# TABLA DE CONTENIDO

## 1 Introducción

Las políticas de seguridad de la información del Ministerio de Hacienda y Crédito Público (MHCP), definen los normas que deben ser seguidas por los funcionarios y terceras partes que hacen uso de los activos de información del MHCP, establecidas por el Ministerio para proteger la Confidencialidad, Integridad y Disponibilidad de la información del MHCP.

Las Políticas de Seguridad de la Información del MHCP están compuestas por normas con características a nivel técnico y a nivel de usuario final, las cuales están agrupadas por temas en 11 políticas.

El presente documento es una extracción de las políticas a nivel de “usuario final” con el propósito de facilitar la comprensión y entendimiento de las mismas a los “usuarios finales”. Esto no exime a los “usuarios finales” cumplir con la totalidad de las políticas de Seguridad de la información a nivel técnico y de usuario.

Las políticas detalladas y agrupadas por temas específicos, las cuales deben ser conocidas y cumplidas por los funcionarios y tercereas partes, con contenido técnico y de usuario final son:

- PL-01-01 Política de Seguridad
- PL 02 - Seguridad Organizacional
- PL 03 - Gestión de los activos de información
- PL 04 - Seguridad del personal
- PL 05 - Seguridad Física y Ambiental
- PL 06 – Gestion Comunicaciones Operaciones
- PL 07 - Control de Acceso
- PL 09 - Gestión de Incidentes
- PL 08 - Adquisición, Desarrollo y Mantenimiento de SI
- PL 09 - Gestión de Incidentes
- PL 10 - Gestión de la continuidad del negocio
- PL 11 – Cumplimiento

## 2 Alcance

Estas políticas de seguridad de la información aplican a todos los **activos de información** del MHCP, durante su ciclo de vida.

Las políticas están orientadas a proteger los activos de información en todos los ambientes, internos y externos, en los cuales se procesan, operan, almacenan, transmiten o usan y estén sometidos a los controles correspondientes para su adecuada protección; a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de servicios como Internet y el correo electrónico; a brindar a los funcionarios pautas para la utilización apropiada de los activos informáticos; y a contribuir a minimizar los riesgos de una eventual pérdida de los activos de información sensitivos para del MHCP.

Estas políticas aplican a todos los funcionarios o 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.

## 3 Definiciones

Para facilitar la comprensión de las políticas se ha construido un documento que contiene un glosario de los términos técnicos que le permitirá al lector conocer el significado de los términos. Ver GL - 01 Glosario políticas de seguridad de la información.doc

## 4 Cumplimiento

El cumplimiento de las políticas de seguridad de la información es obligatorio para todo funcionario o tercera parte. (Si un individuo u organización viola las políticas de seguridad por negligencia o intencionalmente, el MHCP tomará las acciones disciplinarias y legales correspondientes.

## 5 Dominios de la Norma

La norma NTC – ISO/IEC 27001 define los siguientes once (11) dominios que agrupan 131 controles:

1. **Política de seguridad**: Constituye el presente documento; en él se establecen las políticas con respecto a la seguridad de la información del MHCP.

2. **Organización de la seguridad**: Gestionar la seguridad de la información dentro de la Entidad. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros)

3. **Gestión de activos**: Se relaciona con el mantenimiento y protección apropiados de todos los activos de información.

4. **Seguridad del recurso humano**: Busca asegurar que empleados, contratistas y terceras partes entiendan sus responsabilidades en relación con las políticas de seguridad del MHCP y actúen de manera consistente con las mismas.

5. **Seguridad física y del entorno**: Busca prevenir el acceso físico no autorizado a las instalaciones de la Entidad, para prevenir daños o interferencias a los activos de información.

6. **Gestión de comunicaciones y operaciones**: Busca asegurar la correcta y segura operación de las áreas de procesamiento de información y de comunicaciones.

7. **Control de acceso**: Realiza el control físico o lógico del acceso a los activos de la información.

8. **Adquisición, desarrollo y mantenimiento de sistemas de información**: Asegura la inclusión de todos los controles de seguridad en los sistemas de información (infraestructura, aplicaciones, servicios, etc.)

9. **Gestión de incidentes de seguridad**: Busca que los eventos e incidentes de seguridad con los activos de información, sean comunicados y atendidos oportunamente y con los procedimientos definidos para tal fin, de manera que se tomen las acciones correctivas adecuadas y en el momento indicado.

10. **Gestión de la continuidad del negocio**: Enfocado en reaccionar ante las interrupciones de las actividades de la función misional, para proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres; también, es la garantía planeada para asegurar que las operaciones se recuperen dentro del tiempo previsto.

11. **Cumplimiento**: Busca prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

# 6 Premisas básicas de seguridad de la información

Los siguientes principios básicos fundamentan las políticas de seguridad de la información para la infraestructura tecnológica del MHCP:

## 6.1 Autenticidad

La información requerida para el cumplimento de la funciones del MHCP debe ser veraz y estar debidamente autorizada.

## 6.2 Confiabilidad

La información procesada por del MHCP tiene carácter confiable.

## 6.3 Confidencialidad

La información del MHCP debe estar debidamente protegida para que sea accedida por el personal autorizado.

## 6.4 Disponibilidad

Los activos de información deben estar disponibles para soportar los objetivos de la función misional del MHCP.

## 6.5 Integridad

Los activos de información deben estar adecuadamente protegidos para asegurar su completitud y precisión. Las medidas de validación definidas deben permitir detectar las

modificaciones inapropiadas, la eliminación o la adulteración de los activos de información.

### 6.6 No repudio

Los activos de información deben estar provistos de mecanismos que permitan probar que una acción o un evento han tenido lugar y no puedan ser negados posteriormente

### 6.7 Trazabilidad

El MHCP requiere que se pueda realizar seguimiento de los cambios de la información y se identifiquen los agentes de cambio.

### 6.8 Protección de la información

La información debe ser protegida con el nivel necesario en proporción a su valor y el riesgo para la función misional. La protección debe concentrarse en las propiedades de confidencialidad, integridad y disponibilidad de la información.

### 6.9 Protección de los recursos tecnológicos

Los recursos tecnológicos deben ser protegidos con el nivel necesario en proporción a su valor y el riesgo para la función misional. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales de los funcionarios y terceras partes; esta utilización debe hacerse en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

### 6.10 Autorización de usuarios

Todos los usuarios deben ser identificados independientemente con permisos de accesos específicos e individualmente autorizados por razones básicas de la función misional; esta autorización debe estar basada en los principios del “need-to-know” y ”least privilege”. Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización apropiada y auditoria confiable.

### 6.11 Responsabilidad

Los usuarios, dueños y custodios de los activos de información del MHCP son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas de información del MHCP deben generar y mantener pistas apropiadas de auditoría para identificar usuarios y documentar los eventos relacionados con incidentes de seguridad.

### 6.12 Esfuerzo de Equipo

Para que la seguridad de la información sea efectiva, se requiere el esfuerzo de equipo, donde deben participar en forma activa todos los funcionarios que tengan interacción con los activos de la información de la Entidad. Todos los funcionarios y terceras partes deben

cumplir con las políticas de seguridad de la información y, además, desempeñar un papel activo para su comprensión, entendimiento y divulgación.

### 6.13 Revisiones de seguridad

En forma periódica del MHCP debe efectuar las revisiones necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad. Esta tarea debe ser realizada por el Oficial de Seguridad o quien haga sus veces.

### 6.14 Propiedad de la información

La información soportada por la infraestructura de tecnología informática del MHCP pertenece a la Entidad, a menos que en una relación contractual se establezca lo contrario. Sin embargo, la facultad de otorgar acceso a la información es del responsable de la dependencia que genera o es propietaria de esta información.

La información propiedad del MHCP y sobre la cual tiene sus derechos, podrá ser suministrada a los entes de control pertinentes cuando estos lo requieran, con previa autorización expresa y aprobada para estos fines por las directivas de la Entidad.

Para efectos de control del flujo de la información de los procesos de la Entidad, se asignarán responsables de la información, quienes deben asegurar y otorgar acceso a la información que genere su dependencia, con el fin de lograr un adecuado ambiente de control y de segregación de funciones.

En caso de divulgación no autorizada de la información de propiedad del MHCP, se realizarán las investigaciones pertinentes para establecer las responsabilidades del caso y proceder conforme lo establece para estos casos la normatividad y los procedimientos del MHCP.

## 7 Políticas

### 7.1 Política de Seguridad

La Política de seguridad de la información compuesta por las políticas de seguridad relacionadas en el numeral 1, especifica las directrices que deben ser cumplidas por parte de los funcionarios y terceras partes del MHCP, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en su información.

### 7.2 Organización de la seguridad

#### 7.2.1 Asignación de responsabilidades para la Seguridad de la Información

A continuación se describen los roles y responsabilidades en cuanto a Seguridad de la Información:

**Personal Directivo:** El personal directivo de la entidad es responsable que los colaboradores a su cargo conozcan y apliquen las políticas de seguridad de la

información. Las reuniones de grupos primarios serán utilizadas para divulgar las directrices.

**Oficial de Seguridad:** El MHCP mantendrá dentro de su planta de funcionarios un Oficial de Seguridad de la información, cuyas funciones estarán caracterizadas y definidas según la necesidad de la función misional. Para mayor información ver política PL-02-Seguridad organizacional.

> NOTA: Este rol está incorporado en estas políticas obedeciendo a las buenas prácticas en Seguridad y a Lineamientos del Estado; sin embargo, a la fecha de revisión de estas políticas no se ha formalizado aún. Parte de las funciones propuestas las desempeñan los responsables de la Seguridad de la Información del Proceso APO 1.3. Gobierno y Gestión de TIC.

**Dueños de la Información:** Toda información utilizada por la entidad, debe poseer un dueño. Los dueños de la información son los responsables de este activo y deben: definir su clasificación, determinar los niveles de acceso a ella, autorizar la asignación de permisos de acceso y aplicar los controles necesarios para su almacenamiento, procesamiento, distribución y uso.

**Administradores de los Sistemas:** Los administradores de los diferentes sistemas deben, en forma proactiva, implementar las medidas técnicas y los procedimientos, para brindar un nivel apropiado de seguridad de la información utilizando el procedimiento de control de cambios.

**Funcionarios:** Todo funcionario de la entidad es responsable por el cumplimiento de las políticas de seguridad de la información. Adicionalmente cada funcionario está comprometido a reportar al cualquier incidente de seguridad del que tenga conocimiento por los procedimientos establecidos. Ver procedimiento *Apo.1.Man.3.Pr.1- Procedimiento para Gestión de Incidentes de Seguridad*.

**Terceras partes:** Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir las políticas de Seguridad de la Información del MHCP**.**

### **7.2.2** Acuerdos de confidencialidad

Todo funcionario del MHCP y terceras partes que realizan labores para la Entidad que involucren el manejo de información, deben aceptar el carácter de confidencialidad y no divulgación de la información de la entidad; en los casos que amerite, (Contratos de prestación de bienes y servicios que implique uso o entrega de información diferente a la de uso público , pruebas de concepto o similares), se deberá suscribir un Acuerdo de Confidencialidad entre las partes.
Todos los contratos celebrados por el MHCP deben incluir cláusulas de acuerdo de confidencialidad que obliguen al contratista a guardar reserva sobre la información que el MHCP suministre o las configuraciones realizadas.

Los supervisores o interventores de contratos son responsables de:

- Garantizar que las terceras partes y los colaboradores de las mismas, conozcan y acepten las Políticas de Seguridad, en particular lo referente al buen uso, reserva y confidencialidad de la información del Ministerio.
- Velar por que las terceras partes y los colaboradores cumplan los acuerdos de confidencialidad, en el caso que se hayan suscrito.
- Archivar y custodiar bajo los controles necesarios los compromisos suscritos por cada funcionario.

**7.2.3** Identificación de los riesgos relacionados con partes externas

Todo acceso de terceras partes a los activos de la información de la Entidad, debe ser objeto de un análisis de riesgos, implementación de los controles respectivos y autorización por parte del responsable técnico o supervisor, por los coordinadores de grupo, el oficial de seguridad o los funcionarios o terceros que hagan sus veces, responsables de la Seguridad de la Información.

- En situaciones estrictamente controladas, el MHCP permitirá el acceso de terceros a sus redes internas y a los sistemas de información.
- Estos accesos deberán ser explícitamente autorizados por: el Subdirector de Administración de Recursos Tecnológicos y avalados por los responsables de la Seguridad de la Información.
- Los privilegios de sistema para estos usuarios terceros deben ser estrictamente limitados al alcance del sistema en cuestión y a la información necesaria para lograr los objetivos del proyecto.
- En caso de necesitarse una conexión de emergencia que responde a un incidente, esta solicitud se manejará a través del procedimiento de manejo de incidentes.
- Toda conexión de un tercero debe ser solicitada formalmente y debidamente aprobada.
- El análisis de riesgos debe ser conducido por el área responsable de la relación con el tercero, posteriormente será revisado por los responsables de la Seguridad de la Información y finalmente se presentará al Comité de Seguridad que se haya conformado.

## 7.3 Gestión de los activos de información

### 7.3.1 Uso aceptable de los activos

#### 7.3.1.1 Uso general

- Los activos de información pertenecen al MHCP y el uso de los mismos debe realizarse exclusivamente con propósitos laborales.

#### 7.3.1.2 Utilización de computadores personales

- La instalación de software en los computadores suministrados por el MHCP y de los equipos conectados a la red corporativa es una función exclusiva del el CST. Toda instalación debe tramitarse a través de una solicitud al CST.

- 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.

- La SART mantendrá una lista actualizada del software estándar autorizado para instalar en los computadores. El CST solo instalará software estándar de acuerdo a la disponibilidad de licencias de uso.

- Para requerimientos de software no estándar, la SART debe realizar una evaluación de las vulnerabilidades de seguridad y soporte del software y solo si hay un concepto favorable se autorizará la instalación del software previa confirmación de la existencia de las respectivas licencias de uso legales.

- El traslado y movimiento de equipos (excepto los computadores portátiles) debe ser realizado por el l CST, la cual es responsable de mantener el inventario actualizado

- El almacenamiento en los discos duros de archivos de tipo videos, música, fotos o cualquier que no sean de carácter institucional queda prohibido.

- La información almacenada en los computadores debe ser manejada y protegida de acuerdo al nivel de clasificación definido.

#### 7.3.1.3 Utilización de Internet

- La navegación 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.

- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el enlace de Internet.

- No se permite acceso a páginas que transmitan música, videos o imágenes en línea o juegos.

- Los servidores no se les está permitido navegar a Internet.

#### 7.3.1.4 Utilización de correo electrónico y mensajería instantánea

- El correo electrónico debe ser utilizado con propósitos laborales.

- No se permite la opción de Relay de correo para equipos no autorizados

- La información con clasificación diferente a “Pública” no puede ser transmitida por e-mail a no ser que exista una autorización por parte del propietario de la información.

- No se permite el envío de cadenas de correo.

- No se permite el envío de correos 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.

- Los correos electrónicos deben contener la sentencia de confidencialidad con el siguiente contenido:

  *CONFIDENCIALIDAD: Este mensaje y cualquier archivo anexo son confidenciales y para uso exclusivo del destinatario. Esta comunicación puede contener información protegida por derechos de autor. Si usted ha recibido este mensaje por error, equivocación u omisión queda estrictamente prohibida la utilización, copia, reimpresión y/o reenvío del mismo. En tal caso, favor de notificar de forma inmediata al remitente y*

*borrar el mensaje original y cualquier archivo anexo. GRACIAS*

*"CONFIDENTIALITY: This message and any attached file is confidential and for exclusive use of its receiver. Law could protect this comunication. If you receive this message by error, mistake, or omission, it is strictly prohibited its use, copy, print and/or resend it. In that case please notify immediately the sender and delete completely this message and any attached file. THANK YOU"*

#### 7.3.1.5 Utilización de servicios de red

- 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.

#### 7.3.1.6 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.

### 7.4 Clasificación de Información

- La información debe ser protegida en proporción directa a su nivel de sensitividad, sin importar donde resida, su forma, que tecnología fue usada para manejarla y el propósito para el que ella existe. Se debe revisar este nivel de clasificación al menos una vez al año.

- La información del MHCP debe ser clasificada en términos del valor, de los requisitos legales y de su sensibilidad e importancia para la entidad, de acuerdo al esquema de clasificación adoptado por la Entidad en este documento; en el cual se definen cinco (5) niveles de clasificación: pública, de uso interno, restringida y crítica.
  Esta política establece un esquema de clasificación de información de la siguiente forma:

**Tabla de clasificación de información**

| Clasificación | Características |
|---|---|
| **Pública** | Ésta información ha sido explícitamente aprobada por el MHCP para su diseminación pública.<br><br>Los ejemplos incluyen, boletines de noticias, informes de prensa, entre otros.<br><br>**Transporte**: Mediante cualquier medio normalmente utilizado por Min Hacienda.<br><br>**Almacenamiento**: Usualmente esta información es transitoria, por lo tanto se almacenará una copia controlada dentro de la Entidad usando diferentes medios de almacenamiento. |
| **De uso Interno** | Se espera que la revelación o divulgación de esta información, no cause daños serios al MHCP, y su acceso es libre para los funcionarios de la Entidad a través de la intranet.<br><br>Los ejemplos incluyen el directorio de la organización y los calendarios de los empleados.<br><br>**Transporte**: Se puede transportar por cualquier medio que forme parte de la infraestructura tecnológica INTERNA de la entidad.<br><br>**Almacenamiento**: Se mantendrá dentro de los confines de la Organización, física o lógicamente. |
| **Restringida** | Este tipo de información sólo podrá tener acceso su propietario o el grupo al cual pertenece éste y además es de uso exclusivo interno de la organización.<br><br>Los ejemplos pueden ser información personal o reportes realizados por un área específica de la entidad, hojas de vida, historias clínicas.<br><br>**Transporte**: Se debe llevar esta información dentro de los medios designados por propietario de la información y se solicitará acuse de recibo si el destinatario no pertenece a dicha área.<br><br>**Almacenamiento**: Se mantendrá almacenada en los medios designados por el propietario de la información. Solo tendrán acceso los funcionarios explícitamente autorizados |

| Clasificación | Características |
|---|---|
| **Crítica** | La divulgación no autorizada de esta información puede afectar considerablemente el cumplimiento de la misión funcional. El acceso a esta información debe ser estrictamente restringido, basándose en el concepto de "necesidad de saber". La revelación o divulgación de esta información, requiere la aprobación de su respectivo propietario y en el caso de terceros, el acuerdo de confidencialidad debe ser debidamente firmado entre la Entidad y el tercero.<br><br>La información debe ser manejada con todas las precauciones y controles posibles, determinando de esta manera exactamente que personas tienen acceso, además de vigilar su uso, transporte y almacenamiento.<br><br>Ejemplos de información con carácter crítico, Restructuración de planta de funcionarios, planes de privatización, etc.<br><br>Esta es también la clasificación por defecto para la información que no tiene una designación específica.<br><br>**Transporte**: Es obligatorio transportar esta información usando medios seguros, encriptados y siempre se debe considerar acuses de recibo.<br><br>**Almacenamiento**: Se mantendrá cifrada en un medio protegido con controles de acceso o bajo llave (acceso sólo al propietario) |
| **Privilegiada** | Es la información que estando en conocimiento de funcionarios del MHCP sea utilizada de forma indebida para beneficiarse a titulo personal o de terceros.<br><br>La información debe ser manejada con todas las precauciones y controles posibles, determinando de esta manera exactamente que personas tienen acceso, además de vigilar su uso, transporte y almacenamiento.<br><br>Ejemplos de información con carácter Privilegiada: planes de compra, proyectos de adquisición.<br><br>Esta es también la clasificación por defecto para la información que no tiene una designación específica.<br><br>**Transporte**: Es obligatorio transportar esta información usando medios seguros, encriptados y siempre se debe considerar acuses de recibo.<br><br>**Almacenamiento**: Se mantendrá cifrada en un medio protegido con controles de acceso o bajo llave (acceso sólo al propietario) |

- La clasificación de la información aplica para toda la información en posesión o bajo el control del MHCP y también a la información que sea recibida desde terceros, esta información estará en una de las cuatro (4) categorías estipuladas en este documento. Se espera de todos los funcionarios que protejan la información proveniente de terceros con la misma dedicación y cuidado que se haría con la perteneciente al MHCP.

- Cuando la información del MHCP sea utilizada, procesada o accedida 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.

- La información que sea catalogada como “restringida” y “Crítica” que requiera ser transmitida por medios de comunicación públicos debe utilizar un esquema de cifrado con el fin de proteger su confidencialidad.

## 7.5 Seguridad del Recurso Humano

### 7.5.1 Roles y responsabilidades

#### 7.5.1.1 Oficial de Seguridad de la Información

NOTA: Este rol está incorporado en estas políticas obedeciendo a las buenas prácticas en Seguridad y a Lineamientos del Estado; sin embargo, a la fecha de revisión de estas políticas no se ha formalizado aún. Parte de las funciones propuestas las desempeñan los responsables de la Seguridad de la Información del Proceso APO 1.3 Gobierno y Gestión de TIC.

Responsable por preservar, mantener y gestionar la seguridad de los activos de información de la Entidad; dentro de sus funciones esta:

- Definir y establecer las políticas de seguridad de la información.
- Coordinar la implementación de las políticas de seguridad de la información con los diferentes procesos del MHCP.
- Reportar a la alta dirección el estado de la seguridad de la información de la Entidad.
- Definir e implementar la estrategia de divulgación y concientización de Seguridad de la Información para todos los funcionarios y terceros que tengan acceso a los activos de información del MHCP.
- Medir la eficiencia de los controles de seguridad implementadas.
- Hacer una gestión de seguridad de la información que permita mantener la seguridad en niveles razonables.

- Definir y actualizar normas, procedimientos y estándares dentro del SGSI
- Validar la arquitectura de seguridad en todos los ambientes (Desarrollo, Pruebas, Producción, Contingencia y cualquier otro que se requiera).
- Realizar el análisis de riesgo de seguridad de la información
- Evaluar, seleccionar y sugerir la implantación de herramientas que faciliten la labor de seguridad y contingencia.
- Recibir capacitación en seguridad de la información.
- Coordinar estudios de penetración y pruebas de seguridad en todos los ambientes (Desarrollo, Pruebas, Producción, Contingencia y cualquier otro que se requiera).
- Investigar sobre nuevos productos y tecnología de seguridad en todos los ambientes (Desarrollo, Pruebas, Producción, Contingencia y cualquier otro que se requiera).
- Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio.
- Revisión y seguimiento regular de los informes de incidentes sobre seguridad generados por el sistema, analizando las posibles incidencias ocurridas desde la última revisión de los mismos.
- Responsable de adelantar campañas de concientización en temas de seguridad de la información.
- Diseñar alarmas, controles destinados a proteger la confidencialidad y/o acceso adecuado a la información.
- Establecimiento de técnicas de control y evaluación de incidencias que puedan afectar a la seguridad de la información.
- Fomentar la coordinación entre los procesos del MHCP implicadas en el logro de un nivel apropiado de seguridad de la información.

#### 7.5.1.2 Funcionarios

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

#### 7.5.1.3 Usuarios de los sistemas

Los usuarios de los sistemas sean funcionarios, o terceras parte, que hacen uso de los servicios o sistemas de información del MHCP son responsables de dar un uso apropiado a los activos conforme a lo establecido en el “Código Único Disciplinario, ley 734 de 2002” y a las Políticas de Seguridad establecidas.

#### 7.5.1.4 Terceras partes

Las terceras partes que tengan acceso a los activos de información, están obligados a cumplir las políticas de Seguridad de la Información del MHCP, y tienen las mismas responsabilidades que los usuarios de los sistemas

#### 7.5.1.5 Administradores de los sistemas

Los administradores de los diferentes sistemas deben en forma activa implementar las medidas técnicas y procedimientos para brindar un nivel apropiado de seguridad de la información, de acuerdo a las políticas de seguridad de la información del MHCP.

#### 7.5.1.6 Directores, Subdirectores, Jefes de Oficina o Coordinadores de Grupo

Los funcionarios que tengan personas a cargo, son responsables que ellos conozcan, acepten y cumplan las políticas de seguridad de la información. De igual forma es su deber reportar cualquier incidente de seguridad del que tenga conocimiento, por los medios y formas establecidos para ello.

#### 7.5.1.7 Subdirección de Recursos Humanos

Esta área tiene dentro sus funciones realizar la revisión de requisitos para proceder a la posesión como servidor público. Como parte de la función de selección se debe realizar una verificación de los antecedentes y referencias de los candidatos.

#### 7.5.1.8 Oficina de Control Interno

Esta Oficina es la responsable de velar por el cumplimiento de las políticas definidas por el Ministro de Hacienda y ejercer control sobre la gestión y actividades que adelanten las dependencias del MHCP de acuerdo a lo definido en el Sistema de Control Interno.

### 7.5.2 Proceso disciplinario

- Todo incidente de seguridad en los activos de información en los que estén involucrados funcionarios, debe ser investigado por la Oficina de Control Interno Disciplinario de la Entidad, para establecer responsabilidades e imponer las sanciones previstas en la normatividad a este respecto, para ello contará con el apoyo técnico de la Dirección de Tecnología o del Oficial de Seguridad de la Información, en el caso que exista.

- En los incidentes de seguridad de la información en los que estén involucrados terceras partes, que sean reportadas a la Dirección de Tecnología, , serán informados por ésta, de forma inmediata, al Comité de Seguridad de la Información, el que a su vez informará a la Oficina Jurídica para el inicio de las acciones judiciales pertinentes, si es el caso.

### 7.5.3 Responsabilidades en la terminación

**Para los funcionarios**

- La subdirección de recursos humanos es el área encargada de realizar las gestiones necesarias para los traslados o finalización de las relaciones laborales.

- La subdirección de Recursos Humanos es responsable por generar las comunicaciones respectivas para informar a las otras áreas de los traslados o retiros de los funcionarios para que se proceda con las gestiones pertinentes.

- Los directores de Área son los responsables de gestionar la recepción de las actividades y procesos a cargo de los funcionarios que tramitan retiros o traslados de los cargos.

- Las actividades correspondientes a la finalización de las relaciones laborales deben realizarse oportunamente y estar culminadas a más tardar la fecha de culminación de actividades.

- El funcionario 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 las áreas de : Tecnología, Servicios, jefe inmediato, Jano y Recursos humanos.

**Para Terceras Partes**

El supervisor de contrato es el responsable por realizar de forma oportuna las gestiones correspondientes a la finalización de las actividades por parte de los miembros pertenecientes a un contratista o la finalización del contrato

### 7.5.4 Devolución de activos

Los activos asignados a los funcionarios 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 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 las áreas de: Tecnología, Servicios, jefe inmediato, Sistema de Correspondencia de la entidad y Recursos humanos.

**7.5.5** Retiro de los derechos de acceso

- Cuando un funcionario termine su relación laboral o cuando un miembro terceras partes finalice su relación contractual, se debe retirar las cuentas de acceso y devolución de los activos asignados.
- Los usuarios deben diligenciar el formato de entrega de cargo y obtener la firma de los responsables de las diferentes dependencias del MHCP.
- Los accesos lógicos a los activos de información deben ser removidos por los administradores de sistemas de forma inmediata y las cuentas de acceso deben colocarse en estado inactiva.
- La tarjeta de acceso físico debe ser devuelta a la subdirección de servicios, donde se retirarán los accesos.
- El funcionario o terceras partes no podrá extraer información de propiedad del MHCP.
- La subdirección de Recursos Humanos debe enviar un listado de las novedades de retiro del MHCP mensualmente y esta información debe ser revisada por los diferentes administradores del sistema y administradores funcionales para eliminar las cuentas de acceso.
- Los activos informáticos deben ser reintegrados en las mismas condiciones en las cuales se entregaron al funcionario.
- Los encargados de infraestructura de tecnología deben actualizar el inventario de hardware para registrar el activo como disponible.
- Antes de la asignación de un equipo que perteneció a un funcionario retirado se debe hacer limpieza de la información ahí almacenada, cumpliendo con lo establecido en el capítulo “Reutilización de discos duros del ATP 06 – Gestión de Comunicaciones y Operaciones””.
- Es responsabilidad de los Directores, Subdirectores o Coordinadores de Grupo notificar a la división de Gestión Humana el retiro de cualquier funcionario.
- Es responsabilidad de los supervisores o interventores de contratos, informar la finalización de cualquier contrato con terceras partes a los jefes de las dependencias propietarias de servicios informáticos que utilizaba el contratista.

## 7.6 Seguridad física y ambiental

**7.6.1** Seguridad del perímetro y control de acceso físico a zonas restringidas

El acceso físico a las zonas restringidas debe contar con mecanismos de control para evitar ingreso no autorizado, los mecanismos deben contener al menos:

- Sistemas de barreras o puertas contraídas con tarjetas de aproximación personalizadas.
- Las tarjetas de aproximación deben ser programadas basadas en roles de forma que se pueda habilitar el acceso solo a las áreas o pisos requeridos.

- Los visitantes deben registrarse en la recepción donde se lo identificará y se asignará una tarjeta para ingresar al edificio. La tarjeta debe ser regresada al abandonar el edificio.
- Los visitantes deben portar la tarjeta que lo identifica como visitante en un lugar visible y deben permanecer acompañados por un funcionario.
- Las zonas restringidas como centro de cómputo deben contar con mecanismos de control biométrico y monitoreo con CCTV.
- Las zonas restringidas deben contar con monitoreo con CCTV y con control de acceso.
- El acceso físico debe contar con horarios permitidos de ingreso al personal.
- Los ingresos en horarios adicionales deben ser solicitados por el Director del área solicitante a la Oficina de Seguridad del Ministerio mediante correo electrónico.
- Las tarjetas de acceso son de carácter personal e intransferible
- La perdida o hurto de las tarjetas de aproximación debe ser notificada inmediatamente a la oficina de Seguridad física.

**7.6.2** Seguridad en las oficinas y salas

**Oficinas**

- El acceso a las oficinas debe controlarse con un sistema de puertas de acceso controladas por tarjetas de aproximación.
- Los funcionarios y terceras partes deben tener la precaución para evitar facilitar el acceso a las diferentes áreas de personal que no posee la tarjeta de acceso respectiva.
- Los usuarios deben aplicar el concepto de “escritorios limpios” , para mayor información ver “PL 06 Operaciones y comunicaciones”

**Salas**

- Los asistentes a las salas de reuniones deben tener la precaución de no olvidar en las mismas, información de carácter “restringido” o “critico”.
- El responsable por la reserva de la sala debe revisar al finalizar la reunión que no quede material de carácter “restringido” o “critico”.

**7.6.3** Áreas públicas, de entrega y carga.

**Áreas Públicas**

- Se consideran áreas públicas las siguientes (ya sea que estén ubicadas en el Edificio de San Agustín o en Casas de Santa Bárbara): Pasillos de acceso en pisos
- Recepciones Edificio San Agustín (carreras 7 y (9 y Sede casas de Santa Bárbara (Carreras 7 y 6),
- Vestíbulos de ascensores
- Zonas de atención al público: Oficina de atención al cliente.
- Direcciones, Subdirecciones y Oficinas que prestan servicios al público:
  - Oficina de Bonos Pensionales
  - Subdirección de Servicios
  - Grupo de Contratos
  - Dirección de Apoyo Fiscal
  - Dirección de Regulación Económica de la Seguridad Social
  - Dirección General de Presupuesto Público Nacional

- El público en general solo puede ingresar a las áreas públicas en los horarios establecidos para el público previa autorización del funcionario respectivo
- El público debe registrar su ingreso a las instalaciones en porterías los torniquetes de acceso localizados en el Edificio de San Agustín (carrera 7, carrera 8 o en la recepción de la puerta de carga.) y/o en la Sede de Casas de Santa Bárbara.
- Las políticas de seguridad física deben ser aplicadas tanto para el acceso al edificio “San Agustín”, como a la “Sede Casas de Santa Bárbara”, lo que incluye acceso de otras entidades.
- El público no puede ingresar a áreas que no sean de carácter público.
- No se permite acceso de personal armado a las oficinas.

**Áreas de Correspondencia**

- Las zonas de entrega de información deben estar ubicadas en zonas de acceso público en general.
- El acceso a las áreas de entrega solo se permitirá en los horarios establecidos para ello.
- La correspondencia en general será revisada por medio de dispositivos de rayos X.

- Las zonas de correspondencia deben estar ubicadas con acceso directo desde el exterior.

**Áreas de Carga**

- El acceso a las áreas de carga debe hacerse sin utilizar zonas típicamente de tránsito de funcionarios o de acceso público.
- Las actividades de carga en general serán realizadas por acceso directo desde el exterior.
- Las zonas de carga estarán vigiladas con CCTV.
- El acceso a las áreas de entrega solo se permitirá en los horarios establecidos para ello.

### **7.6.4** Seguridad de los Equipos Fuera de las Instalaciones del MHCP.

Para los equipos fuera de las instalaciones se debe suministrar un nivel mínimo de seguridad que al menos cumpla con los requerimientos internos teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior del MHCP.

Se debe prestar especial atención a los dispositivos, tales como: computadores portátiles, PDA, discos extraíbles, memorias USB y en general todo dispositivo que contenga información.

- Tecnologías de cifrado para la información residente en el disco duro.
- Guaya de seguridad para estadías en hoteles y centros de convenciones.
- Contraseña en la BIOS del sistema.
- Maletín que no se parezca a los típicamente usados para el transporte de equipos portátiles.
- Mantener un cuidado especial en los aeropuertos, restaurantes etc. y por ninguna razón dejar el equipo desatendido.
- Utilizar todas las recomendaciones definidas en las políticas de seguridad sobre contraseñas y controles de acceso lógico.
- Pólizas de seguro.
- Los equipos utilizados para eventos y actividades externas no debe poseer almacenada información “restringida” o “crítica”

### **7.6.5** Ingreso y Retiro de Activos de Información de Terceros

- El retiro e ingreso de todo activo de información de propiedad de los funcionarios del Ministerio, utilizados para fines personales 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.

### **7.6.6** Traslado de Activos de Información

El traslado entre dependencias de la Entidad de todo activo de información, es autorizado por el Jefe de la Dependencia origen, y ejecutado por los funcionarios del Centro de Servicios Tecnológicos - CST con copia al Grupo de logística y suministros y a la Dirección de Tecnología.

## 7.7 Gestión de Comunicaciones y Operaciones

### **7.7.1** Gestión del Cambio

- Cualquier cambio a la plataforma tecnológica del Ministerio deberá ser completamente documentado y controlado a través del proceso de gestión de cambios. Ver " **Proceso de Gestión de Cambios (Intranet).**

- Todos los cambios en el ambiente de producción deberán ceñirse a las regulaciones establecidas por la Dirección de Tecnología para la adecuada puesta en producción, Ver "**Proceso de Gestión de Cambios (Intranet)"**

- Los cambios deben claramente detallar las actividades previas, las actividades durante el cambio, las actividades posteriores al cambio y las actividades en caso de regreso del cambio ("Rollback").

- Los Administradores de los sistemas o Coordinadores de Grupo que originan el cambio, son los responsables de presentar el cambio y coordinar todas las actividades para su ejecución.

- Los cambios que se lleven a cabo deben ser evaluados y probados de forma integral y se debe contar con una participación de los administradores de los diferentes componentes de la solución.

- El proceso de Gestión de Cambios debe considerar los niveles de servicio y las necesidades del Negocio del Ministerio.

- El proceso de Gestión de Cambios debe incluir la identificación de los riesgos asociados al cambio y las acciones de corrección.

**7.7.2** Protección contra código malicioso y código móvil

- Los usuarios no pueden instalar ni utilizar software sin la debida autorización de la Dirección de tecnología.
- El MHCP contará permanentemente con las herramientas de protección a nivel de red y de Computadores Personales contra código malicioso que será administrado por la Dirección de Tecnología.
- Todos los equipos de funcionarios y terceras partes que se conecten a la red LAN o a la WI-FI del MHCP deben tener instalado el antivirus actualizado y cumplir con las mejores prácticas establecidas por el Ministerio con respecto al uso del antivirus.
- Es responsabilidad de cada funcionario o tercero, revisar que todos los medios extraíbles sean chequeados con un antivirus provisto por la Entidad antes de procesarlos en los computadores personales o servidores de la Entidad.
- Es responsabilidad del administrador de Antivirus mantener en estado óptimo de funcionamiento (configuración, actualización, licenciamiento) las herramientas y procedimientos que permitan prevenir, detectar y corregir incidentes por código malicioso.
- Es responsabilidad del administrador del Directorio Activo distribuir los parches de seguridad a los equipos del dominio.
- El antivirus debe ser configurado desde la consola para que diariamente realice escaneo de detección de código malicioso y reportar a la consola de Antivirus.
- Los equipos que reporten código malicioso o virus serán aislados de la red LAN y de la WI-FI, hasta tanto sea remediado y se implementen los controles de protección.

**7.7.3** Mensajería electrónica

- El uso del correo electrónico suministrado por el Ministerio debe ser exclusivo para propósitos laborales.
- El acceso a los buzones de correo electrónico debe estar controlado por contraseña.
- La información clasificada como confidencial debe ser cifrada antes de ser transmitida por correo electrónico.
- Los correos electrónicos que vengan de personas desconocidas deben ser tratados con precaución.

- Asegurar qué en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a las personas apropiadas.

- El uso de programas de mensajería instantánea de carácter público como Messenger, ICQ, etc., no está permitido.

- No se deben abrir los archivos anexos a los correos electrónicos, cuyo origen es desconocido o el mensaje no tiene una relación con las actividades del MHCP.

- No se permite el uso de cuentas de correo públicas, tales como Hotmail, Yahoo, Gmail, etc., en los equipos de cómputo del MHCP, salvo excepciones que se autoricen específicamente.. Tampoco se permite el envió de información del MHCP a través de cuentas de correo públicas o personales.

## 7.8 Control de Acceso

### 7.8.1 Registro de usuarios

- Las cuentas de usuario de acceso deben ser individuales e intransferibles, no está permitido el uso de cuentas de grupo.

- Las cuentas pertenecientes a usuarios que ya no laboren para el MHCP o de terceros que finalicen sus actividades, deben ser retiradas de todos los sistemas de forma inmediata.

- Las cuentas de usuario son de carácter personal y no pueden ser compartidas a otros usuarios.

- Las acciones ejecutadas con las cuentas de usuarios, son responsabilidad del propietario de la cuenta.

- Los usuarios por cada sistema deben poseer una única cuenta de usuario.

- La asignación de cuentas o identificadores de usuario se debe realizar bajo el estándar para nombrar usuarios del MHCP.

### 7.8.2 Administración de Contraseñas de Usuarios Finales.

- La contraseña es de carácter personal e intransferible, no debe compartirse o ser revelada a otros. El hacerlo expone al propietario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Las contraseñas predefinidas que traen los elementos nuevos tales como Servidores, Bases de Datos, Aplicaciones, Routers, Switches, etc., deben cambiarse inmediatamente al poner en servicio el equipo.

- Se deben definir los parámetros de control de contraseñas en los sistemas que los permitan que consideren lo siguiente:

  a) **Composición.** La composición de una contraseña dependerá de los dispositivos que interactúan en el intercambio de dicha información, cómo y donde será guardada la contraseña y de cómo se comparará con la información que se provea al sistema. Adicionalmente, debemos analizar la selección de caracteres definiendo la extensión del número de posibles contraseñas que puede validar el sistema.

  Se debe definir cada uno de los posibles caracteres que podrán ser usados en la creación de la secuencia. Las posibilidades son (0-9), (a-z), (A-Z), caracteres especiales.

  b) **Tamaño.** El tamaño está relacionado con la composición, y define el universo de todas las posibles alternativas de la secuencia de caracteres. Se debe definir de acuerdo a 2 variables. La primera tiene que ver con el tamaño del universo de las posibles contraseñas y la segunda dependerá de la entidad, ya sea usuario o proceso, que debe recordar la secuencia de caracteres.

  En la actualidad, con el poder de procesamiento de los equipos de cómputo, como mínimo se debe definir una contraseña de tamaño mínimo de 8 caracteres.

  c) **Tiempo de Vida.** El tiempo de vida se debe analizar de acuerdo a múltiples variables: tamaño de la contraseña, número de veces que se utiliza, riesgo de compromiso, riesgo asociado a la distribución, costo de reemplazo de contraseña, entre otras.

  Se debe tener en cuenta que la contraseña más segura es aquella que solo puede ser utilizada una vez. En la actualidad una contraseña de 8 caracteres debe ser modificada cada 30 días.

  d) **Fuente de Generación:** Se debe tener en cuenta el método de selección de contraseñas, a los usuarios se hace necesario educarlos con el fin de proveerle las herramientas para generar sus contraseñas. Cuando se utiliza la generación de contraseñas por medio de un sistema, debemos garantizar que el método de selección no sea predecible.

  e) **Propiedad:** Una contraseña personal debe ser de propiedad individual con el fin de proveer seguimiento y trazabilidad de las acciones a un único

usuario. Por ningún motivo se debe proveer credenciales iguales a un grupo de personas.

f) **Distribución:** Las contraseñas deben ser distribuidas de una forma segura, entre el sistema, el usuario y el servicio de autenticación. Todos los usuarios deberán acceder por primera vez al sistema, con el fin de garantizar la identidad debemos proveer una primera cadena de caracteres la cual debe ser modificada para activar la cuenta. Esta primera contraseña deberá ser entregada de forma escrita, y debería ser conocida únicamente por el sistema y el usuario. Nunca se debe transportar la contraseña ni información que pueda revelar o dar indicios de la contraseña.

La primera contraseña puede entregarse mediante correo electrónico garantizando un tiempo límite de cambio de contraseña y activación de la cuenta. El proceso de autenticación no debería intercambiar información que pueda provea las capacidades de inferir o asociar la contraseña. En la actualidad el mejor método es el desafío.

g) **Resguardo:** Las contraseñas deben resguardarse en el sistema de autenticación de una forma que minimice la exposición y el reemplazo no autorizado.

h) **Entrada:** Se debe garantizar una forma segura de ingreso de la cadena de caracteres al sistema, evitar el riesgo de detección de la contraseña mediante técnicas como “shoulder-surfing”, “wiretapping”, “keyloggers”, entre otros.

**i) Características específicas de contraseña para SIIF –NACIÓN:**

1. Debe tener fecha de expiración cada 30 días
2. Un historial de contraseñas de 5
3. Se bloqueará la cuenta después de 3 intentos fallidos de conexión (A nivel de autorización, no del Active Directory)
4. Contener entre 8 y 10 caracteres.
5. Contener al menos tres de los siguientes cuatro tipos de caracteres*:*

- Mayúsculas: A, B, C, D, E, ... Z
- Minúsculas: a,b,c,d,e, ... z
- Números arábigos: 0,1,2,3, ... 9
- Caracteres especiales como símbolos de puntuación: , ; : * @ # $ % ^ & entre otros
- No se debe permitir repetir caracteres (e.g. aaa,111)
- No se debe permitir usar números o letras consecutivos
- No se debe permitir secuencias de teclado (e.g. qwertyuio)

- Cuando el CST asigne cuentas de usuario asigne una nueva contraseña, el propietario la utilizará solo en el primer inicio de sesión. En los subsiguientes es obligatorio realizar el cambio de contraseña para garantizar que solo él la conoce.
- Cuando el software lo permita, la Dirección de tecnología limitará a 3 el número de intentos fallidos, luego de lo cual la cuenta quedará deshabilitada y el usuario deberá solicitar su desbloqueo

**7.8.3** Responsabilidades de los usuarios

**7.8.3.1 Uso de la contraseña**

- Las contraseñas son de carácter personal e intransferible.
- Las acciones y operaciones realizadas con las cuentas de usuario son responsabilidad del propietario de la cuenta.
- Los usuarios deben cumplir con las buenas prácticas en la selección y el uso de las contraseñas, estas prácticas se describen en el numeral 4.2.3 Administración de Contraseñas de Usuarios Finales.

**7.8.3.2 Equipo de usuario desatendido**

- En los Servidores Windows se debe habilitar el control automático de bloqueo con contraseña, para las sesiones que permanecen más de cinco (5) minutos inactivas.
- En las estaciones de trabajo Windows se debe habilitar el control automático de bloqueo con contraseña, para las sesiones que permanecen más de tres (5) minutos inactivas.
- Los usuarios deben evitar dejar sus estaciones de trabajo con la sesión abierta.
- Los sistemas de información deben tener configurado la desconexión automática de sesión por inactividad de más de diez (10) minutos.

**7.8.3.3 Política de escritorio y pantalla despejados**

Los funcionarios del MHCP deben adoptar la cultura de “escritorio despejado” o “escritorio limpio” que consiste de los siguientes puntos:

- En los puestos de trabajo solo deben permanecer los documentos y elementos necesarios para la realización de la 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 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.
- Mantener organizado y en orden el puesto de trabajo
- No ingerir alimentos ni bebidas en el puesto de trabajo.
- 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.

**7.8.4** Computación móvil y de trabajo remoto

- El uso de los computadores móviles debe ser con propósitos laborales.
- El funcionario debe tomar copias de respaldo con una periodicidad diaria o semanal según la criticidad y el grado de actualización de la información que se desea preservar. Las copias de respaldo estarán protegidas contra alteración o pérdida.
- La información que tenga clasificación “crítica” o “restringida” NO debe almacenarse en los computadores portátiles, a menos que sea estrictamente necesario, para lo cual deben utilizarse mecanismos de encriptación bajo la autorización y el soporte de la Dirección de tecnología.
- Mantener la configuración establecida por la Dirección de Tecnología. (Ej.: mecanismos de protección antivirus y la activación de un firewall en el equipo portátil).
- El extravió o hurto de los equipos móviles deben ser reportados de forma inmediata, tanto al Grupo de Seguridad Física, como a la Dirección de Tecnología,, para realizar un diagnóstico del impacto de confidencialidad de la información contenida en el equipo.
- Evitar exponer el equipo a factores externos que comprometan su integridad, tales como humedad, humo y polución.

- Los equipos solo pueden ser conectados a redes que tengan corriente regulada.
- Llevar el portátil como equipaje de mano en los viajes de comisión.
- Evitar conectarse a redes públicas que puedan comprometer la información de la entidad.

---

## 7.9 Incidentes de Seguridad

### 7.9.1 Reporte sobre los eventos de Seguridad de la Información

- Los incidentes de seguridad se deben reportar al el CST, área que es responsable de asignar la categoría respectiva a seguridad y asignarlo al equipo respectivo de resolución. Ver “Apo.1.2.PRO.001 ST - Gestión de Incidentes.doc”
- Las investigaciones especiales adelantadas por los entes de control relacionadas con la Seguridad de la información deben ser notificadas a la Dirección de Tecnología
- Los incidentes de severidad grave deben ser reportados a la Dirección de Tecnología, donde se evaluará su impacto y se escalará a las áreas de control si así se requiere.

### 7.9.2 Reporte sobre las debilidades de seguridad

- Los funcionarios del MHCP, contratistas y usuarios del sistema que observen situaciones sospechosas o que claramente sean incidentes de seguridad de la información tienen la obligación de reportar los incidentes de seguridad, por los mecanismos definidos en el numeral 5.1.

## 7.10 Cumplimiento

### 7.10.1 Derechos de propiedad intelectual

El MHCP debe adoptar las medidas para garantizar que la Entidad y los funcionarios de la misma cumplen con los requisitos legales de los derechos de propiedad intelectual; para los mismos se definen las siguientes normas:

- Todo material utilizado por el MHCP que sea objeto de los derechos de propiedad intelectual, debe ser adquirido cumpliendo con los requisitos legales.

- Todo funcionario del MHCP y terceras partes, es responsable de garantizar que todo material utilizado con propósito laboral cumple con la legislación de derechos de propiedad intelectual.

- Está completamente prohibido que usuarios finales instalen programas de software en los computadores personales de la Entidad; esta función es exclusiva del personal de soporte de la Dirección de Tecnología.

- La Dirección de Tecnología debe tener un control de las licencias de los programas de software y velar porque no exista software sin la debida licencia de uso.

- Únicamente La Dirección de Tecnología puede tomar una copia con propósito de respaldo de los medios originales de los programas de software licenciados.

- La instalación por parte de funcionarios del MHCP o terceras partes de programas de software en los computadores personales de la Entidad sin la debida autorización es considerado como un incidente de seguridad.

- Las licencias de uso de los programas de software deben ser debidamente registradas ante el fabricante.

- Programas de software o información de terceras partes sujetas a derechos de autor que no contengan una autorización explícita del propietario no pueden ser instaladas en los activos del MHCP.

- Los funcionarios del MHCP y terceras partes, no pueden por ningún motivo descargar o almacenar archivos de música, fotos, vídeos, o material sujeto a propiedad intelectual en los equipos del MHCP.

- Los funcionarios del MHCP y terceras partes no pueden, por ningún motivo, descargar, instalar, almacenar o utilizar herramientas de software o hardware que puedan ser utilizadas para evaluar o comprometer los sistemas de seguridad de la información, a no ser que exista una autorización de la Dirección de Tecnología; ejemplo de estas herramientas son: crackers de software, software de descubrimiento de contraseñas, detección de vulnerabilidades o utilidades de encripción y desencripción.

- Toda información propietaria o confidencial de terceras partes que haya sido confiada al MHCP, debe ser protegida con los mismos controles que si fuera clasificada como restringida.

## 8 Documentos relacionados

- PL-01-01 Política de Seguridad
- PL 02 - Seguridad Organizacional
- PL 03 - Gestión de los activos de información
- PL 04 - Seguridad del personal
- PL 05 - Seguridad Física y Ambiental
- PL 06 - Gestion_Comunicaciones_Operaciones
- PL 07 - Control de Acceso
- PL 09 - Gestión de Incidentes
- PL 08 - Adquisición, Desarrollo y Mantenimiento de SI
- PL 09 - Gestión de Incidentes
- PL 10 - Gestión de la continuidad del negocio
- PL 11 – Cumplimiento
- GL - 01 Glosario políticas de seguridad de la información

## 9 Historial de Cambios

| FECHA | VERSIÓN | DESCRIPCIÓN DEL CAMBIO | ASESOR SUG |
|---|---|---|---|
| Diciembre – 1 - 2016 | 1 | Revisión para inclusión en el nuevo proceso de la DT de la versión entregada por la firma Digiware durante sus trabajos de consultoría realizados en el año 2008. | Derly Catherine Cifuentes Guerrero |
| Julio 15 2020 | 2 | Revisión ajustada con nuevas políticas e imagen visual | Liliana Parra Ramírez |

## 10 Aprobación

| ELABORADO POR: | REVISADO POR: | APROBADO POR: |
|---|---|---|
| **Nombre:** Digiware<br>**Cargo:** Contratista<br>**Dependencia** Tecnologia<br>**Fecha:** Junio de 2008 | **Nombre:** Alejandro Cruz Tello<br>**Cargo:** Asesor<br>**Dependencia:** Despacho<br>**Fecha:** Julio de 2020 | **Nombre:** Ricardo. Rios Rosales<br>**Cargo:** Director<br>**Dependencia:** Despacho<br>**Fecha:** Julio de 2020 |