
	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

TABLA DE CONTENIDO

OBJETIVO	2
ALCANCE	2
DEFINICIONES	2
DESARROLLO DE POLÍTICAS	5
1. DECLARACIÓN DE LA POLÍTICA	5
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	8
3. SEGURIDAD DE LOS RECURSOS HUMANOS	10
4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN	11
5. CONTROL DE ACCESO LÓGICO	11
6. SEGURIDAD FISICA	17
7. SEGURIDAD DE LAS OPERACIONES	21
8. SEGURIDAD EN LA RED	24
9. SEGURIDAD EN LOS DESARROLLOS.....	26
10. RELACIONES CON PROVEEDORES	27
11. SEGURIDAD EN LA NUBE	29
12. INCIDENTES DE SEGURIDAD	31
13. SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO	32
14. CUMPLIMIENTO REGULATORIO	33
15. ENTRADA EN VIGENCIA DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN	34

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021


OBJETIVO

Establecer los lineamientos de Seguridad de la Información y Ciberseguridad que deben aplicarse a toda la información de la Caja, con el fin de establecer y mantener un ambiente controlado de los riesgos de los activos de información, y el cumplimiento de los requisitos establecidos por los entes de control (Superintendencia de Subsidio familiar, Superintendencia de industria y comercio, entre otros)

ALCANCE

Aplica a todas las unidades de negocio de Colsubsidio, que incluyen: empleados, áreas de apoyo, terceros (proveedores y contratistas), clientes y afiliados que de manera directa o indirecta interactúan con la infraestructura o los activos de información que hacen parte de los negocios o áreas transversales de la caja.


Hace parte del alcance toda la información y recursos de valor (Tecnologías de información y de las comunicaciones -TICs-, Instalaciones, y Tecnologías operacionales -OTs-) asociados a ésta, propios de La Caja o gestionados por Terceros, independiente del formato, medio, en todas sus formas (digital, manuscrita, hablada, impresa), presentación y/o lugar en el que ésta se encuentre ubicada, incluido el ciberespacio. Así mismo, la información generada, procesada, transmitida o resguardada por los procesos de la Caja y activos de información incluidos en dichos procesos.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

DEFINICIONES

Activo de Información: Corresponde a los objetos tangibles o intangibles asociados con la información y que son requeridos para las actividades de los negocios.

Alta dirección: Está compuesta por el Director Administrativo y subdirectores de Colsubsidio.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

Áreas críticas: Áreas físicas donde se almacena, procesa o genera información de uso privado o confidencial que por su alto riesgo representa una vulnerabilidad para la seguridad de la información de Colsubsidio.

Áreas de apoyo: Son las áreas que se encargan de apoyar a los negocios de crédito, salud, recreación, mercadeo y educación en temas administrativos y de operación. Las gerencias encargadas de realizar este apoyo transversal son las gerencias de recursos humanos, gerencia corporativa de tecnología, gerencia recursos compartidos, gerencia de infraestructura.

BSIMM: Siglas de Modelo de Madurez para la Construcción de Seguridad (Building Security In Maturity Model). Metodología que reúne las buenas prácticas y evalúa la madurez de la seguridad en los desarrollos de software.


Cifrar: Es la codificación del contenido de un mensaje o archivo para que llegue solamente a la persona autorizada a recibirlo.

Ciberseguridad: Es el área relacionada con la seguridad de la información que se enfoca en la protección de la información, redes, internet e infraestructuras críticas de TI. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados^[1].

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran¹.

Equipos críticos: Computadores o estaciones de trabajo que son esenciales para la


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

ejecución de un proceso de la caja.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso¹.

Medios de almacenamiento extraíbles: Medios para guardar y portar información de forma electrónica tales como disquetes, CD's, DVD's, discos ZIP, discos ópticos, discos duros externos, memoria digital USB, etc.

Microsoft SDL Security Development Lifecycle (SDL): Es un proceso de desarrollo de software que ayuda a los desarrolladores a crear software y los requisitos de cumplimiento de seguridad de direcciones más seguras al tiempo que reduce los costes de desarrollo.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

OWASP (Open Web Application Security Project): Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro^[2].

Periférico: Elemento o dispositivo del computador que no hace parte de la unidad central, tales como el monitor, mouse, teclado, parlantes, impresora, escáner, unidades de almacenamiento, etc.


Procesos críticos: Son aquellos procesos que son vitales para el funcionamiento y sostenimiento de la caja.

Propietario/responsable de activo de información: Identifica un individuo o una entidad que tiene la responsabilidad asignada y/o aprobada para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de Información. El término “Propietario” no implica que la persona tenga los derechos de propiedad de los activos de información, sino que funcionalmente es conocido como el responsable.

Recurso Informático: Es cualquier componente físico o virtual de disponibilidad limitada asignado a los trabajadores por parte de Colsubsidio para el desempeño de sus labores dentro de la Caja. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

Riesgo de seguridad de la información^[3]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.


Seguridad de la información: Significa la protección de la información y los sistemas de información del acceso no autorizado, la divulgación, la alteración, la modificación o destrucción. En otras palabras, la seguridad de la información es la preservación de las tres propiedades básicas de la información:

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

1. Confidencialidad
2. Integridad
3. Disponibilidad.

Sistema operativo: Programa de computador que organiza y gestiona todas las actividades que sobre él se ejecutan. Algunos sistemas operativos son Windows, Unix y Linux.

Superusuario: Usuario de sistema de información con privilegios de administrador dentro del mismo. Son ejemplos de superusuarios el SA para base de datos, el root para SO Linux o el admin o enable para equipos de red.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

Teletrabajo / Trabajo colaborativo virtual: Es una forma de organización laboral que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

VPN: Es una tecnología que permite la extensión de una red privada como la de Colsubsidio en un espacio de red público, pero protegido por un canal virtual. Para los negocios es de vital importancia debido a las tareas adicionales que se tienen que hacer fuera del horario laboral, para teletrabajo y zonas en las que no hay un canal asignado como el caso de algunas droguerías.

WLAN: Sistema de comunicación inalámbrico en redes internas.

Zona Desmilitarizada: Red local que se ubica entre la red interna de una organización y una red externa, generalmente en internet.


^[1] ISO/IEC 27000:2016

^[2] Para más información consultar www.owasp.org

^[3] ISO /IEC 27005:2011


DESARROLLO DE POLÍTICAS

1. DECLARACIÓN DE LA POLÍTICA

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

1.1 Aspectos generales

1. La información es considerada por Colsubsidio como un activo principal que como tal hace parte fundamental de las operaciones diarias, convirtiéndose en un componente esencial que debe ser protegido para el cumplimiento de los objetivos estratégicos de negocio. Este aspecto hace que todos aquellos a quienes se le haya autorizado el acceso a la información, sean responsables por el buen uso que se le dé a la misma.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	


2. La Alta Dirección de Colsubsidio expresa su compromiso con la Seguridad de la Información y Ciberseguridad estableciendo la presente política y apoyando todas las iniciativas encaminadas a cumplir con las políticas aquí establecidas, integrando todos los requerimientos de seguridad definidos por Colsubsidio en cada una de sus líneas de negocio.

3. Para Colsubsidio, la protección de la información busca la disminución del impacto generado sobre sus activos de información, por la materialización de los riesgos identificados de manera sistemática con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

4. La Alta Dirección apoya la mejora continua en todos los procesos relacionados con la Seguridad de la Información en Colsubsidio para así asegurar que estos son efectivos y cumplen con los requerimientos de seguridad de los negocios y áreas de apoyo.

5. Todos los trabajadores, contratistas y vinculados que tengan relación contractual con Colsubsidio están obligados a conocer, entender, cumplir y hacer cumplir las Políticas de Seguridad de la Información, sus principios y el anexo técnico de la misma.

6. Todo trabajador, tercero o vinculado a Colsubsidio se compromete con la protección de la información y de la infraestructura tecnológica, con el objetivo de asegurar su confidencialidad, integridad y disponibilidad.


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

7. La información personal de los clientes y afiliados, así como los activos de información propios de Colsubsidio, debe ser protegidos de acuerdo con lo establecido con la legislación Colombiana vigente y acorde al nivel de clasificación y valoración definido por Colsubsidio.

8. La Gerencia de Tecnología definirá los lineamientos técnicos que apoyen la aplicación de la presente política.


1.2 Aspectos particulares

1. Colsubsidio ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Gestión de Seguridad de la Información, soportado en lineamientos claros

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

2. Las responsabilidades frente a la Seguridad de la Información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. Colsubsidio protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
4. Colsubsidio protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos, legales y reputacionales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. Colsubsidio protegerá la información de las amenazas originadas por parte del personal.
6. Colsubsidio protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. Colsubsidio controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. Colsubsidio implementará control de acceso a la información, sistemas y recursos de red.


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

9. Colsubsidio garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. Colsubsidio garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. Colsubsidio garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

12. Colsubsidio garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	


2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.1 Organización Interna

Como parte integral para el cumplimiento continuo de la Política, Colsubsidio establece el comité de Seguridad de la Información precedido por el Gerente Corporativo de Tecnología, para proveer el apoyo manifiesto en la gestión, construcción, implementación y mejora continua del modelo de Seguridad de la Información. El comité de seguridad de la información es un órgano consultivo para la administración y el direccionamiento estratégico, conformado por representantes de las áreas relacionadas con la gestión integral de riesgos y seguridad. El Comité se encuentra constituido por:

- Gerente de Tecnología
- Gerente de Servicios Administrativos
- Jefe Seguridad de la información
- Auditor Interno
- Según necesidad y a demanda, un representante del área jurídica de la caja


El Comité de Seguridad de la Información es el ente dentro de la organización responsable por aprobar las normas y procedimientos de seguridad de la Información / Ciberseguridad, así como de verificar su cumplimiento. Es responsable por el mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

2.2 Dispositivos para la Movilidad y el Teletrabajo

2.2.1 Dispositivos Móviles

Audiencia: General


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

1. No se permite la conexión de dispositivos móviles personales a las redes Corporativas de Colsubsidio. Los dispositivos móviles propiedad de Colsubsidio que sean definidos como críticos por la Jefatura de Seguridad de la Información, deberán sin excepción estar cifrados y ser configurados con los controles definidos en los estándares de seguridad para dispositivos móviles.
2. Está prohibido el uso de equipos móviles como medio de almacenamiento, grabación y para capturar información de la Caja. Cualquier excepción deberá ser aprobada por la Jefatura de Seguridad de la Información.
3. En caso de pérdida o hurto de un dispositivo móvil, que se encuentre autorizado para acceder a las aplicaciones o información de la Caja, se debe notificar de manera inmediata al Departamento de Operaciones de TI y a la Jefatura de Seguridad de la Información con el fin de deshabilitar las cuentas de usuario respectivas y evitar accesos no autorizados a la información.
4. Para áreas críticas definidas por la Jefatura de Seguridad de la Información, está prohibido el ingreso y uso de dispositivos móviles, dispositivos de almacenamiento, de capturas audiovisuales (audio y video) y cualquier otro dispositivo no autorizado.

2.2.2 Teletrabajo y trabajo en casa


Audiencia: General

1. Los usuarios que por razones propias del negocio se encuentren autorizados para realizar teletrabajo y trabajo en casa, serán responsables por la protección física del equipo asignado contra acceso, uso no autorizado, pérdida o daño.
2. Los usuarios que se encuentren autorizados para realizar trabajo

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

colaborativo virtual deberán hacer uso de las herramientas colaborativas autorizadas. No está permitido la instalación, almacenamiento o utilización de software no licenciado, si no ha sido autorizado expresamente por la Gerencia de Tecnología.

3. Las conexiones que se realicen desde y hacia los equipos destinados para teletrabajo y trabajo en casa, se deben hacer a través de VPN o la infraestructura de acceso remoto (ej. Terminal services) dispuesta por la Gerencia de Tecnología con previa autorización del jefe inmediato y mediante solicitud en Service Manager. Cualquier otro medio utilizado para realizar conexiones remotas está prohibido, excepto si este fue expresamente autorizado por la Jefatura de Sección de Seguridad de la Información.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

4. Todas las reuniones virtuales entre equipos internos y proveedores se deben efectuar a través de la plataforma definida por la Gerencia de Tecnología. Las invitaciones a reuniones deben generarse por parte de un colaborador de Colsubsidio. Para todos los casos, se debe advertir a los participantes que se realizará una grabación y se podrá decidir si se graba o no la sesión. Las grabaciones de reuniones se consideran contenidos propiedad exclusiva de Colsubsidio como parte de su espacio empresarial y dicha información no puede ser divulgada sin previa autorización por parte del responsable de la misma.


Audiencia: Tecnología

5. Los administradores de cada plataforma o aplicativo tienen la responsabilidad de implementar los controles necesarios para el aseguramiento de los equipos de teletrabajo contra acceso lógico no autorizado, protección de la información y la red Corporativa.


3. SEGURIDAD DE LOS RECURSOS HUMANOS

Audiencia: Empleados y Contratistas

1. Todos los empleados deben cumplir con los procedimientos de verificación y contratación exigidos por parte de la Gerencia de Talento Humano.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3


2. Todos los empleados y terceros vinculados a Colsubsidio deben firmar una cláusula de confidencialidad que tiene como finalidad dar a conocer las obligaciones, compromisos y responsabilidades que tiene el personal en cuanto al manejo de la información se refiere.
3. Los empleados de Colsubsidio deben recibir a su ingreso una capacitación obligatoria de Seguridad de la Información que está a cargo de la Gerencia Corporativa de Talento Humano. Durante la permanencia en la Caja, se deben realizar planes de concienciación de seguridad de la información, donde la Jefatura de Seguridad de la Información genera contenido y es responsabilidad de cada uno de los líderes de proceso apoyar en la divulgación de dichos temas. Para los contratistas se debe socializar las Políticas de Seguridad de la información a cargo del responsable del contrato.
4. Ante cambios de cargo o terminación del contrato laboral, el empleado debe hacer entrega formal mediante acta al jefe inmediato de los activos de información que le fueron asignados.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

Audiencia: Empleados y Contratistas

1. Toda información debe estar identificada, clasificada y valorada acorde con el procedimiento de Gestión de Activos de Información definido por Colsubsidio y debe estar alineado con las definiciones de la circular 002 de la Superintendencia de Subsidio Familiar, en materia de Gestión Documental. Este debe ser ejecutado por lo menos una vez al año en conjunto con los responsables de los inventarios, los propietarios/responsables de los activos de información y la Jefatura de Seguridad de la Información.
2. Los activos de información de Colsubsidio deben contar con un propietario/responsable definido.
3. Todo activo de información debe contar con los controles definidos, para dar tratamiento a los riesgos identificados. Es responsabilidad del propietario del activo verificar la correcta aplicación de los controles.
4. Ningún empleado o tercero que maneje información de Colsubsidio puede divulgar información de la Caja, clientes y afiliados a personas no autorizadas.
5. El propietario del activo clasifica la información a su cargo de acuerdo al procedimiento de Gestión de Activos de Información. Así mismo realiza el tratamiento y manejo acorde con la clasificación asignada.
6. La información digital clasificada como confidencial, debe almacenarse y transmitirse de manera cifrada, a través de los medios establecidos por el


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

Departamento de Operaciones de TI.

7. La información física y los dispositivos de almacenamiento que contienen datos confidenciales, deben destruirse como está definido en el procedimiento de Borrado y Disposición Segura de Medios.


5. CONTROL DE ACCESO LÓGICO

5.1 Controles generales

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3


Audiencia: General

1. Todos los procedimientos y lineamientos definidos para la gestión de accesos son de obligatorio cumplimiento por parte de los responsables, partes involucradas y usuarios.
2. Las cuentas de usuario deben ser asignadas a las personas de acuerdo con el rol y cargo que desempeña en Colsubsidio y según las necesidades específicas del cargo. Solo debe acceder a la información el personal autorizado.
3. Toda transacción y actividad realizada con la cuenta de usuario asignada a los sistemas de información de Colsubsidio, será responsabilidad del propietario de dicha cuenta.
4. Las contraseñas o cualquier otro método de autenticación deben mantenerse bajo reserva y ser entregadas de forma personal o a través de un medio que asegure su confidencialidad.
5. Las cuentas de usuarios, contraseñas o cualquier otro mecanismo de autenticación a los sistemas de información, es información personal e intransferible; por tanto, deben ser tratadas como información confidencial de Colsubsidio. Así mismo, no deben ser divulgadas, publicadas ni compartidas.
6. Las credenciales de propiedad y custodia de Gestión de Accesos y administradores de TI deben ser resguardadas a través de herramientas que garanticen su seguridad, disponibilidad, confidencialidad e integridad.
7. Las cuentas creadas para los diferentes sistemas de información deben ser deshabilitadas por Gestión de Accesos y administradores de TI una vez finalizadas las funciones de los empleados o proveedores que presenten novedades (vacaciones, licencias, incapacidades, entre otras). Es responsabilidad


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

del jefe inmediato informar la novedad de manera oportuna a Talento Humano, quien a su vez debe transmitir la información a Gestión de Accesos.

8. Los empleados de la corporación tienen derecho a ingresar a los sistemas de información que requieran para su desempeño laboral, pero por ningún motivo debe concederse acceso a los sistemas de información adicionales hasta que no exista una autorización formal por los aprobadores con su respectiva justificación.
9. El empleado que identifique que tiene accesos que no corresponden a su cargo o funciones dentro de la organización tiene la responsabilidad de reportarlo inmediatamente al jefe inmediato, quien debe informar a Gestión de Accesos y Seguridad de la Información.
10. Toda autorización y/o evento que implique riesgos de integridad, confidencialidad y disponibilidad en los sistemas de información debe estar avalada por el departamento de operaciones de TI, Jefatura de Seguridad de la Información y/o Gerencia de TI, según corresponda.


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021
		Código: TI.PO.02
		Versión: 3

11. Todos los contratistas, consultores, temporales y proveedores deben pasar por un proceso similar al de los empleados de solicitud de acceso y autorización tramitado por el gestor del proyecto, mejoras o encargado. Los privilegios de estos deben ser revocados inmediatamente por Gestión de Accesos tan pronto culmine el proyecto o cuando los terceros terminen su vínculo con Colsubsidio. Esto debe ser reportado oportunamente por el gestor de proyecto encargado. Adicionalmente, es el responsable de establecer la vigencia y reportar cada 3 meses los accesos que requiera que permanezcan activos.
12. Empleados, proveedores y contratistas no podrán, en ejercicio de las actividades consignadas en un contrato firmado con Colsubsidio, utilizar usuarios genéricos para ningún tipo de actividad. En caso de ser necesario el uso de una cuenta genérica debe ser justificada la necesidad por el negocio y aprobada por Seguridad de la Información.
13. La solicitud de una cuenta genérica debe estar autorizada por el Gerente del Negocio o Jefe de Departamento y el Jefe de Seguridad de la Información. Adicionalmente, el jefe encargado del área solicitante es responsable del buen uso del mismo.
14. Las cuentas de usuario deben ser asignadas a las personas que explícitamente lo han solicitado a través de procedimiento de Gestión de Accesos de Colsubsidio. Para las aplicaciones que no estén administradas por el área de Gestión de Accesos, se debe nombrar un delegado de la administración de accesos, al cual se le debe realizar seguimiento y control.
15. Talento Humano debe informar al área de Gestión de Accesos cualquier novedad (terminación de contrato, vacaciones, licencias, incapacidades o cambios de cargo de los empleados y terceros vinculados a Colsubsidio, entre otros) y de los empleados y terceros vinculados con Colsubsidio.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

Audiencia: Tecnología

16. Los Superusuarios de los diferentes sistemas de información, bases de datos, y sistemas operativos, deben estar en custodia del Jefe de Departamento de Operaciones de TI. No deben ser asignados en ambiente productivo, sobre ningún usuario del sistema y/o rol; exceptuando casos en los cuales por razones propias de negocio se requiera su uso, estas deben estar aprobados por el Jefe de Sección de Seguridad de la Información y el jefe del Departamento de Operaciones de TI.
17. El Superusuario debe utilizarse únicamente en casos de incidentes mayores y por tiempo limitado. Finalizado este periodo se debe acordar un plan con el administrador del sistema

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021
		Código: TI.PO.02
		Versión: 3


para realizar el cambio de la contraseña, el cual debe ser ejecutado máximo 72 horas después de la finalización del tiempo pactado.

18. Todos los Superusuarios deben estar monitoreados por el área de Seguridad de la Información. Este monitoreo debe realizarse al menos de manera semestral.
19. Gestión de Accesos y Administradores de TI deberán verificar el cumplimiento y desarrollo de ciclo de vida de los accesos vigentes, identificando riesgos o fallas que requiera la intervención de los dueños de los activos de información a través de acciones que promuevan la preservación de la confidencialidad, disponibilidad e integridad relacionada con la seguridad de la información.
20. Es responsabilidad de Gestión de Accesos y Administradores de TI realizar un monitoreo permanente de los derechos de acceso asignados e informar las novedades identificadas para la gestión por parte de los dueños de activos de información.

5.2 Control de Acceso a los Sistemas de Información

Audiencia: General

1. Todos los usuarios a los cuales les sean asignadas credenciales de acceso a los sistemas de información son responsables de mantener la confidencialidad de las mismas.
2. Los sistemas de información que soportan los procesos de negocio deben contar


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

con los controles de seguridad necesarios para garantizar la confidencialidad de las credenciales de acceso de los usuarios, esto es responsabilidad del administrador del sistema.


3. La responsabilidad de implementar los controles necesarios para asegurar la confidencialidad de las credenciales de autenticación a los sistemas de Colsubsidio es del funcionario al cual se le asignaron.

5.3 Control de Acceso al Correo Electrónico

Audiencia: General

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3


1. El acceso al correo electrónico está reservado para los funcionarios y terceros autorizados, el cual debe ser utilizado de acuerdo a las necesidades del negocio y para el desempeño de las funciones propias del cargo.
2. Los mensajes por correo electrónico son considerados activos de información, por lo que están sujetos a políticas de monitoreo, auditoría e investigación de eventos.
3. No se permite el uso del correo electrónico para actividades personales, comerciales, cadenas que contengan (bromas, difusión de software malicioso, contenido religioso, juegos, racista, sexista, pornografía, publicitario no corporativo, político, mensajes mal intencionados) o cualquier otro tipo de información que no esté autorizado o atente contra la dignidad de las personas y que comprometan la imagen, reputación y Seguridad de la Información de Colsubsidio.
4. La transmisión de mensajes en forma masiva a través de correo electrónico debe ser autorizado por comunicaciones internas y el Departamento de Operaciones de TI cuyo contenido tratará únicamente asuntos corporativos de Colsubsidio.
5. Se prohíbe el envío de comunicaciones por correo electrónico a los afiliados, clientes, usuarios, empleados, entre otros relacionados con Colsubsidio, que no hayan sido solicitadas o aprobadas por los mismos, de acuerdo con la legislación vigente de protección de datos personales (Ley 1581 de 2012)
6. Está prohibido y de acuerdo con las leyes del país, es un delito la suplantación del correo electrónico asignado por Colsubsidio por parte de otros funcionarios.
7. Los mensajes con archivos adjuntos o enlaces de dudosa procedencia no se deben abrir, ya que pueden contener software malicioso como virus y troyanos que afecten los sistemas de información de Colsubsidio. Estos casos se deben comunicar a la Mesa de Ayuda y reportados como un incidente de seguridad de la

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

Información con copia del evento a la Jefatura de Seguridad de la Información.

Audiencia: Tecnología


8. El Departamento de Operaciones de TI debe garantizar que se generen registros en la plataforma de correos electrónicos, este debe estar configurado de tal manera que todos los mensajes recibidos y/o enviados queden debidamente registrados en logs. Al menos debe quedar registrada la hora y fecha de recepción, la IP de origen y el encabezado del mensaje.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

9. El Departamento de Operaciones de TI debe generar una recuperación de correos según Seguridad de la Información lo requiera para efectos de auditoría y continuidad de la operación.
10. El personal de soporte técnico y/o administradores de los sistemas de información no están autorizados para revisar el contenido del correo electrónico de algún empleado en particular, la única área con potestad de revisar o autorizar la revisión de un correo electrónico es el Comité de Seguridad de la Información.


5.4 Uso de Internet:

1. Los usuarios del servicio de Internet de COLSUBSIDIO deben hacer uso del mismo exclusivamente para las actividades laborales que así lo requieran. Las páginas a las cuales cada cargo tiene acceso se registran en la matriz de acceso de internet vigente. No está permitido el acceso a páginas que no se encuentren autorizadas en dicha matriz.
2. Los usuarios del servicio de Internet tienen prohibido la descarga, uso, intercambio y/o instalación de software, juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual, o que contengan archivos ejecutables y/o herramientas que vulneren la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros, en las estaciones de trabajo o dispositivos móviles asignados.
3. No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento. Las categorías

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

de páginas web vetadas se encuentran en el Procedimiento de Filtrado de Contenido Web para uso de internet corporativo.

4. Los usuarios del servicio de internet que no han sido autorizados tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de COLSUBSIDIO.
5. Para las solicitudes de accesos a páginas web diferentes a las asignadas por Colsubsidio dependiendo del cargo que desempeñen, el trabajador debe crear requerimiento en la herramienta de gestión del servicio el cual deberá ser aprobado por el jefe inmediato y Seguridad de la Información.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021


5.5 Redes Sociales:

1. Los empleados o empresas que prestan servicios a Colsubsidio deben ser cuidadosos con todo mensaje personal que publiquen en grupos de discusión de Internet (blogs, foros, etc.), red social (Facebook, Instagram, Snapchat, Pinterest, LinkedIn, etc.), YouTube, boletín electrónico, prensa o en cualquier otro sistema de información público. Dicho mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la Organización. En redes públicas únicamente las áreas autorizadas explícitamente por la Dirección General de la Caja podrán utilizar el nombre de la Organización con fines de promoción de la imagen corporativa.
2. Es responsabilidad de todos los empleados ser cuidadosos y limitar la cantidad de información personal y de contenido relacionado con su trabajo cuando hacen uso de uso de las redes sociales. No se permite publicar información confidencial y privilegiada de la Caja en redes sociales y/o grupos de discusión de Internet. No se permite utilizar redes sociales u otros medios de comunicación para divulgar información que desprestigie a la Organización, directivos, empleados, clientes, afiliados, usuarios, o proveedores.


6. SEGURIDAD FISICA

6.1 Controles Generales

Audiencia: General


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

1. Toda persona que visite las instalaciones de las diferentes sedes de Colsubsidio debe cumplir con los controles de acceso físico dispuestos por la Caja.
2. Los empleados, contratistas, terceros deben registrar su ingreso o salida, ya sea con la tarjeta de acceso correspondiente o en las bitácoras destinadas para tal fin. Las puertas de acceso deben ser cerradas una vez se realice el ingreso a las distintas áreas en las sedes de Colsubsidio.
3. Los movimientos o traslados de los equipos de cómputo, recursos informáticos y comunicaciones pueden efectuarse por cada unidad de negocio siempre y cuando haya sido aprobado por el área de tecnología.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3


4. Todo empleado, contratista y visitante debe portar en un lugar visible y en todo momento el carné que lo identifique dentro de las instalaciones de Colsubsidio.
5. La tarjeta de control de acceso y el carnet de identificación de Colsubsidio son de carácter personal e intransferible, en este sentido todos los movimientos que se realicen con dicha tarjeta quedarán registrados en la base de datos del sistema de seguridad, y serán responsabilidad directa del empleado al cual le fue asignada.
6. La información confidencial de manera física (documentos impresos, formatos, carpetas, DVDs, equipos de cómputo, dispositivos de almacenamiento, entre otros) de Colsubsidio, debe guardarse bajo llave (gabinete, archivador u otro medio físico seguro) cuando no está en uso, especialmente ante ausencias temporales o prolongadas y según el riesgo catalogado para dicho activo de información.
7. Cualquier alteración o acceso no autorizado a la información que se haga a través de los equipos de Colsubsidio será responsabilidad del usuario al cual le fue asignado dicho activo de información. Es responsabilidad del usuario tomar los controles mínimos de seguridad, como el bloqueo de sesión, para evitar que el computador quede expuesto y se use de manera no autorizada.
8. Bloquear la pantalla de su equipo de cómputo cuando no esté haciendo uso de éste cuando por algún motivo deba ausentarse de su puesto de trabajo y al finalizar la jornada laboral (bloquear con las teclas Windows + L y no solo apagar el monitor).
9. Se debe mantener el escritorio y pantalla limpios en las estaciones de trabajo.
10. Al finalizar la jornada laboral, los colaboradores deberán guardar en un lugar seguro los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada, además

Audiencia: Seguridad Física

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

Todo equipo de cómputo de uso personal o corporativo debe ser registrado por los responsables de seguridad física al ingreso y salida de las instalaciones de Colsubsidio. En caso de excepciones, estas serán aprobadas por la Jefatura de Seguridad Física.

11. Todos los empleados y terceros vinculados a Colsubsidio deben tener acceso único y exclusivamente a las áreas de la Caja de acuerdo con su rol y funciones.
12. Los componentes, equipos de procesamiento de información, comunicaciones y archivos importantes para el negocio de Colsubsidio, deben estar ubicados en áreas de acceso restringido a personal no autorizado, empleando mecanismos de control como tarjetas de proximidad, esquemas biométricos, cerraduras, entre otros. Así mismo, deben contar con cámaras de video que permitan grabar el flujo de personas que entran y salen de dichos


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

espacios. Es responsabilidad de cada una de las Unidades de Servicio notificar al Departamento de Seguridad Física la ubicación de dichos elementos y asignar el presupuesto suficiente para establecer los controles necesarios.

13. Las impresoras y fotocopiadoras de cualquier negocio de Colsubsidio deben tener un control para evitar el uso no autorizado.

Audiencia: Tecnología


14. Todo espacio físico donde resida la infraestructura tecnológica necesaria para la operación de los negocios de Colsubsidio debe contar con al menos un control de acceso para restringir personal no autorizado al centro de cómputo, centro de cableado y/o áreas restringidas que puedan afectar la operación, entre otros.
15. Debe existir protección contra factores ambientales (humedad, temperatura, entre otros) el cual debe ser óptimo para los equipos ofimáticos que se albergan en los centros de cómputo, centros de cableado, e infraestructura crítica para continuidad de la operación.
16. Cada UES es responsable de asignar los recursos necesarios para llevar a cabo lo indicado en los numerales 1 y 2 de este capítulo.
17. Todo ingreso de personas a los centros de cómputo y centros de cableado de la Caja, debe quedar registrado en la bitácora de ingreso. El responsable de administrar dicha bitácora será designado por la Gerencia de Tecnología.
18. El acceso físico a los centros de cómputo y cableado debe ser controlado mediante el uso de tarjeta electrónica, biométrico o llave (en caso de cuartos de cableado) y autorizado por la Gerencia de Tecnología.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

6.2 Seguridad de los Equipos

Audiencia: General

1. No se permite el uso de computadores, dispositivos móviles, periféricos y medios de almacenamiento extraíbles de propiedad del empleado en cualquiera de las sedes de Colsubsidio, sin autorización del jefe de área y la Gerencia de Tecnología. Si existe la


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

autorización, el dispositivo debe ser verificado previamente por el software Antivirus y está sujeto a monitoreo de su uso por parte de Seguridad de la Información.

2. Las UES de Colsubsidio están en la obligación de asignar los recursos necesarios para que el área de Seguridad Física pueda proporcionar unos controles mínimos de seguridad física para evitar robo, pérdida o manipulación de los activos de información, así mismo los empleados deben cumplir los controles dispuestos e informar irregularidades o deficiencias de los mismos a su jefe inmediato.
3. No está autorizado el uso de recursos informáticos (datos, hardware, software, redes, servicios, etc.) y de telecomunicaciones (teléfono, fax, etc.) para actividades que no estén autorizadas o relacionadas con el negocio de Colsubsidio o diferentes a las funciones asignadas al cargo que desempeña el funcionario.
4. Está prohibido que los usuarios realicen cualquier modificación en hardware o software de los recursos informáticos propiedad de Colsubsidio, dicha labor es exclusiva del personal autorizado por parte de la Gerencia de Tecnología.
5. Los equipos críticos definidos por la Jefatura de Seguridad de la información que contengan información confidencial deben contar con el cifrado de dispositivo.
6. Todos los equipos de cómputo que accedan a la red corporativa deben tener instalado el software antimalware corporativo en la última versión aprobada por la Jefatura de Seguridad de la información sin excepciones.
7. Los equipos de cómputo pertenecientes a Colsubsidio no deben conectarse a redes ajenas a las corporativas dentro de las instalaciones de Colsubsidio.


Audiencia: Tecnología.

8. Se debe eliminar toda la información confidencial y de uso interno que se

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

encuentra almacenada en los equipos informáticos que vayan a ser retirados de su uso a nivel corporativo según el procedimiento de borrado y disposición segura vigente, diligenciando el acta de sanitización correspondiente (TI.FC. E10.04)

9. Ningún software o hardware en general, podrá ser utilizado en Colsubsidio sin contar con los controles mínimos o (estándares de seguridad) establecidos por la Jefatura de Seguridad de la Información y sin previa autorización del Departamento de Operaciones de TI.
10. Los únicos responsables de manejo de contraseñas de administrador en la infraestructura tecnológica, con el propósito de realizar instalación, configuración, mantenimiento y

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

actualización de hardware y software debe ser exclusivo de los administradores de operaciones TI.


11. Cuando exista una actualización de seguridad crítica disponible para los equipos, el administrador es el responsable de su instalación en un plazo no mayor a 1 mes. El administrador también es responsable de evaluar en un ambiente controlado, el impacto de su implementación y asegurar que esta no afecte la operación normal.
12. Las actualizaciones de seguridad que no puedan ser instaladas deberán estar debidamente justificadas y la excepción será aprobada y documentada por la Jefatura de Seguridad de la información. El administrador debe proponer controles compensatorios en todos los casos.

7. SEGURIDAD DE LAS OPERACIONES

7.1 Copias de Seguridad (Backups)

Audiencia: General

1. Toda la información sensible que se encuentra almacenada en las plataformas tecnológicas de Colsubsidio y de proveedores, debe contar con actividades periódicas de backups para garantizar acciones de restauración confiables en casos de emergencia y según sea requerido y autorizado por el responsable del activo de la información.
2. Las UES son responsables de definir la política de backup adecuada y asignar recursos suficientes conforme a los requerimientos del negocio. La Gerencia de


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

Tecnología debe asegurar que los backups cumplan con lo requerido por los negocios.

3. Todo backup debe cumplir con el RPO (Punto de Recuperación Objetivo) definido por el negocio. Para los casos en los cuales esto no se cumple, el negocio debe aprobar y firmar la respectiva carta de aceptación de riesgos.

7.2 Instalación y uso de software


Audiencia: General

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

1. No se permite el uso de software de distribución gratuita, licencia libre, shareware, entre otros; a menos que haya sido previamente revisado y aprobado por el Departamento de Operaciones de TI y la jefatura de Seguridad de la Información.
2. Todas las adquisiciones de software deben estar avaladas por la Gerencia de Tecnología y por el líder del negocio o proceso corporativo.
3. No se permite descargar, instalar y/o ejecutar software sin la debida revisión y autorización del Departamento de Operaciones de TI y la Jefatura de Seguridad de la información.
4. Todo el software de Colsubsidio está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está prohibido hacer copias o usar este software para fines personales.
5. Los usuarios no deben escribir, compilar, copiar, propagar, ejecutar o intentar introducir de forma intencional algún código de programación diseñado para auto duplicarse, dañar, extraer información sin autorización o entorpecer el desempeño de cualquier sistema de información de Colsubsidio.

7.3 Uso de Portales Transaccionales


1. Los portales transaccionales deben tener publicado en su “home” la política de seguridad con alusión al uso de los activos de información de Colsubsidio, la cual debe ser de conocimiento de los clientes y afiliados y su aplicación es obligatoria.
2. Los portales de Colsubsidio deben contar con un aviso que comunique las políticas de seguridad aplicables.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

3. Todos los portales que soliciten información de carácter personal a los afiliados deben tener publicado un link a la política de tratamiento de datos de Colsubsidio y solicitar la debida autorización para dicho tratamiento.

7.4 Uso de Sistemas de Información

Audiencia: Afiliados

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

1. Los clientes y afiliados deben utilizar los sistemas de información y comunicación dispuestos por Colsubsidio solo para los fines establecidos por la Caja. Colsubsidio se reserva el derecho de tomar las acciones legales pertinentes para cualquier otra acción que pueda afectar los activos de información de Colsubsidio.
2. Se debe por parte de los clientes y afiliados cambiar la contraseña por lo menos semestralmente, con el fin de evitar accesos no autorizados.

7.5 Controles criptográficos


Audiencia: Tecnología

1. La Jefatura de Seguridad de la Información apoyará en la definición de los sistemas sobre los cuales se aplicarán controles criptográficos en conjunto con el Departamento de Operaciones de TI y la Jefatura de Arquitectura, según corresponda. Es responsabilidad del administrador del sistema aplicar y mantener dichos controles.
2. Todo sistema que use información confidencial debe tener controles criptográficos para los estados que aplique (almacenamiento, transmisión, acceso, captura, entre otros).

7.6 Registro y Seguimiento


Audiencia: Tecnología

1. Todos los sistemas de información de la Caja deben generar logs o registros de

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

toda la actividad realizada por usuarios, excepciones, fallas y eventos de seguridad de la información.

2. Se deben mantener los logs y monitorear con una frecuencia establecida.
3. Los sistemas y la información de registro se deben proteger contra modificación y acceso no autorizado.
4. Todas las actividades de los administradores y operadores de los sistemas se deben registrar. Estos registros deben estar protegidos y se deben revisar con una frecuencia establecida.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021


5. Los relojes de todos los sistemas de información de la Caja deben estar sincronizados para garantizar un correcto registro de eventos.

8. SEGURIDAD EN LA RED

8.1 Controles Generales

Audiencia: General


1. Está prohibido a los empleados y terceros que tengan acceso a la red inalámbrica o cableada de Colsubsidio, menoscabar o eludir los controles establecidos por la Caja para la protección de los activos de información.
2. Cualquier tipo de ataque, así como efectuar un escaneo, prueba o penetración de sistemas de computación, redes en Internet, o redes internas, está estrictamente prohibido, salvo en casos debidamente autorizados por la Jefatura de Seguridad de la Información y por requisitos propios del negocio.
3. Los sistemas de telecomunicación tales como módems, routers, switch, entre otros dispuestos por Colsubsidio, son los únicos autorizados para su uso en la red Corporativa.
4. Queda prohibido toda publicación o intercambio de información sensible de Colsubsidio a través de cualquier medio físico, magnético o electrónico sin el consentimiento y la respectiva autorización del propietario del activo de información y en cumplimiento de los controles establecidos para la protección de la información.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

8.2 Conexiones Remotas

Audiencia: Tecnología

1. Toda conexión remota a la red de Colsubsidio debe ser a través de canales seguros como VPNs o canales dedicados. Éstas deben solicitar autenticación para establecer la conexión remota a la red con el fin de prevenir accesos no autorizados.
2. El uso de la VPN es exclusivo de quienes no se encuentren dentro de la red LAN de Colsubsidio y deban hacer uso de sistemas de información de manera remota debido a las

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	


exigencias particulares de sus negocios. Adicionalmente, está permitido el uso de la VPN a quienes deban correr procesos en horarios no laborales. Todos los accesos por VPN deben ser autorizados por el propietario del activo de información.

3. Toda autorización para conexiones remotas por parte de proveedores debe tener una vigencia de acuerdo con el contrato, una contraseña de acceso y una cuenta de usuario que deberá ser bloqueada una vez finalizada las labores para las cuales se crea, conforme a la Política de Gestión de Accesos vigente.
4. Toda conexión remota sea de empleados o proveedores de Colsubsidio, será monitoreada y podrá ser bloqueada en caso de identificar situaciones inusuales respecto al uso de la cuenta y el acceso a los activos de información. Colsubsidio se reserva el derecho de acceso a la red, así como a tomar las acciones disciplinarias y legales definidas por la Jefatura de Seguridad de la Información, Talento Humano y el Área Jurídica.

8.3 Controles en la Red


Audiencia: Tecnología

1. Las redes de datos deben estar aisladas y divididas en zonas, según las necesidades de la Caja. Debe existir al menos una zona privada y una zona desmilitarizada (DMZ) que aisle los servicios que serán publicados hacia redes externas. Es responsabilidad del Área de Conectividad diseñar la red bajo el principio de acceso mínimo.
2. La red de gestión para los equipos de comunicaciones debe ser una red

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

únicamente destinada con este fin. En todos los casos posibles debe restringirse el acceso a la administración de equipos desde otras redes.

3. Todas las conexiones hacia proveedores o terceros deben aislarse por un firewall diferente al que se utiliza para acceder a internet y a cualquier otra conexión externa.
4. Las redes inalámbricas deben ser redes independientes de la red corporativa, por lo cual deben limitarse las conexiones entre la WLAN y las redes corporativas por medio de firewall. Se debe usar protocolos de cifrado fuerte para las redes inalámbricas.
5. Todos los equipos de comunicaciones deben ser monitoreados y deben tener logs activos. Los logs de monitoreo deben almacenarse por 1 año mínimo. Cualquier excepción debe ser autorizada por el Área de Conectividad y la Jefatura de Seguridad de la información. El log debe contar al menos con información de la fecha y hora, IP origen y destino, y tipo de evento.


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

6. En caso de detectar violaciones a las políticas y procedimientos establecidos o al realizar un mal uso de la red el Área de Conectividad y la Jefatura de Seguridad de la Información procederán a restringir el acceso inmediatamente.

9. SEGURIDAD EN LOS DESARROLLOS


Audiencia: Tecnología

1. Se deben identificar los activos de información y los riesgos asociados para nuevos desarrollos o proyectos, con el fin de establecer los controles para el aseguramiento de la información. Esto es responsabilidad del negocio, el Jefe de TI del negocio, la Jefatura de Arquitectura y la Jefatura de Seguridad de la Información.
2. Los aplicativos de Colsubsidio deben pasar por un proceso de pruebas y aceptación en un ambiente dedicado para tal fin antes de ser liberados a producción.
3. El acceso a la información contenida en las bases de datos sólo está permitido a través de las aplicaciones de los sistemas de Colsubsidio. Sólo tendrán acceso los usuarios autorizados.
4. Con el fin de preservar la confidencialidad de la información, a efectos de no vulnerar las condiciones de seguridad de acuerdo con su clasificación, la información que está en producción no debe ser utilizada para desarrollo o pruebas. En algunas situaciones, las casuísticas de las pruebas funcionales requieren el uso de datos de producción por lo que en caso de ser necesario tener datos real en el ambiente de pruebas, es imprescindible el ofuscamiento de dicha información. Para realizar el ofuscamiento se deben considerar los campos que contienen información sensible de afiliados, clientes o

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	


colaboradores.

5. Es responsabilidad de los desarrolladores (internos o externos) considerar la seguridad de la información desde el inicio del proceso de diseño de los sistemas de Colsubsidio, pasando por cada una de las fases de desarrollo hasta su liberación a producción.
6. Los sistemas de procesamiento y almacenamiento de información de los sistemas operativos y aplicaciones, deben contar con los últimos parches de seguridad provistos por el fabricante debidamente aprobados e instalados, con el fin de dar el aseguramiento adecuado.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

7. No está permitido el acceso a personal no autorizado a editores, compiladores o cualquier otro tipo de utilitarios que estén asociados al ambiente productivo, cuando no sean indispensables para el funcionamiento del mismo.
8. Se debe contemplar en el mantenimiento y en la fase de los desarrollos, el establecimiento de buenas prácticas que provean el diseño, aseguramiento y ejecución para la protección de la información a través de buenas prácticas como OWASP, Microsoft SDL, BSIMM, entre otras. Es responsabilidad de los desarrolladores y administradores de las aplicaciones remediar las vulnerabilidades que sean detectadas.
9. Todos los sistemas de Colsubsidio deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información.
10. Se debe garantizar en los desarrollos y nuevos sistemas en Colsubsidio los siguientes registros de auditoría: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad y cualquier otro definido por la Jefatura de Seguridad de la Información.
11. En las configuraciones de seguridad del software o la aplicación, se debe incluir un parámetro de bloqueo de sesión (timeout) cuando no se detecte actividad del usuario.
12. Para aplicaciones que usen tecnología de validación biométrica el bloqueo de sesión (time out) debe ser de cinco minutos.


10. RELACIONES CON PROVEEDORES

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

10.1 Controles Generales

Audiencia: Proveedores, aliados estratégicos y subcontratistas


1. Los proveedores, aliados estratégicos y subcontratistas que manejen información de o a cargo de la Caja, deben cumplir con las leyes, normas y regulación colombiana en cuanto al manejo de la información. A su vez, deben contar con protocolos para el manejo seguro de la información y permitir su verificación por parte de la Jefatura de Seguridad de la Información antes de formalizar el contrato o acuerdo y durante su vigencia.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

2. Los Proveedores o Contratistas deben informar inmediatamente al gestor de contrato cualquier incidente que afecte la confidencialidad, integridad y disponibilidad de los activos de información, que ponga en riesgo la operación de Colsubsidio. La solicitud de requerimientos e incidentes debe estar totalmente alineados con las políticas corporativas.
3. Un Proveedor de Servicios que realice servicios relacionados con almacenamiento, transmisión o procesamiento de datos de tarjetahabientes, debe cumplir con la Norma de Seguridad de Datos de la PCI y anualmente deben demostrar el acatamiento con la Norma de Seguridad de los Datos (AOC) de la PCI.


Audiencia: Áreas de la Caja responsables de contratos, Gerencia de servicios Administrativos y Supervisores de contratos.

4. Cada UES o área de la caja que contrate a un tercero para soportar actividades propias de sus procesos, debe asignar de su área, un empleado supervisor o interventor, que sea responsable durante toda la vigencia del contrato:
 - Gestionar ante la Gerencia de Servicios Administrativos la inclusión de requisitos para el manejo seguro de la información y cláusulas aplicables al servicio contratado para su uso y tratamiento durante y posterior a la finalización de la relación contractual; estos requisitos deben ser informados y validados por la Jefatura de Seguridad de la Información y estar acorde con los protocolos y herramientas vigentes al interior de la Caja,
 - Reportar oportunamente a la Gerencia de TI a través de los canales dispuestos, las novedades de los empleados del tercero (ingresos,

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021
		Código: TI.PO.02
		Versión: 3

retiros, cambios de cargo, vacaciones, etc.)


- indicar a la Gerencia de Servicios Administrativos cuales, de los aliados estratégicos y proveedores, con relación contractual vigente, tienen acceso a información del o a cargo de la Caja y si el aliado o el proveedor tiene un subcontratista que participe en el servicio y tenga acceso a la información. Lo anterior con el propósito de validar el cumplimiento de los protocolos de manejo seguro de información.
- vigilar y hacer seguimiento periódico al desempeño de los acuerdos de confidencialidad, acuerdos de niveles de servicio, intercambio de información y el cumplimiento de los controles de seguridad de la información.
- controlar los accesos físicos o lógicos de los proveedores y subcontratistas que accedan a la infraestructura física y/o tecnológica de la Caja.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

- reportar los eventos que afecten la seguridad de la información originados durante la prestación del servicio a la Jefatura de Seguridad de la Información.
5. Las áreas de la Caja responsables de contratos, a través del colaborador supervisor del contrato, deben gestionar la inclusión en los contratos de acuerdos de niveles de servicio, planes de continuidad de negocio y de contingencia tecnológica, si aplica.
 6. La Gerencia de Servicios Administrativos debe incluir en el inventario de proveedores y aliados estratégicos el detalle del tipo de información que se maneja (pública, de uso interno, privada o confidencial) o especificar que no se entrega información en desarrollo del objeto del contrato, de acuerdo con los servicios suministrados a la Caja.

10.2 Acuerdos de confidencialidad

1. La Gerencia de Servicios Administrativos, debe incluir acuerdos de confidencialidad en aquellos contratos y acuerdos de servicio en donde se intercambie información pública, de uso interno, privada o confidencial, mediante los cuales se comprometa al proveedor y sus empleados y a los subcontratistas (si los hubiere) a guardar absoluta reserva sobre toda la información que le sea dada a conocer con ocasión del desarrollo del servicio contratado.


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

11. SEGURIDAD EN LA NUBE

11.1 Controles Generales

Audiencia: Empleados y contratistas.

1. Toda contratación de servicios en la nube debe estar avalada y autorizada por la Gerencia de Tecnología de la caja.
2. Toda la información almacenada en la nube debe estar identificada, clasificada y valorada acorde con el procedimiento de gestión de activos de información definido por Colsubsidio.
3. El proveedor de servicios en la nube debe contar y mantener vigente, al menos, la certificación ISO 27001, y de observancia a los estándares o buenas prácticas, tales como


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

Código:
TI.PO.02

Versión:
3

ISO 27017-Controles de Seguridad para Servicios Cloud y 27018-Protección de la Información de Identificación Personal (PII) en la nube. El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3).

4. El proveedor debe ofrecer una disponibilidad de al menos el 99.95% en los servicios prestados en la nube y establecer mecanismos que permitan contar con respaldo de la información que se procesa en la nube, la cual debe estar a disposición de Colsubsidio cuando así lo requiera.
5. Se debe verificar que las jurisdicciones en donde se procesará la información cuenten con normas equivalentes o superiores a las aplicables en Colombia, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.
6. El proveedor de servicios en la nube debe garantizar la independencia de la información y de las copias de respaldo de las otras entidades que procesen en la nube. La independencia se puede dar a nivel lógico o físico.
7. El proveedor de servicios en la nube debe mantener cifrada la información clasificada como confidencial en tránsito o en reposo, usando estándares y algoritmos reconocidos internacionalmente que brinden al menos la seguridad ofrecida por AES, RSA o 3DES.
8. Gestión de accesos y los administradores de TI deben tener bajo su control la administración de usuarios y privilegios para el acceso a los servicios ofrecidos, así como a las plataformas, aplicaciones y bases de datos que operen en la nube, dependiendo del modelo de servicio contratado.
9. El Departamento de Operaciones de TI debe monitorear los servicios contratados para detectar operaciones o cambios no deseados y/o adelantar


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

las acciones preventivas o correctivas cuando se requiera.


10. Se deben establecer procedimientos para verificar el cumplimiento de los acuerdos y niveles de servicio establecidos con el proveedor de servicios en la nube y sus subcontratistas o aliados estratégicos, cuando sean estos quienes prestan el servicio.

11.2 Acuerdos o contratos para servicios de computación en la Nube.

Los acuerdos o contratos que suscriba Colsubsidio para la prestación de servicios de computación en la nube deben contemplar como mínimo los siguientes elementos:

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	


- Las condiciones referentes a capacidad, disponibilidad, tiempos de recuperación, la existencia de planes de continuidad, resolución de incidentes y horarios de atención del proveedor del servicio, las cuales deben prever niveles de servicio que permitan cumplir, cuando menos, con las políticas señaladas en el numeral de Seguridad en la nube de este documento.
- Las condiciones de seguridad de la información y ciberseguridad de los servicios en la nube y las condiciones establecidas para proteger la privacidad y confidencialidad de los datos de los clientes, las cuales deben prever niveles de servicio que permitan cumplir, cuando menos, con las políticas señaladas en el numeral de Seguridad en la nube de este documento.
- La propiedad de la información que se procese en los servicios de computación en la nube, haciendo claridad que los datos son propiedad de Colsubsidio y que no se pueden usar para ningún propósito diferente al establecido en el contrato.
- Las condiciones y limitaciones bajo las cuales se puede subcontratar parte del servicio o realizar cambios a los acuerdos establecidos con sus subcontratistas o aliados estratégicos.
- La entrega a Colsubsidio de informes y certificaciones que demuestren la calidad, desempeño y efectividad en la gestión de los servicios contratados, así como la vigencia de las certificaciones enunciadas en el numeral Seguridad en la Nube de este documento
- La obligación del proveedor del servicio de informar, en cuanto le sea posible, a Colsubsidio sobre cualquier evento o situación que pudiera afectar significativamente la prestación del servicio.
- El borrado seguro de los datos existentes en los medios de almacenamiento cuando finalice el contrato, cuando lo solicite Colsubsidio o cuando el proveedor de servicios en la nube elimine y/o reemplace dichos medios.
- La corrección oportuna y eficaz de las vulnerabilidades informáticas detectadas.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

- La utilización de técnicas de múltiple factor de autenticación para el acceso a las consolas de administración por parte de Colsubsidio.

12. INCIDENTES DE SEGURIDAD


Audiencia: General

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	GERENCIA CORPORATIVA DE TECNOLOGÍA		Código: TI.PO.02
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	Versión: 3

1. Los empleados que utilicen sistemas de información de Colsubsidio deben reportar cualquier amenaza o debilidad en los sistemas o servicios, a la Mesa de Servicio o a la Jefatura de Seguridad de la Información.
2. Los incidentes de seguridad que afecten los activos de información y que deban ser manejados con la participación de la mesa de ayuda, deben mantenerse en estricta confidencialidad, por lo que queda expresamente prohibido divulgarlos a personal no autorizado, a menos que haya sido formalmente autorizado por la Jefatura de Seguridad de la Información.
3. Se debe reportar a la mesa de ayuda, cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad y/o disponibilidad de los activos de información de Colsubsidio, siguiendo el Procedimiento de Gestión de Incidentes de Seguridad de la Información. (TI.PC.E12.05)


13. SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

1. Cada UES es responsable de definir y mantener un proceso para la continuidad del negocio basado en los siguientes aspectos:
 - Entender los riesgos en los procesos de su negocio y su impacto, incluyendo la identificación y sensibilidad de sus procesos críticos.
 - Entender el impacto de las interrupciones o incidentes de seguridad en las actividades del negocio.
 - Formular y documentar planes estratégicos de continuidad del negocio acorde con los objetivos y prioridades de la misma y de Colsubsidio.
 - Asegurar que la administración de la continuidad del negocio sea

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

incorporada en sus procesos y estructura.

- Asignar responsabilidades para la coordinación y administración del plan de continuidad del negocio.
- Los planes de continuidad del negocio deben ser documentados, probados y evaluados por lo menos una vez al año para verificar su funcionamiento adecuado. Estos deben considerar:
 - Condiciones para la activación.
 - Estrategia de recuperación ante desastres.
 - Identificación de responsabilidades y procedimientos de emergencia.


	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

- Planes contingencia de los procesos y tecnológicos. Procedimientos de regreso a la operación normal.
 - Cronograma de pruebas de continuidad de negocio.
 - Roles y responsabilidades individuales de ejecución y propietarios de cada programa.
2. Los planes de continuidad deberán estar almacenados en un lugar seguro dentro de Colsubsidio. Adicionalmente deberá existir una copia en sitio alterno a fin de recuperar las operaciones del negocio en caso de que la contingencia afecte las instalaciones de la Caja, de igual forma debe ser de conocimiento de todos los empleados y distribuido según su inherencia a toda la estructura de Colsubsidio.
 3. Los terceros contratados deben tener planes de continuidad debidamente documentados y se debe garantizar su funcionamiento, con el fin de dar continuidad a las operaciones críticas del negocio.

14. CUMPLIMIENTO REGULATORIO


Audiencia: General

1. Colsubsidio velará por el cumplimiento de las Políticas Seguridad de la

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021


Información estipuladas por la Caja y la legislación aplicable vigente por los entes de control.

2. La Jefatura de Seguridad de la Información en conjunto con el Área Jurídica, determinarán los requisitos que sean de cumplimiento obligatorio y emitidos por entes gubernamentales o privados y cualquier disposición colombiana vigente, definirán e implementarán los controles necesarios para dar cumplimiento y protección a los activos de información.
3. Todos los empleados están obligados a ceder a Colsubsidio los derechos exclusivos de propiedad literaria, licencias, invenciones, u otra propiedad intelectual que ellos creen o desarrollen durante su periodo laboral con la Caja. En el caso de aplicaciones de terceros, este aspecto se registrará por las condiciones y cláusulas establecidas en el contrato de adquisición de productos y/o servicios, con la finalidad de prevenir cualquier disputa

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Código: TI.PO.02	Versión: 3
Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021	

respecto a la propiedad del software, licencias, entre otros, una vez que el proyecto sea completado.


4. Colsubsidio tiene propiedad legal de la información Corporativa almacenada, enviada y compartida en todos sus computadores, sistemas de información y comunicación que hayan sido transmitidos por medio de estos recursos, por lo cual se reserva el derecho de acceder a esta información sin autorización del autor o usuario del recurso, así como también se reserva el derecho de disponer de toda la información corporativa que cualquier empleado haya colocado en los medios de comunicación existentes en Colsubsidio, conforme a la legislación vigente.
5. Colsubsidio se reserva el derecho de monitorear cualquier sistema que sea de su propiedad en caso de presentarse incidentes de seguridad que afecten la seguridad de la información de la Caja.
6. El Departamento de Operaciones de Tecnología deberá revisar periódicamente los acuerdos de licencias de hardware y software instalado a fin de verificar el cumplimiento de los mismos por parte de Colsubsidio.
7. Los contratistas y terceras partes deben cumplir con las disposiciones establecidas por la Legislación Colombiana vigente asociados a la de protección de datos personales, propiedad intelectual y seguridad de la información.
8. Toda información debe mantenerse de acuerdo a las tablas de retención de Gestión Documental. Es responsabilidad de las UES proporcionar la información necesaria para la actualización de dichas tablas, así como informar al Departamento de Operaciones de Tecnología sobre los requerimientos para respaldo que pueda tener la información corporativa.
9. Sea con notificación formal o por medio de detección, Colsubsidio tomará las medidas necesarias, incluyendo, pero no limitándose a desconexión del acceso a internet o bloqueo del acceso a los sistemas de información, con el fin de detener la descarga o distribución de material protegido por derechos de autor en las redes y

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

sistemas de Colsubsidio.

15. ENTRADA EN VIGENCIA DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

La omisión por parte del trabajador en las obligaciones y responsabilidades definidas en esta política será considerada falta grave y por ende, conllevará a la implementación de las medidas pertinentes por parte de la Gerencia Corporativa de Talento Humano.

	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	GERENCIA CORPORATIVA DE TECNOLOGÍA	
	Emitido: Septiembre de 2021	Actualizado: Septiembre de 2021

La presente política aplica a partir del día XXX de 2020 y se revisará de manera anual por la Jefatura de Seguridad de la Información. El monitoreo de cumplimiento a la presente política estará en cabeza del Comité de Seguridad de la Información o a quien este designe.

APROBADO POR:

DIRECTOR ADMINISTRATIVO

SUBDIRECCIÓN GESTION ORGANIZACIONAL

GERENCIA DE TECNOLOGIA