología VPN, cumplirá con el siguiente procedimiento:
    a. El Colaborador o proveedor solicitará por medio del Formulario de Creación VPN el acceso remoto mediante al servicio.
    b. La solicitud debe ser realizada por medio de la Mesa de Ayuda de Tecnología la cual deberá incluir el formato con la justificación para la solicitud de este acceso e indicará el tiempo requerido para el mismo, la información completa de la conexión y la información del aprobador de la solicitud. Esto aplica a todos los colaboradores y proveedores que tiene que realizar tareas fuera de horas laborables o en instalaciones que necesiten este tipo de acceso, participar en proyectos que requieran apoyo remoto, o alguna otra circunstancia especial que así lo amerite.
    c. La OTSI evaluará la solicitud; si aprueba la misma, se procederá a otorgar los permisos y acceso a la VPN. De no aprobar la misma, se devuelve al colaborador o proveedor solicitante con las razones de la decisión.
    d. Una vez procesado el permiso, se notifica al Colaborador o proveedor y se le dan las instrucciones para conectarse vía VPN. Si es necesario, personal técnico asistirá al usuario en el proceso de configurar el VPN.

4.6.7. Seguridad física y Ambiental en centros de Computo y de cableado

a) Las instalaciones con fines específicos que alberguen equipos de procesamiento, almacenamiento, conectividad, seguridad críticos requieren una mayor protección que la proporcionada a las instalaciones comunes. Debe considerarse a todas las funciones de IT y al material relacionado como confidencial y protegerlos de manera acorde. Esto se debe coordinar con el área encarda de la seguridad perimetral de los centros de computo.
b) El acceso a los centros de computo y centros de cableado es restringido y solo el personal por la OTSI puede tener acceso a estos.

c) Solo el personal autorizado por el operador de servicios TICs cuenta con el acceso a los gabinetes (racks) donde se encuentre alojada infraestructura de procesamiento, almacenamiento, networking y seguridad. Si alguna área requiere el acceso a estos gabinetes (rack) se debe solicitar por medio de la Mesa de Ayuda de Tecnología este acceso el cual será analizado por la OTSI.
d) Garantizar el monitoreo y diligenciamiento de la bitácora para los accesos otorgados a los centros de computo (CAN y Externo) previa autorización del responsable del MEN, al personal de soporte técnico, proveedores, operador de servicios TICs, colaboradores, etc.
e) No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la entidad, a menos que esté autorizado.

4.7. Vulnerabilidades

4.7.1. Objetivos Específicos

a) Identificación y evaluación de los sistemas y redes críticas del MEN.
b) Incremento en el conocimiento sobre información de seguridad para su administración.
c) Recomendaciones para reducir las vulnerabilidades de los sistemas y para proteger sistemas, información y redes críticas.
d) Identificación de los puntos vulnerables.
e) Informes o resultados estadísticos del escaneo de vulnerabilidades.
f) Implementación de planes de remediación para mitigar posibles riesgos tecnológicos producto del escaneo de vulnerabilidades.
g) Seguimiento y/o monitoreo periódico para la identificación y mitigación de vulnerabilidades técnicas.

4.7.2. Gestión de Vulnerabilidades.

4.7.2.1. Pre requisito para la evaluación de vulnerabilidades.

a) Contar con el inventario actualizado de sistemas de información, Bases de datos e infraestructura instaladas en el MEN.
b) Disponer de fuentes de información técnica que informen sobre las vulnerabilidades descubiertas.
c) Contar con el Comité de Gestión de Vulnerabilidades.

4.7.3. Caracterización de Gestión de Vulnerabilidades:

4.7.3.1. Fases de Gestión de Vulnerabilidades:

4.7.3.1.1. Fase de Identificación de la Vulnerabilidad.

Para la identificación, caracterización y tratamiento de la vulnerabilidad la OTSI, define los siguientes métodos:

a. Método de Ponderación de las Fuentes que son Vulnerables.

El método de ponderación a las fuentes que son vulnerables en el MEN se encuentra definidos en la siguiente matriz de ponderación de las fuentes de vulnerabilidad.

FUENTES	PUNTUACIÓN (CVSS)
CATEGORIA I	15
CATEGORIA II	10
CATEGORIA III	5
SERVIDORES	15
EQUIPOS PERIMETRALES	15
NETWORKING	10
ESTACIONES DE TRABAJO	5

Matriz de ponderación de las fuentes de vulnerabilidad.

b. Método para caracterizar el grado del Riesgo de la Vulnerabilidad.

El método de caracterizar el grado del Riesgo de las fuentes que son vulnerables en el MEN se encuentra definidos en la siguiente matriz de caracterización del grado del Riesgo de la Vulnerabilidad de las fuentes de vulnerabilidad.

Puntaje	Rango del Riesgo	Descripción
20	Critico	Estas vulnerabilidades incluyen riesgo que podrían comprometer los equipos e inclusive interrumpir el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.
15	Alto	Estas vulnerabilidades incluyen riesgo que podrían comprometer los equipos con degradación en el servicio de las aplicaciones Categoría I, Categoría II y Categoría III
10	Medio	Estas vulnerabilidades incluyen riesgo que podrían comprometer los equipos e inclusive interrumpir el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.
5	Bajo	Estas vulnerabilidades incluyen riesgo que podrían comprometer los equipos e inclusive interrumpir el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.

Matriz de caracterizar el grado del Riesgo de la Vulnerabilidad de las fuentes de vulnerabilidad

c. Método para caracterizar de la Criticidad de las Fuentes de Vulnerabilidad.

El método de caracterizar la criticidad a las fuentes que son vulnerables en el MEN, se encuentra definidos en la siguiente matriz de caracterizar el grado del Riesgo de la Vulnerabilidad de las fuentes de vulnerabilidad.

		FUNTES						
		CATEGORIA I	CATEGORIA II	CATEGORIA III	SERVIDORES	EQUIPOS PERIMETRALES	NETWORKING	ESTACIONES DE TRABAJO
CRITICIDAD	CRITICA	X			X	X		
	ALTA		X				X	
	MEDIA			X				
	BAJA							X

Matriz de caracterizar de la criticidad de las fuentes de vulnerabilidad

4.7.3.2. Administración de las Vulnerabilidades.

4.7.3.2.1. Asignación de Vulnerabilidades.

La administración de las vulnerabilidades después de haberse realizado una depuración, e identificada la fuente vulnerable, esta información es enviada los responsables de cada área, como se especifica en la siguiente matriz.

FUNTES						
CATEGORIA I	**CATEGORIA II**	**CATEGORIA III**	**SERVIDORES**	**EQUIPOS PERIMETRALES**	**NETWORKING**	**ESTACIONES DE TRABAJO**
APLICACIONES	APLICACIONES	APLICACIONES	INFRAESTRUCTURA	INFRAESTRUCTURA	INFRAESTRUCTURA	INFRAESTRUCTURA

Matriz de asignación de vulnerabilidad

4.7.3.3. Remediación.

4.7.3.3.1. Priorización atención de Vulnerabilidad.

La priorización de la atención de las vulnerables en el MEN se encuentra definidos en la siguiente matriz.

		FUNTES						
		CATEGORIA I	CATEGORIA II	CATEGORIA III	SERVIDORES	EQUIPOS PERIMETRALES	NETWORKING	ESTACIONES DE TRABAJO
CRITICIDAD	CRITICA	INMEDIATA			INMEDIATA	INMEDIATA		
	ALTA		4 HORAS				4 HORAS	
	MEDIA			8 HORAS				
	BAJA							24 HORAS

Matriz de Priorización atención de vulnerabilidad de las fuentes de vulnerabilidad

4.7.3.3.2. Tratamiento de la Vulnerabilidad.

El tratamiento de las Vulnerabilidades identificadas será determinado en el Comité de Gestión de Vulnerabilidades en donde se analizara si se:

i. Mitiga la Vulnerabilidad.
ii. Transfiere la Vulnerabilidad.
iii. Acepta la Vulnerabilidad.
iv. Evita la vulnerabilidad.

Pre requisitos para determinar el tratamiento.

v. Identificar las acciones.
vi. Recursos.
vii. Responsabilidades.
viii. Prioridades en la gestión de riesgos de seguridad de la información.

4.7.3.3.3. Priorización atención de la Remediación de la Vulnerabilidad

La priorización de la atención de la remediación de las vulnerables en el MEN se encuentra definidos en la siguiente matriz

		FUNTES						
		CATEGORIA I	CATEGORIA II	CATEGORIA III	SERVIDORES	EQUIPOS PERIMETRALES	NETWORKING	ESTACIONES DE TRABAJO
CRITICIDAD	CRITICA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA
	ALTA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA
	MEDIA	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ
	BAJA	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ

Matriz de Priorización atención de la remediación de la vulnerabilidad

4.7.3.4. Actividades de Gestión de Vulnerabilidades.

Las actividades contempladas para gestión de Vulnerabilidades se detallan en la siguiente matriz:

Fase	Actividades	Fuentes
Identificar vulnerabilidades	Identificación del grado de riesgo que representa la vulnerabilidad / evento identificado. Las alertas son recibidas desde fuentes externas y herramientas internas. Las alertas son revisadas y son ponderadas según su potencial riesgo. Se utilizan herramientas para el seguimiento de vulnerabilidades.	Escaneos (de infraestructura y de aplicación). Pentesting. Auditorías o revisiones de seguridad (tanto técnicas como no técnicas). Notificaciones de terceros. Reporte de Logs.

Administración de la vulnerabilidad:	Asignar un nivel de riesgo a la vulnerabilidad o evento en base al impacto que podría tener sobre el MEN. Identificar los sistemas y equipos afectados. Asignar la revisión de la vulnerabilidad o evento al responsable de la aplicación / plataforma / dispositivo.	Valor CVSS Inventario de activos del Ministerio. Constancia de que la vulnerabilidad está siendo activamente explotada en la propia compañía o en otras compañías.
Fase de Aplicación o Remediación:	Evaluación del Comité de Gestión de Vulnerabilidades. Determinar el procedimiento a seguir en base al nivel de riesgo detectado. Deshabilitar los equipos y sistemas expuestos en caso de ser necesario. Determinar el tipo de solución necesaria. Probar solución. Implementación de la solución en los equipos productivos. Reportar la remediación de los sistemas a “Cumplimiento”. .	Acta de reunión del comité de gestión de vulnerabilidades. Plan de remediación de las vulnerabilidades.
Reporte	Documentar cualquier lección aprendida en el proceso de resolución de esta vulnerabilidad con el objetivo de que futuras vulnerabilidades que guarden alguna semejanza con ésta puedan ser resueltas de manera más eficiente.	KMDB para mesa de ayuda y área de seguridad.

Cumplimiento	Una vez resuelta una vulnerabilidad, debe verificarse que su resolución ha sido eficaz y la vulnerabilidad ha sido realmente eliminada según lo esperado	Comité de gestión de Vulnerabilidades
Gestión de seguimiento vulnerabilidades tratadas en Comité de Vulnerabilidades	Realizar un análisis de la efectividad de las acciones propuestas para la mitigación de vulnerabilidades.	Actas de Comité de gestión de Vulnerabilidades

4.8. Gestión de LOGs

Aplica para toda la plataforma tecnológica que cuente con Sistemas operativos, o Dispositivos de red o dispositivos de seguridad del MEN (MEN) como:

a) Equipos de seguridad perimetral (Firewall, balanceadores, IPS entre otros).
b) Equipos Servidores.
c) Equipos de Networking.
d) Aplicaciones.
e) Equipos de Control de Acceso.

4.8.1. Responsabilidades.

La OTSI para la gestión de Logs define los siguientes roles**:**

Rol	Cargo	Responsabilidades
Responsable de Seguridad de la Información	Oficial de Seguridad de la Información	Vigilar que se cumplan las directrices emitidas en estos lineamientos para conservar el nivel de confidencialidad de la información y actualizar este documento de acuerdo con las necesidades del negocio.
Responsable de T.I.	Coordinador de Infraestructura TI	Es el responsable administrativo por la contención, y gestión de los eventos de seguridad. Debe enterarse, en primera instancia, de las actividades inusuales, o consecuencias de una irrupción no autorizada. El encargado de seguridad analiza y coordina la recolección de evidencia respecto de los incidentes, cuidando en todo momento, que dicha recolección responda a los estándares requeridos en procesos de peritaje forense respecto de la manipulación, mecanismos de obtención y retención de la evidencia. Es el encargado de mantener un registro de los eventos ocurridos, y gestionar los KPI relacionados
Administrador de Plataforma Tecnológica	Operador de servicio TICs	Monitorea plataforma, revisa y extrae información de logs. Realiza contención en los sistemas ante eventuales actividades, o consecuencias, asociadas al incidente.
Colaborador	Usuario de la Información	Realizar la validación de la calidad de los logs requeridos.

4.8.2. Generación de Logs

Fuente	Frecuencia de Generación (En días)	Priorización
Sistemas operativos (Servidores y equipos de red).		
1. Logs de Sistemas,	1	Baja
2. Logs de auditabilidad.	1	Media
3. Logs de Accesos de usuario.	1	Media
4. Logs de antivirus	1	Media
Dispositivos perimetrales (Firewall, balanceadores, IPS entre otros) y Aplicaciones de seguridad.		
1. Logs de servidor de autenticación	1	Alta
2. Logs de VPN+Firewall.	1	Alta
3. Logs Malware.	1	Alta
4. Logs de Accesos de usuario	1	Media
Aplicaciones.		
1. Logs de servidor de correos.	1	Alta

2. Logs de servidor WEB.	1	Alta
3. Logs de servidor de archivo.	1	Alta
4. Logs de servidor de bases de datos.	1	Alta
6. Logs de Accesos de usuario.	1	Media

Matriz de Priorización de Logs

4.8.3. Método de Priorización de Logs.

La OTSI para la fase de identificación contempla los siguientes métodos:

La ponderación para Priorización de Logs se realiza de acuerdo con la matriz descrita a continuación.

Generación (Fuente)	Puntuación
Sistemas operativos.	
Servidores	15
Equipos de red	10
Estaciones de trabajo	5
Dispositivos perimetrales.	
Firewall	20
Balanceadores	15
IPS y IDS	20
Aplicación	
CATEGORIA I	20
CATEGORIA II	10
CATEGORIA III	5

Matriz de Ponderación de Logs

Rango de Criticidad de Logs.

El rango de criticidad para los Logs está determinado por la ponderación y criticidad de los equipos que soportan las aplicaciones (ver matriz a continuación)

Puntaje	Rango de Criticidad	Descripción
15	Alto	Estos Logs son generados por dispositivos críticos como Firewall, Servidores y aplicaciones Misionales.
10	Medio	Estos Logs son generados por dispositivos no tan críticos como Equipos de red y aplicaciones No Misionales.
5	Bajo	Estos Logs son generados por dispositivos no críticos como estaciones de trabajo y aplicaciones No Misionales.

Matriz de Criticidad de Logs

4.8.4. Almacenamiento y Retención.

Se considera determinar los requerimientos de retención y almacenamiento para los Logs generados en un ambiente productivo, como se indica en la siguiente matriz.

FUENTE	Almacenamiento (Tamaño máximo)	Registro
1. Logs de Sistemas.	2 Gigas Diario	Locamente
2. Logs de auditabilidad.	2 Gigas Diario	Locamente
3. Logs de Accesos de usuario.	2 Gigas Diario	Locamente
4. Logs de Accesos inalámbricos.	2 Gigas Diario	Locamente
5. Logs de antivirus	1 Giga Diario	Locamente
1. Logs de servidor de autenticación	2 Gigas Diario	Locamente
2. Logs de VPN+Firewall.	2 Gigas Diario	Locamente
3. Malware.	2 Gigas Diario	Locamente
4. Logs de Accesos de usuario	2 Gigas Diario	Locamente
1. Logs de servidor de correos.	2 Gigas Diario	Locamente
2. Logs de servidor WEB.	2 Gigas Diario	Locamente
3. Logs de servidor de archivo.	2 Gigas Diario	Locamente
4. Logs de servidor de bases de datos.	2 Gigas Diario	Locamente
5. Logs de Accesos de usuario.	2 Gigas Diario	Locamente

Matriz de almacenamiento y retención de Logs

Nota: El tiempo de retención de los Logs es de 3 meses tiempo realizara una compresión de 100:1 es decir aproximadamente 1.8 Gigas y se llevara a un repositorio de información a través del proceso de copias de respaldo.

4.8.5. Frecuencia de Auditoria de LOGS.

La frecuencia de revisión y auditoria de los Logs para dispositivos y aplicaciones catalogados con riesgo alto, se realizará a través del Comité de Gestión de Vulnerabilidades o de acuerdo con la demanda por el área de aplicaciones o infraestructura.

4.9. Conectividad

La autorización de acceso a Internet se concede exclusivamente para actividades relevantes a las funciones desempeñadas. Todos los colaboradores del MEN tienen las mismas responsabilidades en cuanto al uso de Internet.

a) El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
b) No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

4.9.1. Acceso a Invitados:

a) La red inalámbrica (Invitados) es un servicio que permite conectarse única y exclusivamente a personal externo (clientes, proveedores, visitantes) a internet sin la necesidad de algún tipo de cableado. La Red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura del MEN.
b) Los usuarios invitados no tendrán acceso a la Red del MEN ni a ningún recurso de uso privado de la entidad.
c) La red inalámbrica es de tipo Portal Cautivo.

4.9.2. Red Inalámbrica (WIFI)

4.9.2.1. Acceso a colaboradores:

a. La red inalámbrica (MINISTERIO) es un servicio que permite conectarse a la red de la entidad e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de esta.
b. Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
c. Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Ipod, celulares, etc.) con capacidad de conexión Wireless.
d. La OTSI, es el encargado de la administración, habilitación y/o bajas de usuarios en la red inalámbrica dentro del MEN.
e. Para hacer uso de la red inalámbrica MINISTERIO, el solicitante necesariamente deberá estar dentro del dominio de la entidad y tener instalado el programa informático ISE.

4.10. Evaluación de los Riesgos de Seguridad Informática

Se podrán aplicar las técnicas de gestión de riesgos a todos los sistemas informáticos o a los servicios o componentes individuales de los sistemas, cuando sea posible y conveniente.

El proceso de evaluación de riesgos debe considerar:

a. La importancia de la información, del software y de otros activos del sistema informático en cuestión;
b. Las actividades del MEN, los productos y servicios respaldados por los sistemas informáticos en cuestión;
c. El daño que pueda causarse como consecuencia de una violación seria de la
d. seguridad de la información. Los impactos potenciales incluyen la pérdida financiera, el daño a la reputación de la entidad ante el estado colombiano y el público en general, la mala publicidad y el incumplimiento potencial de las funciones de la entidad.
e. d) La probabilidad real de que ocurra dicha violación, teniendo en cuenta los controles existentes y las amenazas imperantes, el entorno en el que se utiliza o funciona el sistema, y la vida útil real de la información en cuestión;
f. e) Los controles adicionales requeridos para reducir los riesgos a un nivel aceptable;

g. f) Las acciones necesarias para implementar y aplicar los controles adicionales
h. correspondientes. Si la Dirección considera que los riesgos identificados por esta
i. evaluación son inaceptables, y estos no se pueden evitar ni reducir
j. satisfactoriamente a través de métodos más efectivos, entonces se deben
k. planificar e implementar mejoras en la seguridad informática.

4.11. Gestión de Borrado Seguro.

4.11.1.1. Generalidades.

La Oficina de Tecnología de Sistemas de Información (OTSI) considera los siguientes requisitos mínimos antes de realizar un procedimiento de borrado seguro.

a. Acta de entrega equipo a Oficina de Tecnología de Sistemas de Información con formato de Activos fijos respectivo.
b. Hacer una copia de respaldo de la información del activo y ponerla a disposición del colaborador al cual pertenecía el equipo de cómputo previa autorización del jefe inmediato.
c. Realizar una validación de las licencias de software asignado al usuario del equipo a realizar el borrado seguro.

4.11.1.2. Método de Borrado seguro de la Información.

4.11.1.2.1. Formateo abajo nivel.

La OTSI considera el método de borrado seguro el formateo abajo nivel con el formateo de las unidades de almacenamiento que a continuación se listan.

Soporte	Tipo
Discos Duros	Magnético
Pen Drive (USB)	Electrónico

Una vez cumplido el tiempo de retención de las cintas de backup se puede realizar el borrado seguro de estas realizándola con las herramientas que cuente el Operador de Servicios TICs, garantizando la correcta eliminación de la información que allí se encontraba.

4.11.1.3. Herramienta para el Formateo abajo nivel.

Todo activo informático que cumpla su ciclo de vida y sea asignado para donación, destrucción o que sea reasignado, se debe garantizar el backup total de la información, sistemas operativos, configuraciones, etc., y este ser almacenado para proceder con el borrado seguro a bajo nivel con las herramientas licenciadas que cuente el Operador de Servicios TICs

4.11.1.4. Tratamiento de eliminación de las licencias de Software.

El tratamiento para eliminación de las licencias de software en la gestión de borrado seguro de los equipos pertenecientes del MEN se realizará en el caso que el equipo se de baja.

4.11.1.5. Paso a Paso para el Borrado Seguro.

DESCRIPCIÓN	RESPONSABLE	REGISTROS
1. Solicitud y justificación del borrado del disco duro.	Área implicada	Formato de solicitud
2. Autorización del Jefe del Área.	Jefe del Área	Aprobación por la herramienta o correo
3. Analizar la solicitud del borrado del disco duro.	Técnico de Infraestructura	No aplica
4. Con la herramienta designada, efectuar borrado seguro del DD.	Técnico de Infraestructura	Aplicativo asignado por la OTSI
5. Velar por que las actividades de copia de respaldo y borrado programado se ejecute en el equipo.	Técnico de Infraestructura	Formato o acta
6. Informar de la liberación de licencias de Software.	Técnico de Infraestructura	Formato o acta
7. Efectuar una revisión de la conformidad de actividades del mantenimiento ejecutado.	Técnico de Infraestructura Personal a Cargo de las funciones	Aplicativo asignado por la OTSI
8. Anexar imagen del Log del borrado del DD	Personal a Cargo de las funciones	Archivo de Imagen
9. Entrega de equipo para disponibilidad de la operación o inactivación del dispositivo.	Personal a Cargo de las funciones	Formato o acta
10. Almacenar la documentación en un recurso de red.	Líder de Infraestructura Personal a Cargo de las funciones	Carpeta en la red

La OTSI establece que el lineamiento de borrado seguro aplica sobre todos los equipos de propiedad y de alquiler del Ministerio.

La OTSI se encargará de controlar cualquier operación realizada sobre un dispositivo: mantenimiento, reparación, sustitución, para evitar fugas de información.

Toda solicitud de borrado seguro a los activos de información del se debe realizar a través de la Mesa de Ayuda de Tecnología. Esta solicitud debe quedar documentada y evidenciada donde conste que se realizó el proceso de revisión y copia de respaldo del equipo.

5. RESPONSABLES

- Jefe de la OTSI

- Coordinador de Infraestructura
- Coordinador de Aplicaciones
- Coordinador de Servicios TIC
- Colaboradores del MEN

6. DEFINICIONES

Colaboradores: (funcionarios, contratistas y/o terceros) de todas las áreas y procesos del MEN 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.
Activos de información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.
Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales suministradas por el MEN.
Activos físicos: Se consideran activos físicos elementos tales como: Computadores, portátiles, módems, impresoras, Equipos de Comunicaciones, PBX, cintas, discos, UPS, etc.
OTSI: Oficina de Tecnología y Sistemas de Información del Ministerio de Educación Nacional.
Seguridad de la información: Se entiende como la preservación de las siguientes características:
Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Adicionalmente, deberán considerarse los conceptos de:
Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
Audibilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
Legalidad: Se refiere al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Ministerio.
Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
Tecnología de la Información: Se refiere al hardware y software operados por el Ministerio o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Ministerio, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
Vulnerabilidad: Debilidad en un sistema, permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.
Analizador de Vulnerabilidades: Herramienta que analiza todos los activos conectados a la red verificando posibles vulnerabilidades y catalogándolas según los estándares internacionales, según los puertos abiertos y configuraciones de los dispositivos hallados.
Comité de Vulnerabilidades: Grupo interdisciplinario conformado por personal de Infraestructura, Aplicaciones, Oficial de Seguridad de la Información, Oficial de Seguridad Informática del Operador de la Red del MEN y el Oficial de Seguridad Informática de la Interventoría. Este Comité se encargará de verificar el correcto desarrollo de las pruebas de vulnerabilidades técnicas, así como implementar planes de acción para mitigar las vulnerabilidades encontradas.
Escaneo de vulnerabilidades: Es una actividad que a través de aplicaciones permite realizar una verificación de seguridad en una red mediante el análisis de los puertos abiertos en toda la red que permite identificar los riesgos de seguridad. Además, identifica las debilidades de un sistema operativo o de software de aplicación.
Falso Positivo: Es un error por el cual un software de análisis de vulnerabilidades reporta que un sistema, aplicación o bases de datos presenta una falla de seguridad, cuando en realidad esta no existe.
Infraestructura Tecnológica (IT): Es el conjunto de hardware y software, que se implementa conformando una plataforma para el funcionamiento de las actividades de una organización u empresa.
MEN: Ministerio de educación Nacional.

7. EXCEPCIONES

No hay excepciones en el lineamiento definido.

8. REFERENCIAS A OTRAS POLÍTICAS, LINEAMIENTOS Y NORMAS EN LAS CUALES SE SOPORTA O TIENE RELACIÓN

- Norma ISO 27001
- Mejores prácticas Cobit, Togaf
- Decretos 5012 del 2009 y 854 del 2011
- Resolución 12646 de octubre del 2012
- Lineamientos del gobierno en línea.

3. Control de cambios		
versión	**Fecha de entrada en vigencia**	**Naturaleza del cambio**
01	30-05-2018	Se crea el manual.
02	El documento entra en vigencia a partir de su actualización en el SIG	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

4. Ruta de aprobación					
Elaboró		Revisó		Aprobó	
Nombre	Luis Carlos Serrano Pinzón	**Nombre**	Alejandro Parra Yuli Andrea Parra	**Nombre**	Hernán Guiovanni Ríos Linares
Cargo	Seguridad Informática	**Cargo**	Asesor OTSI	**Cargo**	Jefe de Tecnologías de la Información

El Ministerio de Educación Nacional declara como única documentación válida la ubicada en el aplicativo SIG, y entra en vigencia a partir de la publicación toda copia de este se declara COPIA NO CONTROLADA