TABLA DE CONTENIDO

1. ANTECEDENTES

En el creciente uso del entorno digital para el desarrollo de las actividades diarias de las entidades o personas del común, es necesario tener en cuenta el acarreo de incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos de tipo económico, político, social afectando la integridad de los ciudadanos en ese entorno. Es por eso que el Gobierno Nacional ha dispuesto de una política de seguridad de la información Nacional con el fin de promover una gestión de riesgos de seguridad digital y unas políticas de seguridad para garantizar la protección y la seguridad de las personas y la infraestructura.
Tal y como lo establece la política de seguridad nacional en el CONPES 3854 de 2016 en su última actualización.

Además de esto el Ministerio de Tecnologías de la Información con los Decretos 1078 y 2573 del 2014 reglamenta fuertemente el tema de la seguridad de la información en las entidades públicas, con el fin de proteger y resguardar los bienes del estado Colombiano. El ministerio de TIC también dispone del Modelo de Seguridad de TI, el cual se encuentra acorde a las buenas prácticas de seguridad y es actualizado permanentemente con los requerimientos técnicos de las normas 27001 de 2013, Ley 1581 de 2012 Protección de datos personales, Ley 1712 de 2014 Transparencia y Acceso a la Información Pública entre otras.

2. PROPÓSITO

La Unidad Administrativa Especial de Organizaciones Solidarias tiene como finalidad aplicar los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios en línea e infraestructura en general con el propósito fundamental de preservar la confidencialidad, integridad y disponibilidad de los activos de información con los que cuenta la entidad. El presente documento establece las políticas de seguridad de la información las cuales deben ser adoptadas por los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la entidad teniendo en cuenta los lineamientos dados por la presente política con el fin de proteger los activos de información contra amenazas, asegurando la continuidad de sus operaciones, minimizando los riesgos y maximizando la eficiencia y las oportunidades de mejora de la gestión de la organización, cumpliendo de esta manera con la misión de la entidad y los objetivos estratégicos establecidos por el Plan Estratégico Institucional.

3. ALCANCE

Las Políticas de Seguridad y Privacidad de la Información son extensibles y aplicables a todos los procesos administrativos, misionales y de control de la entidad, estas deben ser acatadas y cumplidas por la Alta Dirección, Asesores, Directores, Secretarios, Coordinadores, funcionarios, contratistas, terceros, aprendices, practicantes y proveedores que presten sus servicios o tengan algún tipo de relación con la Unidad Administrativa Especial de Organizaciones Solidarias, para el apropiado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de los activos de información de la entidad.
Teniendo en cuenta los lineamientos establecidos en el modelo de seguridad de TI establecido por el Ministerio de Tecnologías de la Información y las mejores prácticas de gestión de seguridad de la información.
Los usuarios tienen la obligación de conocer, acatar y dar cumplimiento a las presentes políticas emitidas y aprobadas por el Comité Institucional de gestión y desempeño de la Unidad Administrativa Especial de Organizaciones Solidarias.

4. DEFINICIONES

• **ACCION PREVENTIVA:** Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencialmente no deseable. Definición tomada de la Norma Técnica Colombiana NTC-ISO9000:2005, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

• **ACTIVO:** Son recursos controlados por la entidad que resultan de un evento pasado y de los cuales se espera obtener potencial de servicio o generar beneficios económicos futuros.

• **AMENAZA:** Todo elemento o acción capaz de atentar contra la seguridad de la información.

• **CARACTERÍSTICAS DE LA INFORMACIÓN:** Las principales características desde el enfoque de seguridad y privacidad de la información son: Confidencialidad, Integridad y Disponibilidad.

• **CONFIDENCIALIDAD:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

• **CUSTODIOS DE LA INFORMACIÓN:** Es el funcionario o grupo de funcionarios a los cuales se les deja en posesión y responsabilidad de velar por la seguridad de la información que no les pertenece. Los custodios de la información física son los responsables de protegerla y resguardarla de accesos indebidos o no autorizados.

• **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad o persona autorizada.

• **INCIDENTE:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

• **INTEGRIDAD:** Propiedad de la información relativa a su exactitud y completitud.

• **INVENTARIO DE ACTIVOS DE INFORMACIÓN:** Lista de todos aquellos recursos (físicos, de información, hardware, software, personas…) dentro del alcance del SGSI, que tengan valor para la entidad y necesiten ser protegidos de riesgos potenciales.

• **INFORMACIÓN PÚBLICA RESERVADA:** Es aquella información que estando en custodia de un sujeto obligado en su calidad de tal, es negado el acceso a la ciudadanía por daño a intereses públicos y bajo el cumplimiento de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

• **INFORMACIÓN PÚBLICA CLASIFICADA:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o sami-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.

• **ISO/IEC 27001:** Norma que establece los requisitos para un sistema de gestión de seguridad y privacidad de la información SGSI. La primera publicación es del 2005; segunda edición 2013. Es la norma base en la cual se certifican los SGSI a nivel mundial.

• **PLAN DE CONTINUIDAD DEL NEGOCIO:** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

• **PROPIETARIO O DUEÑO DE LA INFORMACIÓN:** Es el funcionario o grupo de funcionarios responsables de cuidar, mantener y actualizar los principios de confidencialidad, disponibilidad e integridad de la información o datos a su cargo. Se encargan de definir que usuarios deberán tener permisos de acceso a la información conforme a sus funciones y competencia.

• **ISO/IEC 27002:** Código de buenas prácticas en gestión de seguridad y privacidad de la información. No es certificable.

• **SEGURIDAD DE LA INFORMACIÓN:** Consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información, así como los sistemas implicados en su tratamiento, dentro de la entidad.

• **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI:** Conjunto de elementos interrelacionados entre sí, que basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa y mantiene la seguridad de la información.

• **TELETRABAJO:** Es una forma de organización laboral que se efectúa en el marco de un contrato, que consiste en el desempeño de actividades remuneradas utilizando como soporte las tecnologías de la información y las comunicaciones, para el contacto entre el empleador y el trabajador sin requerirse la presencia física de éste en un sitio especifico de trabajo.

• **TELETRABAJADOR:** Es aquella persona que utiliza las tecnologías de la información para la realización de su profesión. Esta actividad se realiza fuera del establecimiento empresarial.

• **USUARIOS:** Es cualquier funcionario o persona que interactúe con los sistemas de información y datos de la Unidad Administrativa Especial de Organizaciones. Son considerados como los consumidores de la información y deben velar por la preservación de la clasificación de la información en su uso cotidiano.

• **VULNERABILIDAD:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. DECLARACIÓN

LA UNIDAD ADMINISTRATIVA ESPECIAL DE ORGANIZACIONES SOLIDARIAS, para el cumplimiento de su misión, visión, objetivos estratégicos, y apegada a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de proteger los activos de información contra amenazas, asegurar la continuidad de sus operaciones, minimizar los riesgos a la Unidad y maximizar la eficiencia y las oportunidades de mejora de la gestión de la organización.

A continuación, se desglosan las políticas que conforman la política de seguridad y privacidad de la información general de la entidad:

• Política de Gestión de la Unidad Administrativa Especial de Organizaciones Solidarias
• Política de Activos de Información
• Política de Uso de Carpetas Compartidas
• Política de Operaciones de TICS
• Política de Seguridad de Equipos Tecnológicos
• Política de Respaldo de la Información
• Política de Uso de Correo Electrónico
• Política de Uso de Intranet/Internet
• Política de Aplicaciones
• Política para el Uso de Medios Removibles
• Política de Escritorio y Pantalla Limpia
• Política de Teletrabajo

5.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE ORGANIZACIONES SOLIDARIAS

En el ejercicio del cumplimiento de la misión de la Unidad Administrativa Especial de Organizaciones Solidarias se generan bases de datos de la población y organizaciones solidarias beneficiadas de los procesos de la entidad, esta información **NO PUEDE SER PUBLICADA O UTILIZADA PARA FINES COMERCIALES, ÚNICA Y EXCLUSIVAMENTE** para el fomento de las Organizaciones Solidarias, respetando la confidencialidad y los datos personales de carácter sensible de los que se tenga conocimiento en el desarrollo de sus actividades, igualmente tendrá sumo cuidado para que sus actos o acciones no se tipifiquen en una conducta descrita en la Ley 1273 de 2009 como en la Ley 1581 de 2012.
La entidad podría intercambiar información con otras entidades públicas que contribuyan con la labor de fomento de las Organizaciones Solidarias.

Así mismo la entidad con fines estadísticos cuenta con información del registro de entidades solidarias, dicha información es utilizada para la generación de reportes estadísticos, la cual no podrá ser intercambiada con ninguna entidad pública o privada en cumplimiento con lo establecido con CONFECÁMARAS.

En las actividades que la Unidad Administrativa Especial de Organizaciones Solidarias adelante en territorio nacional y en las que consolide información tanto de las personas beneficiadas y organizaciones solidarias, es primordial y necesario contar con la autorización de éstas para el manejo interno de la información.

5.2. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

Inventario de Activos de Información: La Unidad Administrativa Especial de Organizaciones Solidarias mantendrá actualizado el inventario de activos de información, bajo la responsabilidad de los propietarios de la información y centralizado por el grupo de Tecnologías de la Información.

Propietarios de los activos de información: La Unidad Administrativa Especial de Organizaciones Solidarias es el dueño de la propiedad intelectual de los avances, innovaciones y descubrimientos realizados por los funcionarios de la entidad, y los contratistas derivados del objeto del cumplimiento de funciones o tareas asignadas, para el cumplimiento del objeto del contrato.

5.3. POLÍTICA DE USO DE LOS ACTIVOS DE INFORMACIÓN

• Los funcionarios, contratistas y terceros que tengan acceso a las instalaciones de la Unidad Administrativa Especial de Organizaciones Solidarias deberán utilizar únicamente los programas autorizados por el Grupo de Tecnologías de la Información.

• Los funcionarios y contratistas de la Unidad Administrativa Especial de Organizaciones Solidarias deberán solicitar mediante el aplicativo de Mesa de Ayuda requerimientos como:
Registro biométrico para acceso a las instalaciones de la entidad, estas podrán solicitarse únicamente por los coordinadores de cada grupo.
Cancelación de registros biométricos una vez los funcionarios o contratistas se desvinculen de la entidad.
Soporte técnico a equipos de cómputo, impresoras, planta telefónica, scanners y demás dispositivos que sean propiedad de la entidad.
Préstamo de equipos tecnológicos que estén a cargo del Grupo de Tecnologías de la Información.
Instalación de software.

• Periódicamente el Grupo de Tecnologías de la Información realizará una inspección aleatoria de los programas utilizados en cada una de las dependencias de la Unidad Administrativa Especial de Organizaciones Solidarias. La descarga, instalación y uso de programas informáticos NO autorizados será considerado una violación a la política de seguridad y privacidad de la

información.

- Estará bajo custodia del Grupo de Tecnologías de la información los medios magnéticos/electrónicos (CD´s u otros) que vengan originalmente con el software, así como sus respectivos manuales y licencias de uso. Las claves para descargar software del sitio web del fabricante y los passwords de administración de los equipos, también estarán bajo la custodia del Grupo de Tecnologías de la información de la Entidad.

- Los recursos informáticos de la Unidad Administrativa Especial de Organizaciones Solidarias no podrán ser utilizados sin previa autorización escrita, para guardar, divulgar contenido personal o comercial, programas con virus, o cualquier otro uso que no esté autorizado.

- Los funcionarios y contratistas de la Unidad Administrativa Especial de Organizaciones Solidarias deberán informar a su jefe inmediato sobre cualquier violación a la política de seguridad y privacidad de la información. Al presentarse dichas incidencias de seguridad y violación a la política de seguridad los funcionarios deberán repórtalo al Grupo de Tecnologías de la Información a través de la Mesa de Ayuda.

- Todo archivo o material descargado o recibido a través de medio magnético/electrónico, deberá ser revisado por el antivirus para detección de virus u otros programas maliciosos antes de ser instalados o usados en la infraestructura de TIC de la Unidad Administrativa Especial de Organizaciones Solidarias.

- La información producida por la Unidad Administrativa Especial de Organizaciones Solidarias debe ser respaldada de forma frecuente y segura, debe ser almacenada en lugares apropiados que garantice que la información este segura y podrá ser recuperada en caso de desastre, pérdida o incidente con los equipos.

- Los funcionarios y contratistas de la Unidad Administrativa Especial de Organizaciones Solidarias deberán realizar la entrega de los activos físicos/electrónicos asignados para el cumplimiento de sus funciones durante el proceso de desvinculación de la entidad, de igual manera deberán documentar y entregar los conocimientos importantes que poseen de la labor que ejecutan.

- Los usuarios que hagan uso de equipos institucionales en préstamo, NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso. El Grupo de Tecnologías de la Información no se hace responsable por la información guardada en este tipo de equipos.

- Los usuarios que soliciten el préstamo de equipos o elementos informáticos al Grupo de Tecnologías de la Información, deberán firmar el formato de "préstamo de equipos". Los usuarios deberán devolver los equipos o elementos informáticos en las condiciones en las que fueron prestados, de no ser así el usuario deberá responder por el equipo o elemento, según lo determine el Grupo de Tecnologías de la Información.

- En el Disco C:\ de las estaciones de los usuarios se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a estos archivos.

- Los equipos que ingresan temporalmente a la entidad que son de propiedad de terceros: deben ser registrados en la recepción para poder realizar su retiro; posteriormente la Unidad Administrativa Especial de Organizaciones Solidarias no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.

- El Grupo de Tecnologías de la Información no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la Unidad Administrativa Especial de Organizaciones Solidarias; exceptuando los equipos utilizados en la modalidad de Teletrabajo.

- Los documentos que se impriman en las impresoras de la Unidad Administrativa Especial de Organizaciones Solidarias deben ser de carácter institucional.

5.4. POLÍTICA DE USO DE CARPETAS COMPARTIDAS

- Para que los usuarios tengan acceso a la información ubicada en las carpetas compartidas, el jefe inmediato deberá solicitar mediante la Mesa de Ayuda el acceso y permisos, correspondientes al rol y funciones a desempeñar. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.

- La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

- Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en las carpetas compartidas.

- Es responsabilidad de los jefes de cada Grupo mantener depurada la información contenida en las carpetas compartidas de cada dependencia, con el fin de optimizar el uso de los recursos de almacenamiento de la entidad.

- La información que se almacene y comparta en herramientas institucionales como OneDrive y SharePoint debe estar alojada en el equipo de cómputo, cada equipo asignado a un funcionario contiene una partición de disco llamada (DATOS) en la cual se deberá guardar toda la información institucional generada.

5.5. POLÍTICA DE LAS OPERACIONES DE TICS

- El Grupo de Tecnologías de la Información debe realizar seguimiento a la infraestructura tecnológica para evaluar la capacidad de los recursos de red de los sistemas de información con el fin de asegurar la disponibilidad de los servicios tecnológicos con

el paso del tiempo.

- El Grupo de Tecnologías de la Información debe separar los ambientes de desarrollo de nuevos sistemas de información, en pruebas y producción en diferentes servidores y dominios.

- El Grupo de Tecnologías de la Información debe realizar un test de pruebas a los nuevos sistemas de información en ambiente de pruebas, para evaluar la funcionalidad previa a la puesta en producción de las aplicaciones.

- Todo software y hardware nuevo que se vaya a implementar en las instalaciones de la Unidad Administrativa Especial de Organizaciones Solidarias deberá ser gestionado por el Grupo de Tecnologías de la Información de la entidad.

- El grupo de Tecnologías de la Información deberá proponer e implementar técnicas de desarrollo de software seguro, estas deben incluir requerimientos de seguridad que les permitan a los desarrolladores aplicarlas de manera eficiente.

- El funcionario responsable de seguridad de la información deberá asegurarse de borrar el usuario de la base de datos del registro biométrico, una vez el funcionario o contratista finalice labores con la entidad. Esto con el fin de garantizar la seguridad en el acceso a las instalaciones de la entidad.

5.6. POLÍTICA DE SEGURIDAD DE EQUIPOS TECNOLÓGICOS

- El acceso a los servidores de la Unidad Administrativa Especial de Organizaciones Solidarias será permitido únicamente a los funcionarios del Grupo de Tecnologías de la Información.

- Es de carácter prohibido la instalación de software de acceso remoto en los servidores y equipos de la entidad; las instalaciones de estas aplicaciones serán consideradas una violación a la política de seguridad y privacidad de la información.

- Es prohibido el acceso a correos electrónicos, descargas de archivos de internet dentro de los servidores que alojan los sistemas de información de la Unidad Administrativa Especial de Organizaciones Solidarias.

- El acceso al Data Center será permitido únicamente por personal autorizado por la Coordinación del Grupo de Tecnologías de la Información.

- El acceso a la planta de sonido y video en el auditorio (equipos audiovisuales) de la Unidad Administrativa de la Unidad Especial de Organizaciones Solidarias será permitido únicamente por personal autorizado por la Coordinación del Grupo de Tecnologías de la Información.

- El Grupo de Tecnologías de la Información deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.

- El aseo al centro de datos estará a cargo del Grupo de Gestión Administrativa, este deberá efectuarse en presencia de un funcionario / contratista designado por el Grupo de Tecnologías de la Información. El personal de limpieza debe seguir las recomendaciones mínimas durante el proceso de limpieza.

5.7. POLÍTICA DE RESPALDO DE LA INFORMACIÓN

- El Grupo de Tecnologías de la Información es la dependencia responsable de realizar los Backups de la información contenida en las carpetas compartidas, servidores, aplicaciones, unidad (Datos). La información que no se encuentre almacenada en estos espacios el Grupo de TI no será responsable de la perdida.

- La información de cada sistema de información debe quedar respaldada sobre un medio de almacenamiento como disco duro, CD, DVD, Cinta, almacenamiento en la nube, etc.

- El administrador del sistema de respaldo de la información es el responsable de realizar periódicamente los Backups y de definir los requerimientos de seguridad de la información para hacerlos.

- Todas las copias de información deben ser almacenadas en un área adecuada y con control de acceso.

- Las copias de seguridad se realizan con el fin de restaurar los sistemas de información luego de la infección de un virus informático, defectos en las aplicaciones, materialización de amenazas, desastres, catástrofes y por requerimiento legal.

- Periódicamente el Grupo de Tecnologías de la Información verificará la correcta ejecución del procedimiento “Respaldo de información de equipos de cómputo y servidores”.

- Los medios que contengan información y vayan a ser eliminados, deben surtir un proceso de borrado seguro, para posteriormente eliminarlos de forma correcta.

- La pérdida de información que se considere esencial para la operación de la entidad será considerada una violación a la política de seguridad y privacidad de la información.

5.8. POLÍTICA DE USO DE CORREO ELECTRÓNICO

- Cualquier información o documentación relacionada con la Unidad Administrativa Especial de Organizaciones solidarias deberá ser enviada y recibida por medio del correo institucional y evitar el uso para estos fines de otros servicios de correo electrónico. En caso de una contingencia de correo se permitirá el uso de servidores de correo externos. El grupo de Tecnologías de la Información habilitará los permisos necesarios hasta que se restablezca el servicio normal de correos.

- El uso del correo electrónico institucional debe utilizarse exclusivamente para las tareas propias de la función desarrollada por la Unidad Administrativa Especial de Organizaciones Solidarias.

- Es prohibido el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

- El Grupo de Tecnologías de la Información desactivará las cuentas de correo electrónico una vez los funcionarios o contratistas se retiren de la Unidad Administrativa Especial de Organizaciones Solidarias.

- Es responsabilidad del Grupo de Tecnologías de la Información administrar los tipos de licencias del correo institucional y asignarlas a los funcionarios o contratistas según su necesidad y función.

- Cada líder de proceso deberá solicitar mediante la Mesa de Ayuda la creación de una cuenta de correo institucional, así mismo deberá solicitar la desactivación de la cuenta una vez el funcionario o contratista se desvincule de la entidad.

- Todo usuario que reciba mensajes de correo electrónico cuyo origen sea desconocido será responsable de las consecuencias que pueda ocasionar la descarga o ejecución de cualquier archivo adjunto. En estos casos los funcionarios deben reportar al Grupo de Tecnologías de la Información reenviando el correo a soportetics@orgsolidarias.gov.co.

5.9. POLÍTICA USO DE INTERNET / INTRANET

- El servicio de internet/intranet debe ser utilizado de forma razonable y con propósitos laborales. Se considera prohibido el ingreso a páginas web como YouTube, reproductores de música y el uso de redes sociales en la infraestructura de la entidad, salvo aquellos que en el cumplimiento de sus funciones requieran el uso de estas herramientas.

- La descarga de archivos de internet debe ser con fines laborales y de forma razonable para no afectar el servicio.

- El acceso a páginas está restringido por el firewall y antivirus de la entidad. El desbloqueo de páginas se hará mediante solicitud previa del funcionario o interesado y aprobación por parte del Director, Subdirector o Director Técnico.

- La Entidad contará con perfiles personalizados (de equipos de cómputo y acceso), de acuerdo con los niveles de autoridad jerárquicos y consagrados en el manual de Funciones Interno.

- En caso de contingencia, se privilegiará la continuidad del servicio de internet/intranet a las actividades de gestión Misional, Financiera y Jurídica.

- Los funcionarios, contratistas y terceros no deben acceder a redes inalámbricas públicas en las instalaciones, ya que atenta contra la seguridad y privacidad de la entidad.

5.10. POLÍTICA DE APLICACIONES

- La instalación de software debe estar justificada para fines laborales en cumplimiento de las funciones del cargo.

- Ante cualquier solicitud de instalación de software esta deberá solicitarse a través de la Mesa de Ayuda debidamente justificada.

- El software instalado en los equipos de propiedad de la Unidad Administrativa Especial de Organizaciones Solidarias debe contar con licencias actualizadas.

- El software libre no deberá poner en riesgo la integridad, disponibilidad o confidencialidad de la información, medios de procesamiento, almacenamiento o transmisión de información.

- Los funcionarios y contratistas de la Unidad Administrativa Especial de Organizaciones Solidarias no podrán realizar ninguna de las siguientes actividades sin previa autorización del Grupo de Tecnologías de la Información:

  Instalar software en los equipos de la Unidad Administrativa Especial de Organizaciones Solidarias.
  Alterar, cambiar, transformar o adaptar cualquier software de propiedad de la Unidad Administrativa Especial de Organizaciones Solidarias.
  Copiar o distribuir software de propiedad de la Unidad Administrativa Especial de Organizaciones Solidarias.

- Los usuarios serán responsables de todas las acciones realizadas con su “cuenta de usuario”.

5.11. POLÍTICA PARA EL USO DE MEDIOS MÓVILES O REMOVIBLES

- La información que se considere pública reservada y pública clasificada de la Unidad Administrativa Especial de Organizaciones Solidarias, no deberá ser almacenada en medios móviles o removibles personales.

- La información que se considere pública reservada y pública clasificada de la Unidad Administrativa Especial de Organizaciones Solidarias, no deberá ser almacenada en repositorios o archivos públicos de internet personales, tales como: Dropbox, SkyDrive, Box, Google Drive, etc.

- Las memorias flash (USB, SD, Memory Stick, Micro SD, etc.) se deberán emplear sólo para la transferencia de datos y no como dispositivos de almacenamiento. La información transferida deberá ser eliminada.

- No se dejarán conectados los dispositivos USB en los equipos si no están en uso.

- Los Discos externos deberán tener acceso controlado de la información tanto en recepción como en las instalaciones de la

Unidad Administrativa Especial de Organizaciones Solidarias, la cual estará a cargo de los coordinadores de grupo.

- En el caso de medios de almacenamiento ópticos (DVD, CD, Minidisc, Blue-ray, etc.),deberá asegurarse su protección contra factores ambientales que generen deterioro como humedad, acceso no autorizado; contar con identificación apropiada y al término de su uso, la eliminación adecuada.

- Los dispositivos móviles (teléfonos, Smartphone, tabletas entre otros), son una herramienta de trabajo que se debe utilizar únicamente para facilitar las comunicaciones entre los funcionarios de la entidad.

5.12. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

- Los funcionarios y contratistas de la Unidad Administrativa Especial de Organizaciones Solidarias deben conservar el escritorio del equipo libre de información o accesos directos a información que pueda ser alcanzada, copiada por personal no autorizado.

- El personal de la Unidad Administrativa Especial de Organizaciones Solidarias debe bloquear la pantalla de su equipo en los momentos en los que no esté utilizando el equipo o por cualquier motivo que deje su puesto de trabajo.

5.13. POLÍTICA DE TELETRABAJO

- Los funcionarios de la Unidad Administrativa Especial de Organizaciones Solidarias que adopten la modalidad de teletrabajo realizarán sus funciones en equipos o dispositivos de su propiedad, dado que la entidad no cuenta con recursos suficientes para suministrar los equipos a todos los teletrabajadores.

- El Grupo de Tecnologías de la Información deberá garantizar que el antivirus instalado en el equipo del teletrabajador cumpla con características como detención de virus, eliminación de infecciones, capacidad de detención de malware, spyware, pishing entre otros peligros.

- El teletrabajador será responsable de garantizar la protección de la información institucional que maneje en el lugar de trabajo del cual disponga para la realización de sus funciones.

- El Grupo de Tecnologías de la Información realizará una visita técnica al teletrabajador para revisar aspectos como conexiones de red, cableado eléctrico, configuración y estado del equipo, y verificar las condiciones en las que se desarrolla la modalidad de teletrabajo.

6. RESPONSABLE DE IMPLEMENTACIÓN

La Responsabilidad de la aplicación e implementación de la presente política está dada por la Alta Dirección, en cabeza de la Dirección Nacional, la Dirección de Planeación e Investigación y el Grupo de Tecnologías de la Información en función del cumplimiento de las normativas relacionadas con Seguridad y Privacidad de la Información.

7. PROCESOS INVOLUCRADOS EN LA IMPLEMENTACIÓN

La presente política será aplicable a todos los procesos que se desarrollen al interior de la Unidad Administrativa Especial de Organizaciones Solidarias.

8. INDICADORES

Objetivo: Reflejar la gestión y evolución de la aplicación de la política de seguridad de la información en la entidad.

Indicador: (Número total de anomalías cerradas / Número de anomalías encontradas)*100

Metas: MÍNIMA: 75 – 80% SATISFACTORIA: 81 - 90% SOBRESALIENTE: 100%

9. CRONOGRAMA GENERAL DE IMPLEMENTACIÓN

El presente documento de política de seguridad y privacidad de la información entrará en vigencia desde la expedición del acto administrativo que así lo disponga.

10. ANEXOS

Manual de Políticas de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial de Organizaciones Solidarias

CONPES 3854 de 2016

CONPES 3701 de 2011

MODELO DE SEGURIDAD DE TI del Ministerio de Tecnologías de la Información.

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN

ELABORÓ	REVISÓ	APROBÓ

Nombre: Juan David Diaz Salgado **Cargo:** Coordinador grupo de Tecnologías de la Información **Fecha:** 08/Feb/2019	**Nombre:** Revisión Calidad Jorge Muñoz **Cargo:** Profesional Especializado Grupo Planeación y Estadística **Fecha:** 12/Feb/2019	**Nombre:** Martha Cecilia Daza Rivera **Cargo:** Coordinador Grupo Planeación y Estadística **Fecha:** 12/Feb/2019