CONTENIDO

INTRODUCCIÓN

Las políticas establecidas e incluidas en este documento son un componente fundamental para la gestión en seguridad y privacidad de la información del Ministerio de Comercio, Industria y Turismo, en adelante MinCIT, y se convierten en la base para la implementación de los procedimientos, los estándares y controles para la seguridad y privacidad de información.

Este documento es confidencial y de propiedad del MinCIT.

Las actualizaciones se publicarán internamente en el Sistema Integrado de Gestión (en adelante SIG).

Las políticas de seguridad y privacidad de la Información deberán ser conocidas, aceptadas y cumplidas por todos los funcionarios, pasantes, contratistas, proveedores, Entidades del Sector Comercio, Industria y Turismo, Entidades públicas y privadas, y demás partes interesadas del MINCIT que tengan interacción con la plataforma tecnológica y sistemas de Información.

En caso de incumplimiento en lo establecido en esta política por parte del personal de planta, se comunicará al área correspondiente para que esta proceda conforme a los lineamientos de la Ley 734 de 2002 –Código Disciplinario Único.

El incumplimiento de las mismas, por parte del personal contratista o proveedor se convertirá en una causal para determinar la terminación del contrato o convenio, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

Para reportar un evento sospechoso o un incidente de seguridad o de privacidad de la información, el Ministerio ha dispuesto como canal de contacto el correo electrónico soportetecnico@mincit.gov.co.

1. MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.1. OBJETIVO

Establecer y divulgar las Políticas de Seguridad y Privacidad de la Información del Ministerio de Comercio, Industria y Turismo a funcionarios, pasantes y contratistas, proveedores incluyendo personal suministrado por terceros que provean servicios al MinCIT, Entidades del Sector Comercio, Industria y Turismo, Entidades públicas y privadas y demás partes interesadas, esto con el fin de darlas a conocer para su respectivo cumplimiento.

1.2. ALCANCE

Las políticas de seguridad y privacidad de la información son aplicables para todos los aspectos administrativos, técnicos, tecnológicos y de control que deben ser cumplidas por directivos, funcionarios, contratistas, pasantes, proveedores, Entidades del Sector comercio, industria y turismo, Entidades públicas y privadas, ciudadanos y demás partes interesadas, que cumplan con alguna de las siguientes condiciones:

- Acceso a la información tanto física como lógica.
- Ingreso de manera física a las instalaciones o lógica a través de la plataforma tecnológica de la Entidad.

- Uso de equipos informáticos y de telecomunicaciones conectados a la plataforma tecnológica.
- Uso de los servicios informáticos dispuestos por la entidad a través de los canales digitales.
- Diseño, construcción, pruebas, implementación o uso de herramientas tecnológicas o servicios informáticos dispuestos por el la entidad para el desarrollo de sus funciones.

1.3. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN DEL MANUAL

La vigencia del Manual de Políticas de Seguridad y Privacidad de la Información aplica a partir de su aprobación por la Alta Dirección y publicación en el Proceso "Subsistema de Seguridad y Privacidad de la Información".

La revisión del contenido del Manual deberá realizar periódicamente; como mínimo una vez al año o cuando se presenten:

- Cambios organizacionales (estructura orgánica, objetivos estratégicos o metas institucionales).
- Cambios en el entorno operativo de los procesos institucionales.
- Cambios en el entorno tecnológico de la entidad.
- Cambios en el entorno público y de la gestión administrativa de las instituciones.
- Cambios en el marco normativo o regulatorio interno y el que emita el Gobierno Nacional en materia de tecnologías de la información y comunicación, y que le sean aplicables a la gestión del Ministerio.
- Cambios como resultado de la gestión de continuidad operativa de la institución.
- Y cualquier otro cambio que afecte o impacte en la seguridad y privacidad de la información del Ministerio.

La Oficina Asesora de Planeación Sectorial a través del Oficial de Seguridad de la Información o quien haga sus veces, realizará la actualización del Manual de políticas de seguridad y privacidad de la información.

1.4. TÉRMINOS Y DEFINICIONES

Se adoptan los términos y definiciones de la familia de normas técnica ISO 27000 vigentes, y de los estándares que se apliquen de acuerdo al alcance de las políticas.

2. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política general de seguridad y privacidad de la información del Ministerio de Comercio, Industria y Turismo establece el compromiso de la Entidad de proteger la información institucional, implementando los mecanismos y controles adecuados para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la misma, con el fin de mantener la continuidad de las operaciones del Ministerio.

Los mecanismos y controles implementados responden al alcance de las políticas específicas y su aplicación a nivel institucional.

2.1. ORGANIZACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1.1. Organización interna

El Decreto 210 de 2003 determina la Estructura Orgánica del Ministerio de Comercio, Industria y Turismo.

El Manual Especifico de Funciones y de Competencias Laborales determina los empleos que conforman la planta de personal, y establece las funciones esenciales, generales, especificas y comunes definidas para todos los empleos identificados, de acuerdo con el nivel jerárquico de decisión, así como la conformación de las áreas funcionales del Ministerio.

Para efectos de la coordinación de las actividades relacionadas con la gestión de la seguridad y privacidad de la información, se ha establecido el Comité Institucional de Gestión y Desempeño, que entre sus funciones se encuentra "asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información".

El Comité Institucional de Gestión y Desempeño está conformado por la Alta Dirección del Ministerio quienes son los responsables de la toma de decisiones en materia de seguridad y privacidad de la información.

Los Directores y Coordinadores de Grupos son responsables de los procesos institucionales y de la custodia de la información, el cumplimiento normativo sobre los datos, la actualización de los activos de información, la gestión de los riesgos asociados a los activos de información y las acciones de tratamiento pertinente.

La Oficina Asesora de Planeación Sectorial (OAPS), a través del Oficial de Seguridad o quien haga sus veces, es responsable de la gestión de la seguridad y privacidad de la información en la Entidad.

La Oficina de Sistemas de Información (OSI), es responsable del gobierno de las tecnologías de la información del Ministerio, de la seguridad informática, acceso a servicios de tecnologías de la información y aseguramiento de la infraestructura tecnológica.

2.1.2. Separación de deberes

La separación de deberes define los roles, responsabilidades y niveles de autoridad en la interacción de la seguridad y privacidad de la información, en concordancia con el Manual especifico de funciones y competencias laborales, sin perjuicio de lo anterior se establecen los siguientes lineamientos:

- El personal que realiza labores funcionales sobre sistemas de información, sean críticos o no, de la Entidad no pueden tener a su cargo labores de administración técnica. sobre la plataforma tecnológica (sistemas operativos, bases de datos, programas de aplicación, software de comunicaciones, entre otros) que soporten los sistemas de información.
- El personal técnico de la Oficina de Sistemas de Información (OSI) no debe tener decisión sobre los datos que se procesan en los sistemas de información de la entidad.
- El personal contratista y proveedor de servicios de tecnologías de información y comunicación, solo tendrá acceso a la plataforma tecnológica de la Entidad en el marco de su objeto contractual.

2.1.3. Contacto con las autoridades y con grupos de interés especial

El Equipo de Respuesta a Incidentes de seguridad y privacidad de la Información, debe mantener contacto con autoridades y grupos de interés especial, como son:

- ColCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
- CSIRT PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional.
- CCOC – Conjunto Comando Operativo Cibernético de las Fuerzas Militares de Colombia.
- CSIRT GOB MinTIC - Equipo de respuesta frente a Incidencias de seguridad informática del Ministerio de Tecnologías de la Información y las Comunicaciones.
- Grupo de protección de datos personales de la Superintendencia de Industria y Comercio.
- Partes interesadas internas.

Y, demás entes u organismos nacionales o internacionales que tengan relación con la gestión de la seguridad y privacidad de la información, así como también contacto con asociaciones profesionales que permitan la constante actualización del conocimiento en riesgos, ataques y medidas de mitigación.

2.1.4. Seguridad de la información en la gestión de proyectos de tecnologías de la información (TI)

Gestión de proyectos de TI

En concordancia con la metodología del Ministerio, la gestión de proyectos de TI, debe:

- Contar con el concepto técnico de la Oficina de Sistemas de Información (OSI).
- Incorporar los requisitos de seguridad y privacidad de la información.
- Evaluar los riesgos que puedan llegar a impactar la confidencialidad, privacidad, integridad y disponibilidad de la información de la Entidad.

Salida o transporte de Información sensible o crítica

La salida o transporte de información sensible o crítica deberá estar plenamente justificada y contar con la suscripción de un “Acuerdo de Confidencialidad”, que detalle el objeto de la salida de información, transporte y uso final.

2.1.5. Dispositivos móviles

De propiedad del Ministerio

Para los dispositivos móviles, tales como portátiles, tablets, celulares, entre otros, el Ministerio cuenta con:

- **Controles físicos**, para el uso de los dispositivos móviles por parte del personal del Ministerio. Son de aplicación los lineamientos y directrices definidos en los siguientes documentos:
  - Procedimiento GR-PR-001 Administración y control de bienes devolutivos y de consumo.
    - Documento GR-GU-001 Guía para el manejo administrativo de los bienes de propiedad de la Nación MinCIT.
  - Los numerales 2.6.3. Ingreso o retiro de activos y 2.6.4. Equipos fuera de las instalaciones del presente Manual.

- **Controles Lógicos**, se aplican:
  - Para el acceso a los servicios de TI por parte del personal, se aplica el numeral 2.4 Control de Accesos de este Manual.
  - Para la protección de la confidencialidad de la información mediante técnicas de backup.
  - En caso de requerirse, la Oficina de Sistemas de Información (OSI), implementará el proceso de cifrado de la información.

De propiedad del personal o terceros que labora para la Entidad y visitantes del Ministerio

Para los dispositivos móviles de propiedad de personal que labora para la Entidad o del personal visitante en las instalaciones del Ministerio, se aplican:

- **Controles físicos**, relacionados en el numeral 2.6.3. Seguridad de Equipos de este Manual.
- **Controles Lógicos**, relacionados en el numeral 2.4 Control de Accesos de este manual, en lo que respecta al acceso a servicios de TI por parte de los visitantes.

2.1.6. Teletrabajo y trabajo remoto

El MinCIT establece las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Entidad; así mismo, suministra las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

Cualquier funcionario, contratista o proveedor del MinCIT, previamente autorizado por la Oficina de Sistemas de Información (OSI), que requiera tener acceso a la información de la Entidad desde redes externas, debe acceder remotamente mediante un proceso de autenticación y autorización de dirección IP pública; haciendo uso de conexiones seguras (https, VPN).

Teletrabajo

La Oficina de Sistemas de Información (OSI) implementa los controles de seguridad informática necesarios para establecer la conexión remota con los servicios de TI del Ministerio por parte de los funcionarios en modalidad de teletrabajo, de acuerdo con los lineamientos que sobre el tema adopte el Ministerio y coordinados con el Grupo de Talento Humano de la Secretaría General.

Responsabilidades:

La Oficina de Sistemas de Información realizará:

- El alistamiento de los equipos asignados por el Grupo Administrativa al Funcionario en la modalidad de teletrabajo.
- La asignación de credenciales para el acceso a los sistemas de información requeridos por el teletrabajador.
- En caso de requerirse acceso a un servicio TI especifico, se asignará una VPN (Vitual Path Network).

El Funcionario en la modalidad de teletrabajo, debe:

- Hacer uso adecuado y exclusivo de los recursos tecnológicos asignados (computador, tablet, portátil u otros) para el cumplimiento de las funciones asignadas.
- Asegurarse de mantener la debida integridad, confidencialidad y disponibilidad de la información, así como de la privacidad de los datos personales objeto del desarrollo de sus funciones.
- Presentar los recursos tecnológicos asignados para los mantenimientos preventivos programados por la Oficina de Sistemas de Información.
- Reportar a través de la Mesa de Ayuda cualquier evento relacionado con la funcionalidad de los recursos tecnológicos asignados.
- Abstenerse de instalar software o programas ejecutables en los equipos asignados sin previa autorización de la Oficina de Sistemas de Información, quien verificará la necesidad y las implicaciones de seguridad de su instalación.

Trabajo con Acceso Remoto

En los casos en que se precise la realización de trabajo con acceso remoto por parte de funcionarios o personal contratista o proveedor, se debe informar a la Oficina de Sistemas de Información, para que habilite el acceso a los servicios de TI requeridos, previa autorización del Jefe del área del funcionario o del Supervisor del contratista o proveedor.

2.2. SEGURIDAD DEL RECURSO HUMANO

En lo que corresponde a la gestión del personal de planta del Ministerio, el Grupo de Talento Humano aplica los lineamientos normativos y regulatorios vigentes.

En lo que respecta al personal contratista o proveedor el Grupo de Contratos en coordinación con las áreas que tiene bajo su cargo la función de supervisión, aplica los lineamientos normativos y legales para la contratación del personal requeridos de acuerdo con las necesidades institucionales.

El personal del Ministerio sin importar su tipo de vinculación es responsable de la custodia y uso adecuado de los activos asignados en los que se incluyen: equipos, datos e información y aplicativos, entre otros.

Para todos los efectos, el personal del Ministerio deberá acoger las disposiciones de seguridad y privacidad de la información establecidas en este Manual.

2.2.1. Responsabilidad del personal

Todos los funcionarios, pasantes, contratistas y proveedores, así como las partes interesadas autorizados por el Ministerio para acceder a la plataforma tecnológica y de comunicaciones, sistemas de información o aplicativos, hardware de red y software operativo, de programación, entre otros, son responsables del cumplimiento de las políticas, directrices, procedimientos, estándares y controles de seguridad informática y de la seguridad y privacidad de la información definidas por la Entidad.

La información almacenada en los equipos de cómputo (servidores, computadores, portátiles, dispositivos móviles y demás dispositivos de procesamiento y almacenamiento) de la Entidad es propiedad del Ministerio y cada usuario es responsable de proteger su confidencialidad, privacidad, integridad y disponibilidad.

2.2.2. Procesos disciplinarios

En caso de incumplimiento en lo establecido en esta política por parte del personal de planta, se comunicará al área correspondiente para que esta proceda conforme a los lineamientos de la gestión disciplinaria del Ministerio.

El incumplimiento de esta política por parte del personal contratista o proveedor, se convertirá en una causal para determinar la terminación del contrato o convenio, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

2.2.3. Terminación o cambio del tipo de vinculación laboral

Todo personal del Ministerio al momento de su retiro de la entidad, cambio de cargo o de área es responsable de entregar al Jefe inmediato o Supervisor del contrato los activos de información que se originen en desarrollo de sus funciones o actividad contratada.

El Grupo de Talento Humano informa a las áreas responsables de gestionar los activos de la Entidad, sobre el retiro, cambio de cargo o de área de los funcionarios, a fin de:

- Inhabilitar o inactivar, según sea el caso, los usuarios y contraseñas asignados para acceder a los servicios de TI de manera inmediata.
- Inhabilitar o inactivar de manera temporal o permanente, según sea el caso, el carné de ingreso a las instalaciones físicas del Ministerio.

El Grupo de Contratos informa las áreas responsables de gestionar la suspensión, cesión o terminación del contrato, a fin de :

- Inhabilitar o inactivar, según sea el caso, los usuarios y contraseñas asignados para acceder a los servicios de TI de manera inmediata.
- Inhabilitar o inactivar de manera temporal o permanente, según sea el caso, el carné de ingreso físico a las instalaciones del Ministerio.

Los Jefes de área, partiendo de la Alta Dirección a través de los diferentes niveles jerárquicos, así como los supervisiores de contratos deberán:

- Garantizar la copia de la información almacenada en los equipos (computador, portátil o tablet) asignados al funcionario o contratista, antes de su retiro formal de la entidad.
- Garantizar la salvaguarda de la información física en condiciones de disponibilidad, integridad, privacidad y confiabilidad.

Los funcionarios y contratistas deben:

- Realizar la devolución de los activos de información atendiendo los lineamientos definidos en:
  - Procedimiento GR-PR-001 Administración y Control de Bienes Devolutivos y de Consumo
  - Documento GR-GU-001 Guía para el Manejo Administrativo de los Bienes de Propiedad de la Nación MinCIT.
  - Los numerales 2.6.3. Ingreso o retiro de activos y 2.6.4. Equipos fuera de las instalaciones del presente Manual.
- Devolver al Grupo Administrativa el carné que lo acredita como funcionario o contratista del Ministerio, para su disposición final.

2.3. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Se aplican los lineamientos definidos en el documento SG-GU-008 Guía para la Gestión de Activos de Información del Ministerio.

2.3.1. Inventario de activos de información

Todo el personal del Ministerio sin importar su tipo de vinculación, debe mantener actualizado el inventario de activos de Información, en particular cuando se presenten cambios significativos en:

- Los objetivos estratégicos, políticas, directrices, procesos (procedimientos, guías, formatos, controles y riesgos).
- La estructura organizacional.
- En la infraestructura de tecnologías de información y comunicación que afecten los procesos que soporta la Entidad.
- Las normas, regulaciones o estándares relacionados con la gestión de los activos de información.
- Cambios en el entorno que afecten la ejecución de los procesos.

Todos los activos de información identificados en el inventario de activos deben tener un propietario o responsable asociado.

2.3.2. Propiedad de los activos de información

Los propietarios de los activos de información en cualquiera de sus tipos y disposición física o digital son responsables de:

- Identificar, clasificar y actualizar los activos relacionados con sus respectivos procesos, de acuerdo con las disposiciones del numeral 2.3.1 Inventario de activos de información.
- Garantizar que se documenten los controles apropiados para guardar la confidencialidad, integridad, privacidad y disponibilidad de los activos de información y de sus sistemas de información.

2.3.3. Uso adecuado de los activos y recursos de información

Toda la información del Ministerio sin importar el tipo de soporte (físico o digital), debe ser procesada y almacenada de acuerdo con su nivel de clasificación, de manera que se protejan las propiedades de confidencialidad, privacidad, integridad y disponibilidad.

El personal de la Entidad independiente del tipo de vinculación, deberá cumplir los siguientes lineamientos:

- No realizar cambios en la configuración del hardware o software de los equipos (computadores, portátiles o tablets) asignados o delegados para el desarrollo de sus funciones o del objeto contractual.

- Solo las personas autorizadas por la Oficina de Sistemas de Información podrán revisar, instalar, configurar y dar soporte a los equipos de cómputo de propiedad del Ministerio.
- Cumplir con los controles determinados por la Entidad para el manejo y protección de la información.
- Cumplir con los lineamientos definidos en los numerales 2.6.4. Equipos fuera de las instalaciones, 2.6.5. Equipos de usuario desatendido, 2.6.6. Escritorio y pantalla limpia, del presente manual.

2.3.4. Devolución de activos

Aplica lo definido en el numeral 2.2.3. Terminación o cambio de la vinculación laboral de este manual.

2.3.5. Clasificación de la información

Toda información que esté bajo responsabilidad del Ministerio debe ser identificada, clasificada y documentada con base en la SG-GU-008 Guía para la Gestión de Activos de Información del Ministerio.

2.3.6. Etiquetado de la Información

Los activos de información del Ministerio deben ser etiquetados de acuerdo con los parámetros definidos en el documento SG-GU-008 Guía para la Gestión de Activos de Información del Ministerio.

2.3.7. Manejo de la información en medios físicos y electrónicos

El Ministerio como propietario y custodio de la información (física o electrónica), generada como resultado del cumplimiento de su misión y visión, y acogiéndose a la normatividad que le sea aplicable para efectos de la gestión documental institucional, se reserva el derecho de su conservación o destrucción, dependiendo del nivel de criticidad definida para la información con base en los lineamientos del Comité Interadministrativo de Gestión y Desempeño referente a la Gestión Documental, la normativa establecida por el Archivo General de la Nación y el documento SG-GU-008 Guía para la Gestión de Activos de Información.

Información en medios físicos

Para la información impresa o en medios físicos, con respecto a su acceso, uso, transporte, almacenamiento y disposición final, se aplican las directrices del Comité Interadministrativo de Gestión y Desempeño referente a la Gestión Documental, para lo cual se debe:

- Mantener actualizado el inventario de los equipos que están en funcionamiento, identificando el responsable y las características del equipo.
- El responsable del equipo se compromete a mantener y salvaguardar la información contenida en el mismo, para el efecto debe aplicar:
  - Los lineamientos de este manual relacionados con: 2.6.3. Ingreso o retiro de activos, 2.6.4. Equipos fuera de las instalaciones y 2.7.6 Copias de respaldo.
  - Los lineamientos del Proceso Gestión de Recursos Físicos definidos para la devolución de los equipos asignados, de acuerdo con el procedimiento GR-PR-001 Administración y Control de Bienes Devolutivos y de Consumo, y Documento GR-GU-001 Guía para el Manejo Administrativo de los Bienes de Propiedad de la Nación MinCIT.

Información en medios electrónicos

Para la información soportada en medios electrónicos de propiedad del Ministerio, se debe:

Mantener actualizado el inventario de activos de información que identifique los propietarios y usuarios , el nivel de custodia y la criticidad de los mismos.

Para la información clasificada con un nivel de criticidad "Alto" acorde con el documento SG-GU-008 Guía para la Gestión de Activos de Información, y en aplicación del derecho de conservación o destrucción el Ministerio aplicará las técnicas de borrado segura que se encuentren disponibles en al Oficina de Sistemas de Información.

Uso y manejo de medios removibles

- La información crítica o sensible de la entidad que se encuentra almacenada en un medio removible cuya vida útil es menor al tiempo de retención de la información establecida por el MinCIT, se respalda en otro medio para evitar la pérdida de información.
- Todo medio removible es escaneado por software antivirus cada vez que sea conectado a la red interna.
- Los funcionarios y contratistas pueden hacer uso de medios de almacenamiento externo (CD, DVD, pendrive, disco duro externo, cámaras, SD, smartphones, etc.) siendo éstos utilizados únicamente con el fin de facilitar el transporte de información, es responsabilidad de los usuarios mantener la información que están manipulando en los dispositivos
- Los medios removibles no son una alternativa de respaldo de información, siendo responsabilidad de los usuarios mantener la confidencialidad e integridad de la misma.
- En caso de requerirse almacenar información sensible en medios removibles, se realiza mediante herramientas de cifrado.

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.

2.3.8. Uso de internet, correo electrónico y recursos tecnológicos

El MinCIT, controla, verifica y monitorea el uso adecuado de los servicios de internet, correo electrónico, impresión y demás recursos tecnológicos.

La asignación de recursos como computador o portátil a funcionarios, pasantes y contratistas, los debe gestionar el Jefe Inmediato o Supervisor del contratista o proveedor, ante el Grupo Administrativa. La adecuación de estos recursos para la prestación del servicio la realiza la Oficina de Sistemas de Información.

Los funcionarios, pasantes, contratistas, proveedores o partes interesadas deben hacer uso adecuado de los mismos en razón de sus funciones o actividades. El uso de internet, correo electrónico y de otros recursos tecnológicos son considerados herramientas de trabajo esenciales para las labores diarias.

Autenticación de usuarios

La Oficina de Sistemas de Información asignará un nombre de usuario, una contraseña y una cuenta de correo electrónico a funcionarios, pasantes, contratistas o proveedores o partes interesadas, previa autorización de:

- El Grupo de Talento Humano, al ingreso del funcionario y pasante.
- El Grupo de Contratos para los contratistas o proveedores, indicando la fecha de inicio y fecha de terminación del contrato y actividad específica.

Cancelación de cuentas de correo electrónico y deshabilitación de usuarios

La Oficina de Sistemas de Información procederá a deshabilitar la cuenta de correo electrónico asignada a funcionarios, pasantes, contratistas o proveedores o partes interesadas, previa confirmación de desvinculación del personal, por parte del Grupo de Talento Humano o del Grupo de Contratos.

Correo electrónico

Consideraciones generales:

- La cuenta de correo electrónico asignada a funcionarios, pasantes, contratistas y proveedores o partes interesadas, únicamente podrá ser utilizada para finalidades relacionadas con el desarrollo de las funciones correspondientes al cargo o función, u obligaciones definidas en el respectivo contrato, quedando limitado el uso de dicha cuenta al ámbito laboral y profesional.
- Los usuarios no deben utilizar una cuenta de correo electrónico que pertenezca a otra persona. En caso de ausencia temporal o vacaciones o retiro, se debe recurrir a mecanismos alternos como redirección de mensajes.
- Cualquier correo electrónico sospechoso debe ser reportado a soportetecnico@mincit.gov.co.
- Los funcionarios o contratistas que tengan atribuida la gestión de cuentas de correo genéricas asociadas a determinados trámites no podrán en ningún caso hacer uso de ellas por motivos personales.
- Toda la información almacenada, gestionada o transmitida por correo electrónico de la Entidad, es propiedad del MinCIT.
- Cuando se realice el envío de información pública reservada o publica clasificada mediante correo electrónico, se aplican Acuerdos de Confidencialidad.
- El correo electrónico no debe ser utilizado para enviar ni recibir ni contestar mensajes o cadenas de mensajes que pudiesen causar congestión en la red de la Entidad, o que puedan introducir códigos maliciosos o materializar riesgos de seguridad y privacidad de la información.

Internet

Los sitios web de MinCIT están diseñados para publicar la información de la gestión institucional a la que hagan referencia, por lo tanto los funcionarios responsables de administrar o publicar contenidos en los sitios web, deberán cumplir con los requerimientos normativos y regulatorios relacionados con transparencia y acceso a la información; así mismo, no podrán publicar información diferente a la específica del sitio web, ni información personal o de otra índole.

Sin perjuicio de lo anterior, todos los usuarios que acceden a internet, tienen prohibido ingresar a los sitios presentados a continuación. El personal que requiera el acceso a este tipo de sitos como parte del desarrollo de las actividades misionales del MinCIT, deberá previamente justificar la necesidad y obtener la autorización formalizada por parte de su jefe inmediato o supervisor del contrato, la Oficina Asesora de Planeación Sectorial y la Oficina de Sistemas de Información.

- Acceso a sitios web relacionados con actividades de juego o apuestas;
- Acceso a sitios web de contenido para adultos relacionados con pornografía, pedofilia o erotismo.
- Acceso a sitios web de carácter discriminatorio, racista, o material potencialmente ofensivo, menosprecio o acoso explícito.
- Acceso a sitios relacionados a la afectación de la seguridad informática, los cuales puedan poner en riesgo la integridad y confidencialidad de la información del MinCIT.
- Acceso a sitios de descarga de material protegido bajo leyes de derecho de propiedad sin que se cuente con la autorización expresa o licencia de uso respectiva, o archivos electrónicos para usos no relacionados con la misionalidad del MinCIT.
- Acceso a sitios web que inciten a la participación en cualquier actividad ilegal o criminal.

2.4. CONTROL DE ACCESO

2.4.1. Política para el control de acceso

El MinCIT implementa los controles de acceso a la información por parte de funcionarios, pasantes, contratistas y proveedores o partes interesadas, conforme al perfil de acceso establecidos en los sistemas de información o bases de datos, así mismo garantiza la implementación de controles de seguridad física e informática para la protección de las instalaciones de procesamiento de información y cualquier otra área considerada crítica para la operación de la Entidad.

Usuarios

Los usuarios del MinCIT son todos los funcionarios, pasantes, contratistas, proveedores.

Usuarios de consulta

Entidades del Sector Comercio, Industria y Turismo, Entidades públicas y privadas, ciudadanos y demás partes interesadas, que estén relacionadas de forma temporal o permanente con la Entidad.

2.4.2. Acceso a redes y a servicios de red

El acceso a la red de datos del MinCIT se realiza utilizando el nombre de usuario y contraseña asignados por la Oficina de Sistemas de Información a funcionarios, pasantes, contratistas y proveedores, o partes interesadas quienes deben proteger y no compartir sus credenciales de acceso a la red y servicios de red (correo electrónico, red inalámbrica, entre otros) que le son conferidos de acuerdo con su perfil.

Los funcionarios son responsables de su nombre de usuario y contraseña asignados, así como notificar a la Oficina de Sistemas de Información el cambio de su contraseña cuando se sospeche el conocimiento de ésta por terceras personas.

2.4.3. Administración de cuentas de usuario y contraseñas

Los funcionarios, pasantes, contratistas, proveedores o partes interesadas, deben cumplir con las políticas para el uso de cuentas de usuario y contraseñas, relacionadas con la responsabilidad de cualquier acción que se realice utilizando la cuenta de usuario y contraseña asignada, así mismo se deberá tener en cuenta lo siguiente:

- Las cuentas de usuario y contraseñas se establecen de acuerdo con los estándares y directrices definidas por la Oficina de Sistemas de Información, con el propósito de que no sean fáciles de descifrar.
- Las cuentas de usuario y contraseñas son de uso personal e intransferible y por ningún motivo se deben prestar o facilitar a otros funcionarios, pasantes, contratistas, proveedores o partes interesadas.
- Las cuentas de usuario y contraseñas no deben ser reveladas por vía telefónica, correo electrónico, o ser escritas en ningún medio, excepto cuando son entregadas en custodia, previa autorización del Jefe inmediato del funcionario o contratista y de la Oficina de Sistemas de Información.
- No se debe habilitar la opción “recordar clave en este equipo“, que ofrecen los programas o aplicaciones o navegadores web, esto con el fin de limitar el acceso a los aplicativos a personas no autorizadas, especialmente para los funcionarios, pasantes, contratistas, proveedores o partes interesadas con acceso remoto autorizado a la plataforma tecnológica y aplicativos o sistemas de información de la entidad.
- Reportar al correo electrónico soportetecnico@mincit.gov.co, cualquier sospecha de uso no autorizado del usuario y contraseña asignados.

2.5. CRIPTOGRAFÍA

2.5.1. Política sobre el uso de controles criptográficos

En el MinCIT no se permite el uso de herramientas o mecanismos de encripción o de firmas digitales diferentes a las definidas y autorizadas por la Oficina de Sistemas de Información.

2.5.2. Gestión de certificados de firma digital

El MinCIT dispone de la infraestructura tecnológica necesaria para soportar la operación de certificados de firma digital .

La Oficina de Sistemas de Información administra la plataforma para la gestión de los certificados de firma digital para los aplicativos que implementan dicha funcionalidad.

Los funcionarios y contratistas deben informar cualquier evento o incidente relacionado con el uso de la firma digital asignada al correo electrónico soportetecnico@mincit.gov.co.

2.6. SEGURIDAD FÍSICA Y AMBIENTAL

2.6.1. Áreas seguras

MinCIT cuenta con los mecanismos de control de ingreso y acceso físico a las instalaciones de la entidad por parte de funcionarios, pasantes, contratistas, proveedores o partes interesadas, los cuales son coordinados con los responsables de la seguridad a través del Grupo Administrativa del Ministerio con la Administración del Edificio Centro de Comercio Internacional – ECCI.

El ingreso a las instalaciones del Ministerio y el acceso a las áreas seguras como son el Archivo Central y bodegas por parte de funcionarios, pasantes, contratistas, proveedores o partes interesadas, deben ser autorizados por el funcionario responsable del área física específica o Supervisor del contratista o proveedor de acuerdo al alcance de la actividad que se requiera adelantar y deben ser acompañados por un funcionario del área durante el tiempo que dure la visita o actividad.

El ingreso a los centros de cómputo y centros de cableado del Ministerio solo está autorizado a personal técnico que desarrolla trabajos técnicos en estas áreas. El acceso será autorizado por el Coordinador del Grupo de Ingeniería y soporte técnico de acuerdo al alcance de la actividad que se requiera adelantar y deben ser acompañados por un funcionario del área durante el tiempo que dure la visita o actividad.

2.6.2. Seguridad de equipos

MinCIT cuenta con controles que le permiten monitorear la disponibilidad e integridad de la infraestructura tecnológica, así como los niveles adecuados de mantenimiento y soporte a la infraestructura de red, plataformas operativas, sistemas de información, aplicativos, entre otros.
En caso de pérdida o robo del dispositivo móvil de propiedad del Ministerio de Comercio, Industria y Turismo, el responsable del dispositivo reporta inmediatamente el hecho al Jefe inmediato, Grupo Administrativa y al Grupo de Ingeniería y Soporte Técnico, y de inmediato se realizan las siguientes acciones:

- Inhabilitar los servicios asociados al dispositivo.
- Las credenciales son modificadas.
- Se notifica a los grupos de interés donde potencialmente se pudieron haber comprometido activos de información.

2.6.3. Ingreso o retiro de activos

MinCIT aplica los controles para el registro de entrada y salida de las instalaciones de la entidad de personas, equipos y elementos.

El ingreso o retiro de los equipos de cómputo por parte de los funcionarios o contratistas deberá quedar registrado en la recepción del piso o bodega desde el cual se realice la entrada o salida.

El ingreso o retiro de información debe ser autorizado por el propietario de la información – Líder o responsable de proceso, quien deberá informar a la Oficina de Sistemas de Información para aplicar los controles para el almacenamiento, transporte o transferencia de la información desde o hacia otras organizaciones.

2.6.4. Equipos fuera de las instalaciones

Los funcionarios que desarrollan sus funciones en sitio o en modalidad de teletrabajo y contratistas con asignación de portátiles, tablets, notebooks, memorias USB o cualquier otro dispositivo de propiedad del Ministerio, son responsables y custodios del bien asignado, así como de la información que en el dispositivo se encuentre almacenada, para lo cual deben tener en cuenta que:

- El MinCIT asigna los equipos portátiles con guaya de seguridad, por lo tanto los funcionarios y contratistas deben anclar estos equipos al punto de trabajo.
- Los equipos portátiles son para uso exclusivo de las funciones asignadas por la entidad y no deben ser manipulados por personas diferentes a los responsables,como se dispone en el numeral 2.3.3. Uso adecuado de los activos y recursos de información del presente Manual.

2.6.5. Equipos de usuario desatendido

Los servidores, computadores y portátiles tendrán habilitado el control automático de bloqueo de sesión. Por defecto el bloqueo se habilita después de diez (10) minutos de inactividad, y solo se podrán desbloquear con el usuario y contraseña asignada.

Los funcionarios, pasantes, contratistas, proveedores o partes interesadas con equipos asignados por el Ministerio, deben bloquear su computador o portátil cada vez que se retiren temporalmente de su lugar de trabajo y una vez finalizada su jornada laboral deben apagarlo.

Los computadores y portátiles del Ministerio solo deben mostrar en el escritorio de pantalla el papel tapiz o fondo de pantalla o protector de pantalla institucional, o el definido para comunicar temas de interés institucional, de acuerdo con el protocolo de comunicaciones del MinCIT.

2.6.6. Escritorio y pantalla limpia

El MinCIT promueve:

- La política de escritorio limpio en los lugares de trabajo para proteger la información crítica o sensible en medios impresos.
- La política de pantalla limpia en computadores, portátiles y servidores, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Los funcionarios, pasantes, contratistas, proveedores o partes interesadas deben tener en cuenta las siguientes consideraciones:

- En los lugares de trabajo solo deben permanecer los documentos y elementos necesarios para la realización de las labores. No se deben dejar documentos originales, preliminares o finales con información reservada o clasificada a la vista de otras personas, o desatendidos en otro lugar diferente al sitio de trabajo. Las copias de trabajo deben ser destruidos antes de ser arrojados a la basura. No se deben reutilizar documentos impresos que contengan información reservada o clasificada.
- Se debe aplicar los controles de seguridad y privacidad de la información identificados para los activos sensibles y críticos determinados por el Ministerio con el fin de salvaguardar la información reservada o clasificada que se encuentre en cualquier medio.
- La liberación de los trabajos de impresión o de escáner de documentos se realizará a través de autenticación cumpliendo con los requerimientos de disponibilidad, confidencialidad y cero desperdicio de papel.

2.7. SEGURIDAD DE LAS OPERACIONES

2.7.1. Procedimientos de operación documentados

Se tienen establecidos los procedimientos, registros e instructivos de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada del MinCIT.

Todas las tareas relacionadas con el mantenimiento de la infraestructura tecnológica, del centro de cómputo, de computadores, portátiles, plantas eléctricas, aíre acondicionado y demás dispositivos, se realiza de forma programada, es comunicada su ejecución y documentada.

2.7.2. Gestión de cambios

La Oficina de Sistemas de Información aplica el procedimiento IC-PR-029 Gestión de cambios de Tecnologías de la Información, para la plataforma tecnológica y coordina con los líderes y responsables de procesos y con las partes interesadas el desarrollo de los cambios, a fin de minimizar la afectación de la operación de los procesos y servicios críticos, y mantener la disponibilidad, integridad o confidencialidad de la información.

2.7.3. Gestión de capacidad

La Oficina de Sistemas de Información aplica el procedimiento de gestión de capacidad de la plataforma tecnológica, con el objeto de garantizar la disponibilidad de los recursos tecnológicos requeridos por los procesos del negocio. Para lo cual tiene en cuenta los siguientes actores:

- Las necesidades detectadas a los grupos de interés para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.
- La gestión para el almacenamiento en archivo de gestión, archivo central o eliminación de acuerdo a los tiempos establecidos en las tablas de retención documental (TRD)
- Definición anual del cambio, la transición o cierre definitivo de las aplicaciones, sistemas de información, bases de datos, equipos o ambientes.

2.7.4. Separación de los ambientes de desarrollo, pruebas y operación

El MinCIT cuenta en su infraestructura de procesamiento de información con ambientes separados para desarrollo, pruebas y producción. Así mismo, controla el paso de software y aplicaciones de un ambiente a otro.

La Oficina de Sistemas de Información coordina la realización de la instalación, desarrollo o pruebas de software, en los entornos de desarrollo y de producción; y del uso de muestras de datos reales en ambientes de desarrollo y pruebas.

2.7.5. Protección contra códigos maliciosos

Todos los servidores, computadores y portátiles del MinCIT tienen instalado y actualizado el software de antivirus con actualización en línea, así como los sistemas operativos y software base de acuerdo a los siguientes lineamientos:

- Prohibición de ejecución de aplicativos no autorizados por el MinCIT
- Definición anual del cambio, la transición o cierre definitivo de las aplicaciones, sistemas de información, bases de datos, equipos o ambientes.
- Concienciar a funcionarios, contratistas, pasantes y terceros acerca de las amenazas informáticas actuales, de falsas alarmas (hoaxes) y de cómo proceder frente a las mismas.

2.7.6. Copias de respaldo

La Oficina de Sistemas de Información aplica el procedimiento de copias de respaldo para la información crítica de la Entidad contenida en los servidores y sistemas de información del MinCIT.

Los funcionarios y contratistas son responsables de la realización de las copias de respaldo de la información almacenada en los computadores y portátiles asignados. Los funcionarios y contratistas deben solicitar apoyo al personal de soporte técnico de la Oficina de Sistemas de Información para la realización de las copias o backups de información.

2.7.7. Control de software operacional

La Oficina de Sistemas de Información aplica los procedimientos de IC-PR-018 Asesoría y Asistencia Técnica en Materia Informática e IC-PR-019 Actualización de Tecnología para el desarrollo y mantenimiento de software hecho en casa o por fábrica de software. Así mismo aplica los procedimientos de “gestión de cambios” y de “gestión de capacidad” para asegurar los cambios y recursos requeridos.

Para los desarrollos en la modalidad de fábrica de software se aplican los “acuerdos de niveles de servicio” establecidos en cada uno de los contratos.

2.8. SEGURIDAD DE LAS COMUNICACIONES

2.8.1. Controles de redes y seguridad de los servicios de red

La Oficina de Sistemas de Información administra la red de telecomunicaciones y demás equipos y dispositivos conectados a la red y coordina el acceso de contratistas y proveedores a recursos de acuerdo con la actividad a realizar.

2.8.2. Separación en las redes

La plataforma tecnológica del MinCIT está distribuida en segmentos de red independientes – VLANs - para cada servicio, separando las redes de servicios internos de la Entidad, de las conexiones con terceros y del acceso a Internet.

2.8.3. Transferencia de información

El intercambio de información reservada o clasificada del MinCIT con proveedores y partes interesadas está amparado mediante decretos, convenios o acuerdos de confidencialidad, que garanticen los controles requeridos para asegurar la integridad y confidencialidad de la información.

2.8.4. Acuerdos de confidencialidad o de no divulgación

En la contratación del MinCIT se especifican cláusulas de confidencialidad o se suscriben acuerdos de confidencialidad para el manejo adecuado de la información a la que deban tener acceso durante la ejecución del contrato.

2.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La Oficina de Sistemas de Información aplica los procedimientos de “Asesoría y asistencia técnica en materia de TICS” y “Actualización tecnológica” para el desarrollo y mantenimiento de software hecho en casa o por fábrica de software. Así mismo aplica los procedimientos de “gestión de cambios” y de “gestión de capacidad” para asegurar los cambios y recursos requeridos.

Para los desarrollos en la modalidad de fábrica de software se aplican los “Acuerdos de Nivel de Servicio - ANS” establecidos en cada uno de los contratos.

El MinCIT cuenta con las licencias de software y los derechos de uso para los productos desarrollados por terceros

2.10. RELACIONES CON LOS PROVEEDORES

En la contratación del MinCIT se especifican cláusulas de confidencialidad o se suscriben acuerdos de confidencialidad para el manejo adecuado de la información a la que deban tener acceso los proveedores durante la ejecución del contrato.

2.11. GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Oficina de Sistemas de Información aplica el procedimiento de gestión de incidentes para dar respuesta oportuna a los eventos e incidentes que puedan impactar de forma negativa los activos de información MinCIT. Para la adecuada gestión de los incidentes de seguridad y privacidad de la información, se deben tener en cuenta que:

1. Los funcionarios, pasantes, contratistas, proveedores y partes interesadas deben reportar al correo electrónico soportetecnico@mincit.gov.co cualquier riesgo materializado, amenaza o vulnerabilidad detectada respecto a la seguridad y privacidad de la información en los sistemas de información o los servicios usados en la Entidad.

2. En caso de requerirse apoyo externo el MinCIT reportará los incidentes de seguridad teniendo en cuenta los lineamientos de la política nacional de seguridad digital y el apartado de Contacto con las autoridades y grupos de interés especial del presente Manual.

Para efectos de mantener la continuidad de la gestión de Tecnologías de la Información y Comunicación que soportan los negocios del Ministerio, se conformará el Equipo de Trabajo para la Respuesta a Incidentes de Seguridad y Privacidad de la Información, del cual formarán parte:

- El Jefe de la Oficina de Sistemas de Información.
- El Jefe de la Oficina Asesora de Planeación Sectorial y el Oficial de Seguridad o quien haga sus veces.
- El Secretario General o su delegado.
- El Director o Jefe de Oficina propietario del sistema de información o servicio de TI afectado.
- El Jefe del equipo SOC/NOC.
- El personal técnico relacionado con el Sistema de información o servicio de TI afectado.

2.12. CONTINUIDAD DE LA GESTIÓN DE TI

La continuidad de la gestión de TI se encuentra alineada con la continuidad del negocio del MinCIT y el cumplimiento de sus objetivos estratégicos.

La oficina de sistemas de información aplica los procedimientos que apoyan la adecuada gestión de la plataforma tecnológica para asegurar su disponibilidad.

2.13. CUMPLIMIENTO DE REQUERIMIENTOS

2.13.1. Cumplimiento de las obligaciones legales

El Ministerio da cumplimiento a las normas y regulaciones relacionadas con los lineamientos y directrices para:

- La gestión de la seguridad y privacidad de la información en procesos, en el entorno de información y comunicación institucional y el entorno tecnológico.
- La salvaguarda en los contratos y convenios mediante la suscripción de compromisos o acuerdos de confidencialidad sobre el manejo de la información institucional en cualquiera de sus formas.
- El uso de licencias de software adquirido con terceros o el desarrollado "in House".
- El uso y publicación de documentos creados en la entidad, así como los otorgados por terceros que se requieran para documentar las actividades de la misión institucional.

2.13.2. Derechos de propiedad intelectual

El cumplimiento de las normas de propiedad intelectual emitidas por la Dirección Nacional de Derechos de Autor, relacionadas con los Derechos de Autor para el Uso de Software, material fílmico, fotográfico, de audio o de derechos conexos, cuenta en el Ministerio con los procedimientos, mecanismos y controles para garantizar el cumplimiento de las restricciones legales al uso del material protegido, así:

- El Ministerio solo podrá autorizar el uso de material (documentos, fotografías, videos) producidos como parte del ejercicio misional, o haciendo uso de material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.
- El Ministerio conserva las pruebas y evidencias de propiedad de licencias, discos maestros, manuales de producción de terceras partes.
- El Ministerio verifica que sólo se instalen productos con licencia y software autorizado
- El Ministerio da cumplimiento a las normas, regulaciones y demás directrices que emita el gobierno nacional para el uso de software por parte de los entes Estatales

2.13.3. Privacidad y protección de información de datos personales

El MinCIT en cumplimiento de las normas y regulaciones para la protección de los datos personales cuenta con la política de protección de datos personales.

2.13.4. Revisiones de seguridad de la información

El MinCIT asegura el cumplimiento de las políticas de seguridad y privacidad de la información en sus procesos institucionales.

ELABORÓ	REVISÓ	APROBÓ
Nombre: EDUARDO ANDRES OSPINA JARRO **Cargo:** Contratista(s) **Fecha:** 28/Ago/2018	**Nombre:** EDGAR GREGORIO CARRILLO MONCADA **Cargo:** Jefe Oficina de Sistemas de Información **Fecha:** 02/Oct/2018	**Nombre:** ALEJANDRO TORRES PERICO **Cargo:** Jefe Oficina Asesora de Planeación Sectorial **Fecha:** 08/Oct/2018 **Nombre:** EDGAR GREGORIO CARRILLO MONCADA **Cargo:** Jefe Oficina de Sistemas de Información **Fecha:** 09/Oct/2018