1. OBJETIVO

Establecer lineamientos necesarios, con el fin de garantizar la seguridad de la información digital de COMCE-SOLDICOM, basado en la identificación y valoración de los riesgos asociados a este proceso.

2. ALCANCE

Aplicable a todos los procesos, así como a todos los aspectos administrativos, contractuales y de control que deben ser cumplidos por los colaboradores de COMCE-SOLDICOM.

3. DEFINICIONES

- **Administración de Riesgos:** Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Control:** Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Confiabilidad de la Información:** Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Incidente de Seguridad:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Impacto:** Resultado de un incidente de seguridad de la información.
- **Privacidad de la información:** El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Propietario de la información (titular):** Es la unidad organizacional o proceso donde se crean los activos de información.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

- **VPN:** Red virtual privada por sus siglas en ingles Virtual Private Network.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. RESPONSABILIDADES Y AUTORIDADES

Presidencia Ejecutiva: Encargada de realizar la valoración de la documentación producida y recibida en cada una de las dependencias de COMCE-SOLDICOM, en los diferentes soportes, tanto virtuales como en papel, desde su origen hasta su disposición final, con el objeto de facilitar su uso y garantizar la seguridad de la información.

Dirección de comunicaciones: Encargada de llevar a cabo la implementación de los lineamientos generales prescritos en este Procedimiento de Seguridad de la Información de COMCE-SOLDICOM.

Coordinadores y directores de proyectos: Los directores de los distintos proyectos que se ejecutan por parte de COMCE-SOLDICOM, serán responsables de velar por el correcto cargue de la documentación a la nube de cada uno de sus servidores, con la información requerida, a efectos de verificar el cumplimiento de la aplicación del presente procedimiento.

Todos los niveles de la organización: Todos los colaboradores, contratistas y trabajadores en misión, son responsables de Salvaguardar la información suministrada por COMCE-SOLDICOM, que se deriven del ejercicio de sus funciones, en cumplimiento del presente Procedimiento de Seguridad de la información.

5. DESARROLLO

5.1 GESTIÓN DE COPIAS DE SEGURIDAD

Con el objetivo de seguir optimizando y asegurando una gestión eficiente de la información, así como brindar una herramienta de seguridad de la información digital que se genera en los distintos procesos adelantados por COMCE-SOLDICOM, se ha desarrollado y actualizado la siguiente estrategia integral para mejorar el manejo de copias de seguridad en los diferentes equipos de trabajo:

5.1.1 Procedimientos de copia de seguridad.

Se socializará el procedimiento definido para realizar copias de seguridad en el Drive de los archivos locales de cada equipo. Esto incluirá la frecuencia de las copias, los tipos de archivos a respaldar y las herramientas a utilizar.

5.1.2 Implementación de unidades en Drive.

Se crearon y actualizaron las unidades compartidas en la suite de Google Drive de cada proyecto de COMCE-SOLDICOM, que sirven como repositorio principal para las copias de seguridad. se instruye a los equipos sobre cómo acceder y utilizar estas unidades de manera efectiva.

- **Gestión de acceso de usuarios:**

✓ La Dirección de Comunicaciones sólo otorgará a los usuarios, los accesos solicitados y autorizados por el jefe inmediato.
✓ La Dirección de Comunicaciones debe garantizar que las estaciones de trabajo con perfil de administrador local sean las que estén autorizadas, en caso contrario se debe modificar el permiso en la configuración de la estación de trabajo.

5.1.3 Inducción en la ruta de archivos y acceso al Drive.

Se realizará una sesión de inducción general en la que se explicará a los equipos la estructura de carpetas y la jerarquía de archivos en las unidades compartidas de Drive. Además, se brindará orientación sobre la forma de realizar subidas, descargas seguras y eficientes. También se establecerá un cronograma para que cada área de trabajo actualice la información que tiene alojada en las unidades compartidas. Se alimentará el formato de inventario de equipos de cómputo, en el cual está definida la ruta a utilizar, para salvaguardar la información de cada proyecto.

5.1.4 Capacitación permanente

Se brindará información cuando se requiera a los trabajadores de COMCE, con el fin de mantener a los equipos actualizados sobre las mejores prácticas para realizar copias de seguridad y el uso eficiente de las herramientas en la nube. Esto garantizará que todos los miembros del equipo estén al tanto de cualquier cambio o mejora en el proceso.

5.1.5 Monitoreo y evaluación regular

Se implementará un monitoreo constante para asegurarse de que los procedimientos de copia de seguridad se sigan de manera adecuada. Se realizarán revisiones regulares para identificar posibles fallas y oportunidades de mejora.

5.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

5.2.1 Usuarios únicos.

Cada usuario tendrá asignado un único correo de identificación para tener acceso al DRIVE que utilice. El cual será asignado con diferentes roles para administrar cada uno, ejemplo: Unidad de coordinación de comunicaciones, coordinación de Planeación y seguimiento presupuestal, coordinación Jurídica, etc.

5.2.2 Creación y salvaguarda de la información en el DRIVE.

Los responsables de cada proyecto y los que hagan parte de este, deberán asegurar la correcta administración de los usuarios de DRIVE siendo los únicos autorizados para crear, eliminar o inhabilitar los mismos. Bajo la supervisión y acompañamiento del desarrollador web y tecnologías o del área de comunicaciones.
Todos los archivos de datos y las bases de datos criticas utilizadas por los proyectos de la entidad, deberán contar con el respaldo necesario para recuperase en caso de imprevistos o ataques a la seguridad de la información.

5.2.3 Bases de datos a terceros.

Está prohibida la entrega de las bases de datos de la entidad a proveedores, contratistas y en general a terceras personas para efectos de revisión, pruebas o verificación de datos. En caso de ser necesario que terceras partes requieran las bases de datos, la Presidencia Ejecutiva deberá proporcionar una forma segura mantenimiento los lineamientos de seguridad de la información establecidos en Manual de Protección de Datos.

5.2.4 Seguridad física de los equipos Portátiles.

Los colaboradores deberán procurar la seguridad física de los equipos portátiles cuando se encuentre fuera de las instalaciones.

Es responsabilidad de los trabajadores de COMCE-SOLDICOM la conservación y uso correcto de los equipos suministrados. Deberán ser utilizados únicamente para fines del negocio aprobados por la entidad y deberán someterse a todas las instrucciones técnicas que se impartan. El producto del uso de dichos recursos de tecnología de la información será de propiedad de la entidad.

5.2.5 Reporte de incidentes de seguridad

Los empleados deberán reportar cualquier incidente, vulnerabilidad o riesgo potencial que afecte la seguridad de la información.

5.2.6 Notificación de terminación de contrato

Una vez el trabajador termine su contrato laboral, deberá dentro el proceso de desvinculación laboral diligenciar el respectivo paz y salvo, posterior al bloqueo de los privilegios y accesos proveídos a su nombre y de la devolución de los activos de información. Gestión Humana de SMT, realizará su respectivo proceso salvaguardando los equipos portátiles.

Todos los activos de información provistos a los trabajadores, tales como equipos portátiles, tarjetas de identificación, software, datos, documentación, manuales etc., deberán ser entregados apropiadamente y de forma inmediata en el momento de la terminación del contrato.

5.3 USO DEL CORREO ELECTRÓNICO CORPORATIVO.

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal. Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo diariamente. Así mismo, es su responsabilidad mantener espacio libre en el buzón. Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos, personales, en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres. En

el caso de recibir un correo no deseado o no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al oficial de seguridad de la información.

Los mensajes que formen parte de un procedimiento administrativo, u otros que se tengan que conservar, sólo se pueden eliminar de la cuenta de correo si previamente han sido debidamente archivados en la carpeta que corresponda para dicho fin.

Al trabajador que se le asigne una cuenta de correo electrónico corporativo de la entidad es responsable de:

- Conservar el usuario y contraseña de acceso a su correo electrónico de forma secreta y segura, además de no facilitar en ningún momento esta información a terceros.
- No utilizar una contraseña poco segura o fácilmente deducible.
- No seguir cadenas de mensajes.
- No abrir mensajes sospechosos. Comunicarlo de forma inmediata y directa a comunicaciones y presidencia.

5.4 REDES SOCIALES

El uso y publicación de información en las redes sociales deberá ser controlado de tal forma que no comprometa la seguridad de la información de la entidad.

Solo los usuarios autorizados por la Presidencia Ejecutiva podrán hacer uso de las redes sociales de COMCE-SOLDICOM y deberán emplear contraseñas “fuertes” para su uso. Se procurará controlar el acceso restringido de forma automática a través de filtrado de contenido.

5.5 CUMPLIMIENTO Y SANCIONES.

Todos los trabajadores de COMCE-SOLDICOM, los contratistas, proveedores deben cumplir y acatar el presente procedimiento en materia de protección y seguridad de la información.

El incumplimiento de algún lineamiento de seguridad de la información por un trabajador, proveedor o contratista es causal para iniciar acciones disciplinarias o contractuales, las cuales de acuerdo con su gravedad pueden derivar la terminación de la vinculación laboral del empleado y los contratistas y/o proveedores la terminación del contrato suscrito con la COMCE-SOLDICOM.

6. REGISTROS DE CREACIÓN Y/O CAMBIOS

Versión	Fecha	Actualización / Cambio	Realizó
01	14/09/2023	Creación del documento	Mauricio Veloza Coordinador de comunicaciones
02	15/04/2024	Actualización Logo, desarrollo del proceso y cambio de codificación	Adriana Arango Coordinadora de comunicaciones