# MANUAL SEGURIDAD DE LA INFORMACIÓN

Colombia Compra Eficiente

## AGENCIA NACIONAL DE CONTRATACIÓN COLOMBIA COMPRA EFICIENTE

## Tabla de contenido

## I. Introducción

El propósito de este manual es contar con un medio en donde se tenga documentado aspectos del Sistema de Gestión de Seguridad de la Información de acuerdo con el MSPI y con la Política de Seguridad de la Información aprobada por Colombia Compra Eficiente el 23 de mayo de 2016. El Manual de Seguridad describe la Política de Seguridad y Privacidad de la Información y especifica conductas, responsabilidades y restricciones que los funcionarios, contratistas y dependencias de Colombia Compra Eficiente deben cumplir.

Colombia Compra Eficiente tuvo en cuenta en el diseño del SGSI y de este manual: (i) el estándar internacional ISO27001 y las normas ISO27000, (ii) prácticas aceptadas de Seguridad de la Información y (iii) el Modelo de Seguridad y Privacidad de la Información del programa de Gobierno en Línea del Ministerio de Tecnologías de Información y las Comunicaciones.

## II. Objetivo

El Manual de Seguridad y Privacidad de la Información de Colombia Compra Eficiente define lineamientos para proteger sus Activos de Información contra pérdida de Confidencialidad, Integridad o Disponibilidad, de forma accidental como intencionada, especificando medidas organizacionales, técnicas y físicas definidas en la Política de Seguridad y Privacidad de la Información.

## III. Definiciones

- **Activo de Información.** Es la información que reside en medio electrónico o físico, que tiene un significado y valor para Colombia Compra Eficiente y por tanto requiere protección.
- **Acuerdo de Nivel de Servicio.** Es el estándar de calidad de la prestación de un servicio fijado por el proveedor del servicio y su cliente.
- **Confidencialidad.** Es el principio de la Seguridad de la Información que busca asegurar que la información de la entidad sea accedida únicamente por el personal autorizado para el efecto.
- **Cláusula de Confidencialidad.** Es la obligación establecida en un contrato para establecer las condiciones en las cuales la información que conozcan las partes con ocasión de la ejecución del contrato puede y debe ser divulgada.
- **Criptografía.** Conjunto de técnicas que buscan proteger u ocultar la información de observadores no autorizados.
- **Dato Personal.** Es cualquier tipo de dato que identifique o permita la identificación de una persona.
- **Disponibilidad.** Es el principio de la Seguridad de la Información que busca asegurar que la información sea accesible y utilizable cuando sea requerida.
- **Grupo de proyecto.** Es el grupo de trabajo definido por la Dirección de Colombia Compra Eficiente con un propósito específico y conformado por miembros de diferentes áreas de Colombia Compra Eficiente.
- **Incidente de Seguridad.** Es un evento inesperado y no deseado que compromete la Seguridad de la Información.

- **Información Confidencial**. Es la información que tiene restricciones para su uso y que puede estar etiquetada como "Clasificada" o "Reservada".
- **Integridad.** Es el principio de Seguridad de la Información para evitar su modificación o alteración y garantizar su consistencia, exactitud y completitud.
- **Plan de Continuidad de Negocio**. Es el plan para restaurar las funciones críticas de Colombia Compra Eficiente parcial o totalmente y recuperar sus Activos de Información, luego de una interrupción no deseada o un desastre.
- **Política de Seguridad y Privacidad de la Información**. Es el documento aprobado el 23 de mayo de 2016 que muestra el compromiso de Colombia Compra Eficiente con la Seguridad de la Información, define lineamientos y medidas organizacionales para garantizar la Seguridad de la Información.
- **Recurso Tecnológico.** Es cualquier medio tecnológico de Colombia Compra Eficiente.
- **Seguridad de la Información**. Es el conjunto de medidas que busca preservar la Confidencialidad, la Integridad y la Disponibilidad de la información.
- **SGSI.** Es el Sistema de Gestión de Seguridad de la información conformado por un conjunto de elementos, prácticas y procesos para implementar, operar, mantener y mejorar la Seguridad de la Información.
- **Sistema de Información**. Es el conjunto de elementos que interactúan para apoyar los objetivos de un negocio como por ejemplo la información, actividades, hardware, software entre otros.
- **Subdirección de IDT.** Es la subdirección de información y desarrollo tecnológico de Colombia Compra Eficiente.
- **Privacidad.** Es el ámbito de la vida privada de una persona, el cual debe mantenerse confidencial.
- **Mesa de Ayuda**. Es el grupo encargado de apoyar en administración y solución de problemas tecnológicos internos propios de Colombia Compra Eficiente.
- **Mesa de Servicio**. Área encargada de atender los requerimientos y solicitudes de todos los partícipes de la compra pública.
- **Backup.** Es la copia de respaldo de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Dato Personal privado.** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- **Dato Personal sensible**. Es aquel Dato Personal de especial protección, por cuanto afecta la intimidad del titular y su tratamiento puede generar discriminación.
- **Dato Personal semi-privado.** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general.

## IV. Contexto

Colombia Compra Eficiente fue creado por medio del Decreto Ley 4170 de noviembre 3 de 2011 con el objetivo de ser una entidad rectora en el sistema de compras que busca la eficiencia y transparencia en la Compra Publica. La misión de Colombia Compra Eficiente es:

- Ofrecer a los partícipes de la compra pública un sistema de información que permita hacer transacciones en línea, con instrumentos y herramientas que respondan a sus necesidades

y que ofrezca información suficiente y de calidad para tomar decisiones, y para cumplir las metas y objetivos de las Entidades Estatales, el Plan Nacional de Desarrollo y los planes territoriales de desarrollo, generando valor por dinero en la compra pública y confianza en el Sistema, promoviendo la competencia, la transparencia y asegurando el acceso a la información

- Formular políticas públicas encaminadas a cumplir los objetivos del Sistema de Compra Pública y ofrecer herramientas para su gestión y hacer análisis constante de la normativa vigente y su aplicación
- Asistir técnicamente y trabajar en equipo con los partícipes de la compra pública
- Apoyar el desarrollo del mercado de compra pública, y monitorearlo
- Analizar, evaluar y monitorear el comportamiento del Sistema de Compra Pública en busca de la innovación y mejora continua del mismo.

Teniendo en cuenta lo anterior, Colombia Compra Eficiente cuenta con los siguientes sistemas de información misionales que apoyan el sistema de Compra Publica:

- Secop: Sistema de información que permite la publicación de los procesos de compra realizados por las entidades públicas.
- SecopII: Sistema de información que permite realizar los procesos de contratación en línea.
- TVEC: Sistema de información que permite el proceso de compra de las entidades públicas mediante los acuerdos marco.
- Sintesis: Esta aplicación permite a las Entidades estatales la consulta de las normas, jurisprudencia y decisiones arbitrales sobre las compras públicas.

En ninguno de los anteriores sistemas de información, ni dentro de las funciones de Colombia Compra Eficiente, se maneja o se ejecutan transacciones monetarias de las demás entidades del estado. Siendo las anteriores aplicaciones solo herramientas que optimizan y permiten una transparencia y mayor participación en la compra pública.

Teniendo en cuenta lo anterior, la mayoría de la información que maneja Colombia Compra Eficiente es información pública. Y la información confidencial, en especial presentación de ofertas, reposa en los sistemas de información con controles de seguridad automáticos, los cuales se encuentran tercerizados con diferentes proveedores, dependiendo del sistema de información.

Adicional a los sistemas misionales, Colombia Compra Eficiente cuenta con sistemas de apoyo que se encuentran en el Centro de Datos localizado en las instalaciones de Colombia Compra Eficiente o en la nube privada o pública que Colombia Compra Eficiente tiene contratado. Sin embargo, estos son independientes a las plataformas misionales y por ende su indisponibilidad no afecta a los usuarios de las plataformas misionales.

Para más información sobre Colombia Compra Eficiente se puede consultar la página web colombiacompra.gov.co

## V. Manual de Seguridad y Privacidad de la Información

### 1. Seguridad de los recursos humanos

**Objetivos establecidos en la ISO 27001:**

- Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
- Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
- Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

**Conductas, responsabilidades y restricciones:**

**Selección de personal y contratación**

- La Secretaría General debe verificar la información suministrada por los candidatos a un cargo antes de su vinculación definitiva, tanto para las personas vinculadas laboralmente como para las vinculadas a través de contratos de prestación de servicios.
- La Secretaría General debe incluir en los contratos de prestación de servicios una Cláusula de Confidencialidad.
- Los funcionarios y contratistas de Colombia Compra Eficiente deben suscribir un documento de Aceptación de la Política de Seguridad de la Información en el cual manifiestan que conocen y aceptan la Política de Seguridad de la Información.
- La Secretaría General debe informar a la Subdirección de IDT la desvinculación o cambio de funciones de funcionarios o contratistas inmediatamente luego de que esta se produzca.

**Capacitación**

- El Plan Institucional de Capacitación de Colombia Compra Eficiente debe incluir un plan de capacitación de la Seguridad de la Información.
- El Oficial de Seguridad de la Información debe diseñar y liderar el programa de capacitación y sensibilización de la Seguridad de la información para funcionarios y contratistas de Colombia Compra Eficiente.
- Para los cambios de Roles, Se debe generar una capacitación sobre la documentación del SGSI con los nuevo funcionarios y contratistas y, en caso de ser necesario, realizar una actualización sobre esta.
- La Dirección de Colombia Compra Eficiente debe promover la participación de funcionarios y contratistas a las capacitaciones sobre Seguridad de la Información.

**Procesos disciplinarios**

- Secretaria General, en situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información, deberá tramitar el cumplimiento de la ley 734 de 2002 y demás normas externas e internas que reglamenten los procesos disciplinarios o sancionatorios para los funcionarios y contratistas de la Entidad.

## 2. Gestión de activos

**Objetivos establecidos en la ISO 27001:**

- Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
- Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
- Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

**Conducta, responsabilidades y restricciones:**

### Activos físicos y tecnológicos

- Los funcionarios y contratistas en el momento de su vinculación deben ser informados de los recursos tecnológicos que hay a su disposición y deben hacer uso adecuado, eficiente y de forma ética y en cumplimiento de las leyes y reglamentos vigentes.
- Los funcionarios y contratistas en el momento de su desvinculación de Colombia Compra Eficiente o en el momento de asumir nuevas funciones, deben entregar los Activos de Información a su cargo y los recursos tecnológicos que le fueron confiados durante su vinculación.
- Los funcionarios y contratistas de Colombia Compra Eficiente cuando deciden destruir o desechar documentos físicos deben asegurarse hacerlo de forma tal que no haya fuga de Información Confidencial.

### Identificación y clasificación de Activos de Información

- El propietario de un Activo de Información debe identificar y clasificar su información de acuerdo con la metodología establecida por Colombia Compra Eficiente.
- El oficial de Seguridad debe liderar el análisis de riesgos de Seguridad de la Información para definir las condiciones de uso y protección de los Activos de Información.
- Los propietarios de la información deben participar activamente en los análisis de riesgos de Seguridad de la Información.
- Los propietarios de los Activos de Información deben revisar periódicamente los controles de seguridad definidos para sus Activos de Información.
- Los activos de información pertenecen a Colombia Compra Eficiente y el uso de estos debe emplearse exclusivamente con propósitos laborales o contractuales, teniendo en cuenta su clasificación.

### Etiquetado de la información

- El Comité Directivo debe definir un esquema de etiquetado de la información el cual muestre el nivel de Confidencialidad de la información.
- Los funcionarios y contratistas deben etiquetar la información, tanto digital como física de acuerdo con la clasificación de Confidencialidad y siguiendo el esquema de etiquetado.

- Los funcionarios y contratistas deben utilizar las medidas apropiadas para proteger la información de acuerdo con su etiquetado. En consecuencia, deben imprimir o escanear documentos confidenciales cuando sea estrictamente necesario y verificar que no haya copias en las impresoras o en otros lugares, y en caso de encontrar copias recogerlas inmediatamente para evitar su divulgación no autorizada.

**Uso de recursos tecnológicos**

- La Secretaria General es el área encargada de autorizar movimientos y asignaciones, y definir el uso correcto de recursos tecnológicos de Colombia Compra Eficiente.
- La Subdirección de IDT es el área encargada de instalar, reparar o retirar cualquier componente de software o hardware de los recursos tecnológicos de Colombia Compra Eficiente.
- La Subdirección de IDT es el área encargada de borrar de forma segura, en los casos que sea necesario, el hardware de almacenamiento cuando sea reasignado, transferido o dispuesto a cualquier título.
- Los funcionarios y contratistas deben respetar la asignación de recursos tecnológicos.
- Los funcionarios y contratistas deben aceptar las condiciones e instrucciones definidas por la Subdirección de IDT y Secretaria General sobre el manejo de los recursos tecnológicos de Colombia Compra Eficiente.
- Los funcionarios y contratistas, ante una falla o problema de hardware o software en un Recurso Tecnológico de Colombia Compra Eficiente, deben informar el caso a la Mesa de Ayuda, quien es la responsable de la asistencia adecuada y, además, el funcionario o contratista debe abstenerse de solucionar directamente el problema.
- En caso de pérdida o robo de un Recurso Tecnológico, los funcionarios y contratistas deben informar inmediatamente al líder de la dependencia, a la Subdirección de IDT y a Secretaria General para que se inicie el trámite interno y debe poner la denuncia ante la autoridad competente, si es necesario.

**Dispositivos personales**

- La Subdirección de IDT debe establecer los lineamientos para que funcionarios y contratistas usen sus dispositivos personales para acceder a la información de Colombia Compra Eficiente y las reglas que estos deben aceptar y respetar para el efecto.
- Los funcionarios y contratistas deben evitar usar dispositivos móviles con acceso a la información de Colombia Compra Eficiente en lugares que no ofrezcan garantías de seguridad física para evitar pérdida o robo de estos y pérdida de la Confidencialidad de la información.

**Documentos relacionados:**

- Anexo - 10. Esquema de etiquetado de la Información
- Anexo - 4. Lineamientos para periféricos y unidades externas de almacenamiento
- Anexo - 5. Lineamientos para las estaciones de trabajo
- Anexo - 6. Lineamientos para el uso de dispositivos personales
- Anexo - 1. Lineamientos para el almacenamiento de información y Backups de usuario

## 3. Control de acceso

**Objetivos establecidos en la ISO 27001:**

- Limitar el acceso a información y a instalaciones de procesamiento de información.
- Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
- Evitar el acceso no autorizado a sistemas y aplicaciones.

**Conducta, responsabilidades y restricciones:**

### Identificación y autenticación individual

- La Subdirección de IDT debe garantizar que los equipos de cómputo de Colombia Compra Eficiente se puedan conectar a las redes de la entidad, usando los lineamientos definidos en los anexos de este documento.
- Los funcionarios y contratistas son responsables de sus credenciales de usuario y las acciones realizadas a partir de estas en las diferentes plataformas tecnológicas, servicios de red y sistemas de información de Colombia Compra Eficiente.
- Los funcionarios y contratistas no deben revelar o compartir sus credenciales de usuario.
- Los funcionarios y contratistas deben acoger los lineamientos para la configuración de contraseñas definidos por la Subdirección de IDT.
- Los funcionarios y contratistas deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario acogiéndose al procedimiento establecido para tal fin.

### Control y administración de acceso

- La Subdirección de IDT debe establecer controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no puedan tener accesos privilegiados a dichos recursos, servicios o sistemas.
- Los propietarios de los Activos de Información deben definir los perfiles de usuario y autorizar los permisos de acceso a dichos recursos.
- Los propietarios de los Activos de Información deben verificar los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a sus Activos de Información.

### Administración y monitoreo de usuarios de altos privilegios

- La Subdirección de IDT otorgará los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios y contratistas designados para dichas labores, entregando cuentas personalizadas a cada uno de los administradores.
- La Subdirección de IDT debe definir las medidas pertinentes que permitan el monitoreo de las cuentas privilegiadas en las diferentes plataformas tecnológicas.

### Acceso a la red inalámbrica

- Los funcionarios y contratistas deben acceder a la red inalámbrica interna de Colombia Compra Eficientes solo con equipos autorizados.
- Los funcionarios y contratistas no deben entregar las credenciales de acceso a la red inalámbrica de Colombia Compra Eficiente a visitantes o personas no autorizadas.
- Los funcionarios y contratistas que deseen conectar equipos a la red WIFI, distintos a los equipos laborales asignados por Colombia Compra Eficiente, deben conectarse únicamente a la red definida por la Subdirección de IDT.
- Visitantes podrán ingresar libremente a la red de Visitantes de Colombia Compra Eficiente siguiendo el proceso de registro definido por la Subdirección de IDT.

**Acceso remoto**

- La Subdirección de IDT debe implementar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de Colombia Compra Eficiente y restringir los accesos permitiendo únicamente al personal autorizado, de acuerdo con las labores desempeñadas.
- Los funcionarios y contratistas que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión y deben tomar las medidas pertinentes para asegurar dichas conexiones.

**Documentos relacionados:**

- Anexo - 7. Lineamientos para las contraseñas
- Anexo - 8. Lineamientos para el acceso a la red inalámbrica

## 4. Criptografía

**Objetivos establecidos en la ISO 27001:**

- Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

**Conducta, responsabilidades y restricciones:**

- La Subdirección de IDT debe verificar que todo Sistema de Información o aplicativo que requiera realizar transmisión de información clasificada o reservada, utilice mecanismos de cifrado para dicha actividad.
- La Subdirección de IDT establecerá los lineamientos de administración, protección y ciclo de vida de las llaves criptográficas

**Documentos relacionados:**

- Anexo - 11. Cifrado de sistemas de Información y/o Aplicativos
- Anexo - 12. Guía para el cifrado de la información y aplicación de Criptografía
- Anexo - 13. Lineamientos para la administración, protección y ciclo de vida de las llaves criptográficas

## 5. Seguridad física y del entorno

**Objetivos establecidos en la ISO 27001:**

- Prevenir el acceso físico no autorizado, el daño y la interferencia a la información a las instalaciones de procesamiento de información de la organización.
- Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

**Conducta, responsabilidades y restricciones:**

- La Subdirección de IDT y Secretaria General deben proveer las condiciones físicas y medioambientales necesarias para la correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo.
- El líder de infraestructura, el Subdirector de IDT o quienes ellos deleguen son los únicos que autorizan el acceso a personal no autorizado a los centros de cómputo, y deben llevar registro de ese ingreso en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Las salidas e ingresos de personal a las instalaciones de Colombia Compra Eficiente deben ser registrados; por consiguiente, los funcionarios y contratistas deben cumplir completamente con los controles físicos establecidos.
- Los funcionarios y contratistas deben portar el carné que los identifica como tales. En caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo inmediatamente a la Secretaría General.
- Los funcionarios y contratistas no deben ingresar a áreas a las cuales no tengan autorización.
- Los funcionarios y contratistas deben guiar a los visitantes para seguir el protocolo establecido de ingreso de visitantes.

### Escritorio y pantalla limpia

- Los funcionarios y contratistas deben velar por la seguridad en sus puestos de trabajo. Para ello, cuando dejen desatendido el puesto de trabajo, deben bloquear sus estaciones de trabajo, colocar la guaya en el caso de usar equipos portátiles y no dejar documentos visibles o dispositivos como medios extraíbles que pongan en riesgo la Seguridad de la Información.

**Documentos relacionados:**

- Anexo - 3. Lineamientos para el mantenimiento de los centros de cómputo

## 6. Seguridad de las operaciones

**Objetivos establecidos en la ISO 27001:**

- Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

- Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
- Proteger contra la pérdida de datos.
- Registrar eventos y generar evidencia.
- Asegurarse de la Integridad de los sistemas operacionales.
- Prevenir el aprovechamiento de las vulnerabilidades técnicas.
- Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

**Conducta, responsabilidades y restricciones:**

**Copias de seguridad**

- La Subdirección de IDT es el área encargada de definir y mantener los procedimientos de respaldo y las herramientas tecnológicas necesarias.
- La Subdirección de IDT debe definir y ejecutar los procedimientos de respaldo adecuados para la información de la compra publica
- Los funcionarios y contratistas son los encargados de realizar las copias de seguridad de su información mediante el mecanismo definido por la Subdirección de IDT.

**Código malicioso**

- Los funcionarios y contratistas no deben cambiar o eliminar la configuración de software de seguridad, como antivirus, en los equipos de cómputo.
- Los funcionarios y contratistas deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los funcionarios y contratistas que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para tomar las medidas de control correspondientes.

**Gestión de vulnerabilidades**

- La Subdirección de IDT debe revisar periódicamente la aparición de nuevas vulnerabilidades y generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en las plataformas tecnológicas.

**Documentos relacionados:**

- Anexo - 1. Lineamientos para el almacenamiento de información y Backups de usuario

## 7. Seguridad de las comunicaciones

**Objetivos establecidos en la ISO 27001:**

- Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

- Mantener la Seguridad de la Información transferida dentro de la organización y con cualquier entidad externa.

**Conducta, responsabilidades y restricciones:**

**Seguridad de los servicios de red**

- La Subdirección de IDT debe implementar los mecanismos de seguridad que considere pertinentes en la configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la entidad.

**Segregación de redes**

- La Subdirección de IDT debe segregar la red teniendo en cuenta la información, los usuarios y las plataformas tecnológicas y acogiendo las buenas prácticas de configuración que considere pertinentes.
- La Subdirección de IDT establecerá e implementará los controles de acceso y tráfico a las redes y subredes con el fin de mejorar su rendimiento y seguridad.
- La Subdirección de IDT debe procurar que la red para visitantes esté aislada de la red corporativa.

**Transmisión de información**

- Los funcionarios y contratistas que necesiten realizar o hacer envío de Información Confidencial fuera del ámbito de Colombia Compra Eficiente deben cifrar el contenido con el propósito de proteger su Confidencialidad e Integridad.
- La Subdirección de IDT definirá los procedimientos adecuados de intercambio de información entre las plataformas de Colombia Compra Eficiente con los sistemas de terceros.

**Uso de correo electrónico corporativo**

- Los funcionarios y contratistas en ninguna circunstancia deben utilizar una cuenta de correo institucional que no sea la suya. Los buzones de correo son propiedad de Colombia Compra Eficiente y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus labores.
- Los funcionarios y contratistas no deben enviar archivos adjuntos que contengan extensiones ejecutables, en ninguna circunstancia.

**Documentos relacionados:**

- Anexo - 11. Cifrado de sistemas de Información y/o Aplicativos

## 8. Adquisición, desarrollo y mantenimiento de sistemas

**Objetivos establecidos en la ISO 27001:**

- Asegurar que la Seguridad de la Información sea una parte integral de los sistemas de información durante todo el ciclo de vida.
- Asegurar que la Seguridad de la Información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
- Asegurar la protección de los datos usados para pruebas.

**Conducta, responsabilidades y restricciones:**

- La Subdirección de IDT debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La Subdirección de IDT debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de Colombia Compra Eficiente.
- La Subdirección de IDT debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- La Subdirección de IDT debe considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los sistemas de información, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores y gestores de aplicaciones de terceros deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada Sistema de Información que se quiera, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Los desarrolladores y gestores de aplicaciones de terceros deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores y gestores de aplicaciones de terceros deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores y gestores de aplicaciones de terceros deben certificar la transmisión de Información Confidencial por medio de canales seguros.
- Los desarrolladores y gestores de aplicaciones de terceros deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Los desarrolladores y gestores de aplicaciones de terceros deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores y gestores de aplicaciones de terceros deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema,

identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales deberían estar cifrados.
- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
- Los desarrolladores deben cumplir con los demás lineamientos establecidos y buenas prácticas que se hayan adoptado

## 9. Relaciones con los proveedores

**Objetivos establecidos en la ISO 27001:**

- Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
- Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

**Conducta, responsabilidades y restricciones:**

- La Secretaría General debe definir los modelos de Acuerdos de Confidencialidad o de Intercambio de Información entre Colombia Compra Eficiente y terceras partes. Dichos acuerdos deben prohibir la divulgación de la información entregada por Colombia Compra Eficiente a los terceros y la destrucción de dicha información una vez cumpla su cometido, al igual que los requisitos y clausulas asociadas al tratamiento de la información y su seguridad.
- Los propietarios de los Activos de Información deben verificar el cumplimiento de los Acuerdos de Confidencialidad o Acuerdos de intercambio establecidos.
- Los propietarios de los Activos de Información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

## 10. Gestión de Incidentes de Seguridad de la Información

**Objetivos establecidos en la ISO 27001:**

- Asegurar un enfoque coherente y eficaz para la gestión de incidentes de Seguridad de la Información, incluida la comunicación sobre eventos de seguridad y debilidades.

**Conducta, responsabilidades y restricciones:**

- El Comité Directivo debe brindar los recursos necesarios para una investigación adecuada de los Incidentes de Seguridad reportados, que permita identificar las causas, proporcionar soluciones y prevenir que vuelvan a ocurrir.
- El grupo de atención a incidentes debe evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares y escalar al Comité Directivo los que se considere pertinente.
- Los propietarios de los Activos de Información deben informar los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización por el medio definido.
- Los funcionarios y contratistas deben reportar a la Mesa de Ayuda cualquier evento o incidente relacionado con la información o los recursos tecnológicos con la mayor prontitud posible.
- En caso de conocer la pérdida o divulgación no autorizada de información definida como clasificada o reservada, los funcionarios y contratistas deben notificarlo a los propietarios de los activos.

**Documentos relacionados:**

- Anexo - 9. Lineamientos de Incidentes de Seguridad de la Información

## 11. Gestión de continuidad de negocio

**Objetivos:**

- La continuidad de Seguridad de la Información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.
- Asegurar la Disponibilidad de instalaciones de procesamiento de información.

**Conducta, responsabilidades y restricciones:**

- El Comité Directivo debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas, generando un Plan de Continuidad de Negocio.
- El Comité Directivo debe aprobar un plan de recuperación ante desastres para los casos que considere necesario y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para los servicios y Sistemas de Información que se incluyan.
- El Comité Directivo debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y continuidad de negocio, verificando la Seguridad de la Información durante su realización y la documentación de dichas pruebas.

- Los Dueños de procesos deben generar la documentación necesaria que podría ser utilizada en caso de un evento adverso, teniendo en cuenta la Seguridad de la Información. Estos documentos deben ser evaluados para garantizar su efectividad.
- La Subdirección de IDT debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos que determine la entidad.
- La Subdirección de IDT debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos del Colombia Compra Eficiente.

## 12. Cumplimiento

**Objetivos establecidos en la ISO 27001:**

- Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con Seguridad de la Información y de cualquier requisito de seguridad.
- Asegurar que la Seguridad de la Información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

**Conducta, responsabilidades y restricciones:**

- Los funcionarios y contratistas deben cumplir con las leyes de derechos de autor, por lo tanto, no deben duplicar contenido o software sin la autorización del propietario de los derechos de autor. La reproducción no autorizada es una violación de ley; no obstante, dependiendo de la licencia otorgada, se puede permitir su uso, copia o reproducción bajo escenarios específicos.

**Privacidad en Datos Personales**

- El Comité Directivo debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, contratistas, proveedores y demás terceros de Colombia Compra Eficiente de los cuales reciba y administre información.
- La Subdirección de IDT debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, contratistas, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
- Los funcionarios y contratistas que tengan bajo su custodia información con datos personales deben asegurar que a dicha información solo tendrán acceso aquellas personas que tengan una necesidad legítima y acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos.

## VI. Anexos

### 1. Lineamientos para el almacenamiento de información y Backups de usuario

Colombia Compra Eficiente define los siguientes espacios de almacenamiento y los lineamientos que deben seguir los funcionarios y contratistas de Colombia Compra Eficiente de la siguiente manera:

- Disco duro, instalado físicamente en el computador personal o en el portátil asignado a cada funcionario o contratista. Los Discos Duros tienen una capacidad de almacenamiento entre 500 Gigabytes 1 Terabyte dependiendo del tipo de equipo asignado.

  Este espacio es de uso libre para el funcionario o contratista, cumpliendo con la normatividad legal, en especial respetando los derechos de autor. La información que se encuentre allí contenida es responsabilidad del funcionario y contratista y por ende no se realiza ningún Backup a la información.

- Disco de internet (OneDrive), es el servicio de almacenamiento que presta Microsoft como parte de la suscripción de Colombia Compra Eficiente a las licencias de Office 365 y al cual se accede a través de Internet. El OneDrive tiene una capacidad de 1 Terabyte para cada funcionario o contratista que tenga una cuenta de Office 365 asignada.

  Este espacio de almacenamiento debe contener toda la información de trabajo. El usuario es responsable de tener y organizar su información en este espacio del almacenamiento. Al ser un espacio de almacenamiento en la nube, se garantiza la Disponibilidad y la Integridad ante cualquier borrado por parte del usuario. Se podrá recuperar un archivo hasta 30 días después de eliminado. El usuario mismo puede recuperar la información o solicitar ayuda a la Mesa de Ayuda para recuperar su información.

- Espacio colaborativo (Servidor Nube), es el servicio de almacenamiento que proporciona la Subdirección de IDT a todas las dependencias. El Director, Subdirector o Secretario encargado de cada dependencia será el encargado de la creación o eliminación de nuevos espacios colaborativos, especificando el grupo de personas que podrá tener acceso. En este espacio los funcionarios y contratistas podrán trabajar con las personas asignadas la información asociada al objetivo de cada carpeta. Adicionalmente, el espacio cuenta con una copia de respaldo diaria de los archivos, que permite recuperar las versiones de archivos de 1 día atrás y los archivos eliminados.

### 2. Lineamientos para el archivo electrónico de gestión documental

El archivo electrónico de gestión documental es el lugar donde reposan todos los documentos electrónicos de Colombia Compra Eficiente, siguiendo los lineamientos y estructura de las Tablas de Retención Documental. El archivo digital se encuentra en SharePoint, asignando una carpeta para cada proceso de la entidad.

Cada carpeta contará con un responsable asignado por el Director, Secretario General o Subdirector de su respectiva dependencia, quien se encargará de gestionar el manejo de este espacio, el cargue

de los documentos, los permisos necesarios que requiera y validar que la información en su carpeta este completa, terminada y acorde a los lineamientos definidos por el área de Gestión Documental.

Para la gestión de los permisos, el encargado de la carpeta podrá solicitar los permisos por medio de la plataforma, los cuales serán revisados por el área de Seguridad de la Información, para ser posteriormente aprobados o rechazados.

### 3. Lineamientos para el mantenimiento de los centros de cómputo

Con el fin de prevenir y mitigar cualquier riesgo de seguridad relacionado con los cuartos técnicos, Colombia Compra Eficiente define los siguientes lineamientos específicos:

- El cableado de red debe estar protegido contra daños o accesos no autorizados, Uno de los métodos para lograr estos es utilizando mallas metálicas de protección y evitando la exposición de dispositivos de red en áreas de acceso público.
- Con el fin de evitar la interferencia, los cables de energía y de datos deben estar separados entre sí.
- Las puertas deben asegurarse y cerrarse por sí solas.
- Antes de autorizar a un empleado para ingresar al centro de cómputo, ya sea temporalmente o no, se debe diligenciar el formato de autorización para dar ingreso al centro de cómputo.
- No se permite el ingreso de alimentos o bebidas en el centro de cómputo.
- No se permite fumar en el centro de cómputo.
- Los residuos deben arrojarse siempre en cestos, los cuales deben vaciarse periódicamente. No se debe permitir que los residuos se apilen en el piso o sobre los equipos.
- Los líquidos inflamables (incluyendo productos de limpieza) deben permanecer fuera del centro de cómputo.
- Mantenga el centro de cómputo limpio y ordenado.
- La puerta de salida debe encontrarse libre de obstrucciones en todo momento.
- Todo personal de limpieza que acceda al centro de cómputo debe encontrarse autorizado para acceder a éste.
- La temperatura en el centro de cómputo debe mantenerse a un nivel adecuado. Los mismos deberán tener una temperatura entre 18 y 22 grados Celsius con una humedad relativa del 50%.
- Se debe tener un registro de todos los dispositivos que ingresen y salgan del centro de cómputo, así como su responsable.
- Los centros de cómputo deben estar equipados con sensores de humedad y temperatura, los cuales deberán ser probados periódicamente.
- Mantener un inventario de todas las llaves y guardarlas en un lugar seguro.

### 4. Lineamientos para periféricos y unidades externas de almacenamiento

- Los funcionarios y contratistas son responsables por la custodia de los medios de almacenamiento institucionales asignados.
- Los computadores deben tener configurada la herramienta de antivirus institucional y tener habilitado el escaneo automático de virus.

- Los funcionarios y contratista no deben guardar información clasificada o reservada de Colombia Compra Eficiente en memorias USB sin tener mecanismos que la protejan (cifrado).

## 5. Lineamientos para las estaciones de trabajo

- Los funcionarios y contratistas no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la entidad.
- Los funcionarios y contratistas no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables, con excepción de que se requiera un trabajo remoto.
- Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o lugares que puedan afectar la seguridad de esté.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su Integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

## 6. Lineamientos para el uso de dispositivos personales

Los funcionarios y contratistas que hagan uso de sus dispositivos personales para la realización de sus actividades laborales deben seguir los siguientes lineamientos:

- Los funcionarios y contratistas deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos cuando no se está haciendo uso de estos.
- Los funcionarios y contratistas deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Los funcionarios y contratistas deben evitar usar los dispositivos personales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los funcionarios y contratistas deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde repositorios confiables.
- Los funcionarios y contratistas deben asegurar sus dispositivos personales con las medidas y controles necesarios para prevenir la fuga de Información Confidencial.

## 7. Lineamientos para las contraseñas

La complejidad de las contraseñas de los sistemas de información son responsabilidad de cada funcionario y contratista. Para ello, los funcionarios y contratistas deben cumplir con los siguientes lineamientos:

- La cuenta institucional (Correo, directorio activo, OneDrive, POXTA etc..) de cada funcionario y contratista debe contar con tres de los siguientes elementos: (i) mayúsculas, (ii) minúsculas, (iii) números y (iv) caracteres especiales. De igual manera la contraseña debe

tener una longitud mínima de 8 caracteres. El sistema exige el cambio de contraseñas cada dos meses y no es posible repetir alguna de las 3 últimas contraseñas.

- Las cuentas del Sistema de información SECOP II deben cumplir con una longitud mínima de 8 caracteres como mínimo y contener mayúsculas, minúsculas, números y símbolos. No se exige el cambio de contraseña.

- Las cuentas del Sistema de Información de Tienda Virtual del Estado Colombiano (TVEC) deben contener 8 caracteres como mínimo, combinando letras y números. No se exige el cambio de contraseña.

Los funcionarios y contratistas deben cumplir las siguientes restricciones a la hora de establecer una contraseña:

- No se debería utilizar información personal en una contraseña.
- No se debería utilizar palabras que estén en un diccionario o enciclopedia común.
- No se debería utilizar su mismo nombre de usuario.
- No se debería utilizar el nombre de un familiar, de su colegio, universidad, iglesia, o alguna agremiación conocida.
- No se debería utilizar el nombre o sigla de su entidad, ni nada relacionado con la misma.
- No se debería utilizar secuencias de teclas predecibles o encontradas en el teclado. Ej. 123456789, qwertyuiop, asdfghjklñ, abcdefghijk, etc.
- No se debería utilizar secuencias de letras o caracteres únicos. Ej. 1111111, aaaaaaaa, BBBBBB.
- No se debería utilizar secuencias alternadas de pocos caracteres. Ej. aSaSaS, aaAABBcc, 123aBC, etc.

## 8. Lineamientos para el acceso a la red inalámbrica

Colombia Compra Eficiente cuenta con las siguientes redes inalámbricas con sus respectivas características:

- CCE-CORP es la red inalámbrica a la cual solo debe ingresar los equipos autorizados de funcionarios y contratistas de Colombia Compra Eficiente. Los funcionarios y contratistas deben seguir los demás lineamientos de seguridad definidos en esta política y hacer uso adecuado de su conexión de internet. Todos los equipos de cómputo de Colombia Compra Eficiente deben estar configurados para acceder a la red de corporativos.

- CCE-MOVIL es la red inalámbrica a la cual los funcionarios y contratistas pueden hacer uso para los dispositivos personales. El acceso a esta red inalámbrica se hace mediante las credenciales personales de cada funcionario o contratista.

- Zona WIFI gratis para la gente es la red inalámbrica a la cual pueden ingresar visitantes, por lo cual tendrá las restricciones necesarias para garantizar la Seguridad de la Información. Para poder ingresar a la red de visitantes, se debe solicitar la contraseña a la Mesa de Ayuda o en Recepción.

## 9. Lineamientos Incidentes de Seguridad de la Información

Todo Incidente de Seguridad debe ser comunicado a la Mesa de Ayuda o directamente al área de Seguridad de la Información para ser tratado y gestionado de la manera correcta.

¿Cómo identificar si es un evento o incidente de Seguridad?

Un evento de seguridad compromete o tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la Seguridad de la Información. Mientras que un Incidente de de Seguridad de la información es un evento o serie de eventos no deseados o inesperados, que han comprometido la seguridad de la información.

Colombia Compra Eficiente clasifica los incidentes de seguridad de la siguiente manera:

- Ataques informáticos e ingeniería social: cuando (i) un tercero, haciendo uso de herramientas tecnológicas, intenta tomar el control, desestabilizar o dañar una plataforma tecnológica (Ataque informático); o (ii) cuando un tercero busca obtener Información Confidencial que pueda perjudicar o exponer a una persona u organismo. Dentro de esta categoría encontramos incidentes de seguridad como DoS, Defacement, Spam, Phishing y Spoofing.

- Acceso no autorizado o perdida de datos: cuando un tercero no autorizado, de manera intencional o no, logra tener acceso a un Sistema de Información o documentos comprometiendo la Confidencialidad, Integridad o Disponibilidad de la información.

- Infección por malware: cuando un dispositivo tecnológico contiene un programa o código malicioso que compromete la Confidencialidad, Integridad o Disponibilidad del dispositivo o la información que contenga.

- Afectación a la seguridad física: cuando (i) ocurre una pérdida o robo de equipos, dispositivos o documentos que afectan la Confidencialidad, Integridad o Disponibilidad de la información de la Entidad; (ii) cuando ocurre un daño a elementos físicos que comprometa la Seguridad de la Información o (iii) cuando hay un ingreso no autorizado a instalaciones o áreas restringidas.

- Incumplimiento de la Política de Seguridad: cuando existe un incumplimiento de la política de seguridad por parte de un funcionario o contratista. Dentro de esta categoría encontramos incidentes como: (i) el tratamiento inadecuado de datos personales, (ii) Abuso y/o mal uso de los activos o recursos tecnológicos, (iii) Incumplimiento del acuerdo de Confidencialidad, (iv) Ausencia de etiquetado de la información, entre otros.

Para más información consultar la guía de incidentes de seguridad.

## 10. Esquema de etiquetado de la Información

Todo funcionario y contratista que genere o manipule documentos debe velar para que los documentos estén etiquetados de acuerdo con su nivel de Confidencialidad siguiendo el siguiente esquema:

- Borrador: se le etiqueta como "Borrador" a aquellos documentos que estén en construcción y no sean oficiales. Estos documentos no están obligados a comunicarse a los ciudadanos por ser documentos en construcción.
- Publico: se le etiqueta como "Publico" a aquellos documentos que no tienen carácter "Clasificado" o "Reservado" y por ende pueden ser consultados por cualquier persona y no perjudicaría a Colombia Compra Eficiente.
- Clasificado: se le etiqueta como "Clasificado" a aquellos documentos que contengan información que pueda llegar a dañar derechos a personas naturales o jurídicas (artículo 18 ley 1712 de 2014). Véase índice de información clasificada y reservada.
- Reservado: se le etiqueta como "Reservado" a aquellos documentos que contenga información que pueda llegar a dañar intereses públicos (artículo 19 ley 1712 de 2014). Véase índice de información clasificada y reservada.

Para el caso en que un documento de contenga información que pueda llegar a dañar intereses públicos (Reservado) y dañar derechos de personas naturales o jurídicas (Clasificado), el documento será etiquetado como reservado.

Si un documento "Borrador" puede llegar a dañar derechos de personas naturales o jurídicas (Clasificado) se deberá etiquetar con los dos criterios: "Borrador Clasificado"; de igual manera, si un documento "Borrador" puede llegar a dañar intereses públicos (Reservado) se deberá etiquetar con los dos criterios: "Borrador Reservado".

Los funcionarios y contratistas deben velar por la especial custodia de los documentos etiquetados con "Clasificado" o "Reservado", ya que su inadecuado uso puede traer consigo efectos negativos a Colombia Compra Eficiente.

## 11. Cifrado de sistemas de Información y/o Aplicativos:

En los casos en que es necesario contar con mecanismos de cifrado en los sistemas de información y/o aplicativos debido a que trasmiten información tipificada como clasificada o reservada, se deben tener en cuenta las siguientes indicaciones generales:

- Contar con controles de cifrado en las credenciales utilizadas para acceder a dichas herramientas, además de verificar que estas contraseñas cumplan con lo indicado en los "lineamientos para contraseñas" del presente documento.
- Cuando se trata de trasferencia tipo Cliente/Aplicación, los datos deben ser cifrados en el extremo o en el servidor antes de enviarse por la red o almacenarlos en un formato de cifrado adecuado.
- En enlace/Red, utilizar técnicas de cifrado de red estándar incluyendo SSL, VPNs, y SSH. Puede ser hardware o software y si es posible cifrado de extremo a extremo.

- Se debe verificar que los sistemas de información y/o aplicaciones de Colombia Compra Eficiente, ya sean propias o tercerizadas cuenten con algoritmos de cifrado en los casos en que se requiere encriptar datos.
- Acogiendo lo indicado en el lineamiento de seguridad y privacidad de los sistemas de información - LI.SIS.22 del MPSI, la Subdirección de IDT garantiza que, en el diseño de los sistemas de información, se incorporan componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.

## 12. Guía para el cifrado de la información y aplicación de Criptografía

Los funcionarios y contratistas deben cifrar la Información Confidencial y critica de manera apropiada y eficiente, lo anterior cuando las circunstancias lo exijan y de acuerdo con el valor dado al activo de información; el cifrado de la información se puede realizar con diversas herramientas y algoritmos, dentro de las disponibles en Colombia Compra Eficiente esta:

Cifrado con 7-zip:

- Buscar el archivo o carpeta que se desea cifrar con 7-Zip.
- Clic derecho en el archivo o carpeta, seleccionar "7-Zip" y seleccionar "Añadir al archivo".
- Introducir una contraseña o frase de paso en los campos de texto cifrado. Es necesario introducir la contraseña en ambos campos de contraseña.
- Revisar el apartado "Cifrar nombres de archivo" para evitar que nadie pueda ver los nombres de archivo contenidos si no tienen una contraseña.
- clic en "Aceptar" para cifrar el archivo o carpeta. A continuación, puedes eliminar el original, si quieres. Siempre y cuando tengas la contraseña, puedes acceder al archivo desde el archivo cifrado.

Protección con Office:

- En el documento office (ej.: Word, Excel, PowerPoint) seleccionar "archivo", seleccionar "información", seleccionar "Proteger Documento" y seleccionar "cifrar con contraseña". Es necesario introducir la contraseña dos veces.
- clic en "Aceptar" para cifrar el documento. A continuación, el archivo queda cifrado y siempre solicitara la contraseña al momento de abrirlo.

## 13. Lineamientos administración, protección y ciclo de vida de las llaves criptográficas

Además de aplicar lo indicado en "lineamientos para contraseñas", es necesario aplicar buenas prácticas en el manejo de llaves criptográficas, de no hacerlo es posible que el procedimiento de encriptación no cumpla con su objetivo primordial y exponga información tipificada como reservada y clasificada por Colombia Compra Eficiente, en estos casos se debe tener cuenta lo siguiente:

- Cuando se utilice cifrado simétrico y se remita la información a un destinatario, se debe contar con un canal seguro para el intercambio de las claves.
- No remitir en el mismo paquete de información cifrada la clave de desencriptación, así mismo no remitir mensajes con señas o indicios sobre la clave empleada.
- Para información con un alto índice de confidencialidad, se recomienda emplear mecanismos que utilicen cifrado asimétrico (sistemas de cifrado de clave pública) o hibrido.

- En lo posible no contar con claves con un periodo de vida extenso, en cuanto más tiempo permanece activa, más insegura será.
- Las llaves privadas se deben de mantener en secreto y con una custodia adecuada.
- Evitar la eliminación, modificación o pérdida de llaves necesarias para descifrar datos cifrados de forma permanente, en estos casos es necesario contar con un procedimiento de recuperación ya sea de la información o de la llave, como por ejemplo "key Escrow".

Para más información se puede consultar a la Mesa de Ayuda.

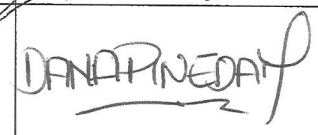
### 14. Grupos de proyecto

Los Grupos de proyecto cuentan con un líder quien debe:

- Cumplir con las funciones del propietario de Activos de información generada para la función del grupo de trabajo.
- Definir los perfiles de usuario y autorización a la información y recursos del grupo de trabajo.
- Gestionar los permisos de acceso a los diferentes Sistemas de Información de su grupo de trabajo.
- Solicitar y administrar las carpetas de espacio colaborativo en el servidor Nube que requiera.
- Responder por las carpetas de gestión documental asociadas y gestionar los permisos asociados.
- Informar los incidentes de seguridad que identifique.
- Preparar y generar la documentación necesaria que pueda ser utilizada en caso de un evento adverso y tener un plan de contingencia.
- Exigir al Grupo de proyecto cumplir con los lineamientos de seguridad establecidos en el presente manual.

Funcionarios y contratistas pertenecientes a un grupo de proyecto deben acatar todos los lineamientos del presente Manual.

## I. Autorizaciones

| | Fecha | Nombre | Firma | Cargo o Perfil |
|---|---|---|---|---|
| Elaboró | 01/06/2018 | L. Alejandro Ruiz A. |  | Subdirección de Información y Desarrollo Tecnológico |
| Revisó | 26/06/2018 | Dana Pineda Marín |  | Subdirectora de Información y Desarrollo Tecnológico |
| Aprobó | 19/07/2018 | Comité Institucional de Gestión y Desempeño | Acta Comité Virtual No. 4 – julio 19 de 2018<br>Director General | |