TABLA DE CONTENIDO

[1. Introducción 2](#_Toc5197841)

[2. Objetivo 2](#_Toc5197842)

[3. Alcance 2](#_Toc5197843)

[4. Productos esperados 2](#_Toc5197844)

[5. Términos y definiciones 2](#_Toc5197845)

[6. Políticas específicas 2](#_Toc5197846)

[6.1. Organización de seguridad de la información 3](#_Toc5197847)

[6.2. Propietarios de los activos de información 3](#_Toc5197848)

[6.2.1. Utilización de computadores 3](#_Toc5197849)

[6.2.2. Dispositivos móviles 3](#_Toc5197850)

[6.2.3. Utilización de Internet 4](#_Toc5197851)

[6.2.4. Utilización de correo electrónico y mensajería instantánea 4](#_Toc5197852)

[6.2.5. Utilización de servicios de red 4](#_Toc5197853)

[6.2.6. Utilización Almacenamiento en la nube – OneDrive y Sharepoint 5](#_Toc5197854)

[6.2.7. Conexiones remotas 5](#_Toc5197855)

[6.3. Clasificación de Información 6](#_Toc5197856)

[6.4. Roles y responsabilidades 6](#_Toc5197857)

[6.5. Devolución de activos 6](#_Toc5197858)

[6.6. Seguridad de los equipos y entorno 6](#_Toc5197859)

[6.7. Política de escritorio y pantalla limpia 6](#_Toc5197860)

[6.8. Gestión comunicaciones y operaciones 7](#_Toc5197861)

[6.9. Control de acceso 7](#_Toc5197862)

[6.10. Gestión de incidentes 8](#_Toc5197863)

[Documentos relacionados 8](#_Toc5197864)

[7. Historial de cambios 8](#_Toc5197865)

[8. Aprobación 8](#_Toc5197866)

## Introducción

El modelo de seguridad de la información del Ministerio de Hacienda y Crédito Público (MHCP) está basado en la norma técnica ISO 27001:2103, este documento describe las políticas específicas y procedimientos a tener en cuenta por funcionarios, contratistas y terceros. Las políticas incluidas en este manual se establecen como parte fundamental del Sistema de Gestión de Seguridad de la Información.

## Objetivo

Establecer las políticas y normas de seguridad de la información de cumplimiento por parte de funcionarios, contratistas y terceros. De esta manera garantizando la protección de los activos en los cuales se procesa, opera, almacena, transmite información.

## Alcance

Estas políticas aplican a todos los funcionarios/contratistas/pasantes desde su vinculación a la entidad y hasta su retiro, y a terceras partes que accedan a los activos de la información del MHCP; estos están sujetos a los mismos requerimientos de seguridad y tienen las mismas responsabilidades de los funcionarios de la Entidad respecto a la seguridad de la información.

## Productos esperados

Protección de los activos en los cuales se procesa, opera, almacena, transmite información a partir de la aplicación de buenas prácticas para el uso seguro de los servicios y recursos TIC por parte de los usuarios de los mismos.

## Términos y definiciones

* **Escritorio Limpio**: característica del puesto de trabajo y componente de las políticas de seguridad de la información que busca evitar la exposición de información sensible o confidencial que reposa en medios diferentes a los electrónicos o digitales como es el medio impreso.
* **Terceras partes**: personas naturales o jurídicas, que en virtud de algún tipo de contacto con el Ministerio tienen acceso a información institucional o a servicios tecnológicos, sin que medie vinculación formal.

## Políticas específicas

Las políticas y normas relacionadas en este documento están orientadas a proteger los activos de información propiedad del MHCP y garantizar el uso apropiado de los dispositivos tecnológicos y servicios a disposición como Internet y correo; contribuyendo de esta manera a minimizar los riesgos por eventuales perdidas de los activos de información.

### Organización de seguridad de la información

El MHCP establecerá el sistema de seguridad de la información en el cual se relacionarán los roles y responsabilidades considerando actividades de administración, operación y gestión de la seguridad de la información.

* Los funcionarios, contratistas, pasantes y partes externas que realicen labores en la entidad, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares estipulados de la seguridad de la información.

### Propietarios de los activos de información

* Los activos de información pertenecen al MHCP y el uso de los mismos debe realizarse exclusivamente con propósitos laborales.
* Son propietarios de los activos de información los Administradores funcionales responsables por la información de sus procesos de negocio y Administradores técnicos responsables del hardware o sistemas de información según corresponda el tipo de activo.

###  Utilización de computadores

* La instalación de software en los computadores suministrados por el MHCP y de los equipos conectados a la red corporativa es una función exclusiva de la Centro De Servicios Tecnológicos y toda instalación debe tramitarse a través del mismo.
* Todo software utilizado en los equipos propiedad del ministerio, de los equipos conectados a la red corporativa o que se utilicen en las instalaciones del MHCP deben poseer las licencias de uso legal y la mesa de ayuda solo instalará software estándar de acuerdo a la disponibilidad de licencias de uso.
* Para instalación de software no estándar, la Dirección de Tecnología a través de SART (Subdirección de Administración de Recursos Tecnológicos) debe realizar una evaluación de seguridad y soporte del mismo. Solo si hay un concepto favorable se autorizará la instalación previa confirmación de la existencia de las respectivas licencias de uso legales.
* Los usuarios son responsables de apagar el equipo a su cargo al finalizar la jornada laboral.
* El traslado y movimiento de equipos (excepto los computadores portátiles) debe ser realizado por el área de Centro De Servicios Tecnológicos, la cual es responsable de mantener el inventario actualizado.
* Queda prohibido el almacenamiento en los discos duros de archivos de tipo videos, música, fotos, juegos o multimedia en general que no sean de carácter institucional.

### Dispositivos móviles

* Los dispositivos móviles institucionales entregados a funcionarios (teléfonos inteligentes, tabletas y computadores portátiles) por parte de la entidad se proporcionarán con las condiciones y herramientas necesarias para su uso responsable.
* Se debe evitar la instalación de programas y aplicaciones desde fuentes desconocidas, solo debe realizarse desde las tiendas oficiales para los dispositivos móviles institucionales.
* Las configuraciones de seguridad provistas en los dispositivos móviles institucionales no se deben modificar, ni desinstalar el software provisto con ellos al momento de su entrega.
* Los usuarios deben evitar la conexión hacia o desde la infraestructura del MHCP, a redes inalámbricas públicas que no requieran contraseña y a dispositivos desconocidos a través de Bluetooth u otro medio de transferencia de datos (Airdrop, NFC).

### Utilización de Internet

* La navegación en internet desde la infraestructura del MHCP se hará de forma controlada de acuerdo con lo establecido en la circular 013 del 9 de abril de 2015.
* La navegación y descarga de archivos en Internet debe realizarse de forma razonable y con propósitos laborales.

No se permite la navegación a sitios de alto riesgo o que pueda comprometer la posición del MHCP. Los sitios no permitidos son los de contenido: pornográfico, chistes, religiosos, terroristas, hackers, racistas, comunidades sociales, publicación de videos en línea, juegos políticos o cualquier contenido que represente riesgo de virus; código malicioso, etc.

### Utilización de correo electrónico y mensajería instantánea

* El correo electrónico debe ser utilizado con propósitos laborales.
* No se permite el envío de cadenas de correo y con contenido que atente contra la integridad humana de las personas o instituciones, tales como: pornográfico, chistes, religiosos, terroristas, hackers, racistas, políticos o cualquier contenido que represente riesgo de virus; código malicioso, etc.
* No se deben enviar correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red.
* Solo las áreas debidamente autorizadas pueden enviar correos masivos.
* La utilización de programas o utilitarios de mensajería instantánea de carácter público no están permitidos, ya que representan elementos de exposición pública y evaden los controles perimetrales.

### Utilización de servicios de red

* Los recursos de red que ha dispuesto el MHCP, tales como File Server, Intranet, SharePoint, etc, deben ser utilizados para el almacenamiento de información que sea para propósitos laborales exclusivamente. .
* El acceso a internet se debe realizar únicamente a través de los navegadores provistos por la Dirección de tecnología e instalados por el CST en cada uno de los equipos.
* Es responsabilidad de los funcionarios/contratistas/pasantes de la Entidad, almacenar la información relevante del Ministerio en los servidores de archivos dispuestos por la Dirección de tecnología, para que la misma sea respaldada según la política definida.
* Ningún tipo de información que se refiera a la misión funcional del MHCP puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo. Para estos casos, es responsabilidad de cada usuario replicar la información en las carpetas de archivos que residen en los servidores.

### Utilización Almacenamiento en la nube – OneDrive y Sharepoint

El servicio de almacenamiento en la nube basado en OneDrive y SharePoint,, comprende herramientas de trabajo colaborativo para el almacenamiento de documentos individuales y/o grupales, que facilitan la colaboración y el trabajo en equipo, por lo que su uso se debe enfocar en el almacenamiento de documentos en desarrollo o de apoyo a la gestión de los procesos, en determinados momentos, o para compartir documentos públicos de interés para otras entidades del estado o ciudadanía en general, de acuerdo con los objetivos de cada proceso misional.

Por lo tanto, la publicación de información en los servicios en la nube provistos por el Ministerio, deben seguir los siguientes lineamientos:

* La información publicada no debe ser de carácter confidencial ni poner en riesgo la integridad y confidencialidad de los procesos misionales y de apoyo del Ministerio de Hacienda, de manera que se pueda configurar una fuga de información, la cual será responsabilidad del usuario a quien se le haya asignado el uso del servicio.
* No está permitido en las cuentas asignadas a cada funcionario/contratista/pasante de One Drive y/o Sharepoint,, almacenar información personal o que no corresponda a asuntos propios de la actividad laboral realizada en la entidad. Igualmente, los documentos almacenados deben corresponder a actividades laborales, por lo que no está permitida la utilización del servicio para actividades comerciales, publicitarias y en general, ajenas a las funciones de la entidad.

Lo anterior, de acuerdo con las Políticas de Seguridad de la información de la entidad (Ver numeral 7.3.1.5 Utilización de Servicios de Red del documento Apo.1.Man.3.2 Políticas Seguridad Información, el cual establece *“Los recursos de red que ha dispuesto el MHCP, tales como File Server, Intranet, SharePoint, etc, no deben ser utilizados para el almacenamiento de información que no es para propósitos laborales; ejemplos de información no permitida son: Material pornográfico, videos, películas, música, fotos, etc.”*

En el caso de material audiovisual que requiera ser publicado en los servicios de almacenamiento en la nube, se harán excepciones siempre y cuando estén justificadas por el Director, Subdirector o jefe del área, y estén acordes con actividades del proceso soportado

.

* Es responsabilidad de cada funcionario/contratista/pasante que cuente con recursos asignados en OneDrive y/o SharePoint, salvaguardar y dar un adecuado manejo a la información almacenada, así como también otorgar el acceso y los permisos que considere a otras personas para acceder a la información almacenada. Los servicios de almacenamiento en la nube tienen opción de compartir información en forma pública sin restricciones o de restringirla a un número limitado de contactos; el uso de una u otra opción corresponde a la decisión del funcionario/contratista/pasante a quien se le ha asignado la cuenta del servicio.
* Es responsabilidad del funcionario/contratista/pasante a quien se asigne la cuenta de One Drive y/o SharePoint,, garantizar que la información que se almacene en dichas herramientas cumpla con la política de gestión de activos, incluida en las Políticas de Seguridad de la Información de la entidad (Ver numeral 7.2 del documento Apo.1.Man.3.2 Políticas Seguridad Información) y haya sido objeto de asignación de criterios de clasificación de información
* Toda información que se publique utilizando servicios de almacenamiento en la nube, debe ser copia de la almacenada en los servidores de archivos de la institución. Sin embargo, es responsabilidad de cada usuario procurar la salvaguarda de la información publicada en la nube, pudiendo adicionalmente, descargar una copia de todos los datos, a un equipo local, en cualquier momento
* Los servicios de almacenamiento en la nube tendrán como procedimientos de copias de respaldo, únicamente los contemplados dentro de los servicios de Office 365 (recuperación de archivos borrados durante los últimos 90 días).
* La asignación de cuentas para el uso de servicios de almacenamiento a contratistas y pasantes estará sujeta a la solicitud y aprobación parte del supervisor del contrato y/o encargado de la pasantía, quien asume la responsabilidad de determinar el tipo y clase de información que compartirá el contratista y/o pasante. A la finalización de un vínculo laboral o contractual con la entidad, es su deber exigir la entrega de la información publicada, antes realizar el proceso de desaprovisionamiento de la cuenta, como parte del procedimiento formal de retiro que tenga establecida la entidad.
* El uso de servicios de almacenamiento en la nube como Dropbox, Google Drive y similares, queda prohibido, dadas las situaciones de riesgo y seguridad para la información publicada y por los riesgos de propiedad de los documentos e información contenidas en esos repositorios.
* Para un mejor uso y aprovechamiento de los servicios de almacenamiento en la nube, hay que tener en cuenta las siguientes limitaciones:
* Uso de Caracteres no válidos. Algunos caracteres tienen un significado especial cuando se usan en los nombres de archivo en OneDrive y SharePoint como "\*" para los caracteres comodín y "\" en las rutas de nombre de archivo. Si un archivo o carpeta que esté intentando cargar en OneDrive contiene cualquiera de los caracteres enumerados a continuación, puede impedir que los archivos y carpetas se sincronicen. Por tanto, se debe cambiar el nombre del archivo o de la carpeta para quitar estos caracteres antes de cargarlo.
* Caracteres que no se permiten en nombres de archivos y carpetas en OneDrive y SharePoint : " \* : < > ? / \ | ~ " # % & \* : < > ? / \ { | }.
* Nombres de carpeta o archivo no válidos. No se permiten los siguientes nombres para archivos o carpetas: .lock, CON, PRN, AUX, NUL, COM1 - COM9, LPT1 - LPT9, \_vti\_, desktop.ini, o cualquier nombre de archivo comenzando con ~ $.
* Tamaño de carga de archivo: 15 GB
* Longitud del nombre y la ruta de archivo: Se aplica a la ruta completa, incluido el nombre de archivo, la cual debe contener menos de 400 caracteres para OneDrive y SharePoint; si se supera ese límite, se generará un mensaje de error.

Cualquier duda o inquietud que tengan, por favor consultar con el Centro de Servicios Tecnológicos.

### Conexiones remotas

Las conexiones remotas deben contar con las aprobaciones requeridas para establecerla a los dispositivos de la infraestructura del MHCP, de igual manera deben acatar las condiciones de uso establecidas para dichas conexiones.

### Clasificación de Información

* Cuando la información del MHCP sea utilizada, procesada o accesada por terceros, es obligación de la tercera parte respectiva conocer y prestar el cuidado y protección de acuerdo a la clasificación establecida por el MHCP.

### Roles y responsabilidades

* Todo funcionario/contratista/pasante de la entidad es responsable por el cumplimiento de las políticas de seguridad de la información. Adicionalmente cada funcionario está comprometido a reportar al CST, cualquier incidente de seguridad del que tenga conocimiento, por los medios y formas establecidos para ello.

### Devolución de activos

* Los activos asignados a los funcionarios/contratistas/pasantes o terceras partes que finalizan su relación laboral o contractual deben ser reintegrados a la entidad en las condiciones y estado en que le fueron entregados.
* El funcionario/contratistas/pasantes es responsable por obtener las firmas del “Formato de entrega de cargo”, la cual debe contar con las evidencias en señal de devolución a satisfacción por parte de jefe inmediato (o quien él designe) y las áreas de Tecnología, Servicios, y Recursos Humanos.

### Seguridad de los equipos y entorno

* El retiro e ingreso de todo activo de información de propiedad de los funcionarios del Ministerio, utilizados para fines personales debe hacerse mediante orden escrita con visto bueno de la Subdirección de Servicios. El personal de vigilancia de recepción verifica o registra, respectivamente, las características de identificación del activo de información.
* El retiro e ingreso de todo activo de información de los visitantes que presten servicios al MHCP (Consultores, periodistas, otros) será registrado y controlado en las porterías del edificio. El personal de vigilancia de recepción verifica o registra, respectivamente, las características de identificación del activo de información.
* Cada vez que un funcionario/contratista/pasante se ausente de su lugar de trabajo, debe bloquear el computador, guardar en lugar seguro cualquier documento, medio de almacenamiento (USB – Disco Duro).
* Los funcionarios/contratistas/pasantes deben evitar divulgación de temas laborales en lugares públicos, de esta manera contrarrestar las posibilidades de obtener información confidencial por parte de cibercriminales

### Política de escritorio y pantalla limpia

Los funcionarios/contratistas/pasantes del MHCP deben adoptar la cultura de “escritorio limpio” que consiste en:

* En los puestos de trabajo de los funcionarios/contratistas/pasantes solo deben permanecer los documentos y elementos necesarios para la realización de sus labores.
* Los archivadores y escritorios deben permanecer cerrados con llave.
* No dejar documentos confidenciales a la vista de otras personas.
* No arrojar documentos confidenciales a la basura, estos deben ser destruidos.
* Al finalizar las labores diarias o si el funcionario/contratista/pasante se va a ausentar de su puesto de trabajo, todos los documentos confidenciales deben ser guardados en sitio seguro.
* Evitar papeles autoadhesivos que contengan información confidencial, especialmente contraseñas
* Las estaciones de trabajo deben ser apagadas al finalizar la jornada.
* Los trabajos de impresión que contengan información confidencial deben ser recogidos de forma inmediata por quien los origina.
* La impresión de documentos críticos y restringidos deben estar protegidos de forma que solo se impriman cuando el usuario originador los libere con clave.

### Gestión comunicaciones y operaciones

* Todo proceso que involucre intercambio de información del MHCP y terceras partes debe contar con un contrato o convenio interadministrativo el cual defina claramente las obligaciones y derechos de cada una de las partes, el dueño de la información es el responsable de garantizar que exista el contrato.

### Control de acceso

* Las acciones y operaciones realizadas con las cuentas de usuario son responsabilidad del propietario de la cuenta.
* Las contraseñas son de carácter personal e intransferible.
* Los usuarios deben evitar dejar sus estaciones de trabajo con la sesión abierta.
* Las solicitudes de acceso a sistemas, aplicaciones y servicios corporativos serán atendidas teniendo tomando en consideración, que los usuarios deben tener acceso solo a los recursos o servicios necesarios para la ejecución de sus actividades.
* La solicitud de acceso de usuarios externos a los servicios o soluciones informáticas del MHCP debe realizarse a través del Centro de Servicios Tecnológicos (CST). Nueva

### Gestión de incidentes

* Los usuarios de los servicios TIC del MHCP que observen situaciones sospechosas o que claramente sean incidentes de seguridad de la información tienen la obligación de reportar los incidentes de seguridad, a través del CST.

## Documentos relacionados

* Apo.1.3.Man.3.2.Políticas de Seguridad de la Información
* Apo.1.3.Man.3.2.2.Política de Gestión de activos
* Apo.1.3.Man.3.2.2.PoliticaControlAcceso

## Historial de cambios

| FECHA | VERSIÓN | DESCRIPCIÓN DEL CAMBIO | ASESOR SUG |
| --- | --- | --- | --- |
| Mayo 2017 | 1.0 | Creación del documento | Derly Catherine Cifuentes Guerrero |
| 01-04-2019 | 2.0 | Se incluye la descripción del almacenamiento en la nube y se ajusta a la plantilla establecida por el SUG | Andrea Catalina Cuesta Ruiz |
| 06-08-2019 | 3.0 | Se ajusta lo referente a utilización de almacenamiento en la nube incluyendo Sharepoint | Andrea Catalina Cuesta Ruiz |

## Aprobación

|  |  |
| --- | --- |
| ELABORADO POR: | **Nombre**: Alejandro I. Cruz**Cargo**: Asesor**Dependencia**: Despacho Dirección de TecnologíaFecha: 15-07-2019  |
| REVISADO POR: | **Nombre**: Alejandro I. Cruz**Cargo**: Asesor**Dependencia**: Despacho Dirección de TecnologíaFecha: 15-07-2019  |
| APROBADO POR: | **Nombre:** Ricardo Ríos Rosales**Cargo:** Director de Tecnología**Dependencia:** Despacho de la Dirección de Tecnología Fecha: 17-07-2019 |