I. 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.

II. PROPÓSITO

La Unidad Administrativa Especial de Organizaciones Solidarias (UAEOS) 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.

III. 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.

IV. DEFINICIONES

- **Acción correctiva**: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.
- **Acción preventiva:** Es una medida de tipo pro-activo orientada a prevenir potenciales no conformidades.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Características de la información:** Las principales características desde el enfoque de seguridad y privacidad de la información son: Confidencialidad, Integridad y Disponibilidad.
- **Confidencialidad**: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Custodio 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 legitimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.
- **ISO/ICE 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.

V. DECLARACION

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 Gestión de Activos de Información
- Política de Uso de Carpetas Compartidas
- Política de Control de Acceso a la plataforma tecnológica
- Política de Operaciones de TICS
- Política de Protección contra Malware
- Política de Respaldo de la Información
- Política de Control de Acceso a usuarios

- Política de Gestión de Contraseñas
- Política de Seguridad de equipos tecnológicos
- Política de Uso de correo electrónico
- Política de Uso de Internet/Intranet
- Política de Aplicaciones
- Política de Seguridad del Sistema de Videovigilancia (Sv)
- Política de Uso de medios removibles
- Política de Seguridad del Archivo de Gestión Documental
- Política de Escritorio y pantalla limpia
- Política de Teletrabajo – Trabajo en casa
- Política de Seguridad Digital
- Política de Seguridad para el Desarrollo de Software

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 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 publicas 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 publica 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.

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.

POLÍTICA DE USO DE LOS ACTIVOS DE INFORMACIÓN

- Los funcionarios, contratistas y terceros que tengan acceso a las instalaciones de la UAEOS deberán utilizar únicamente los programas autorizados por el Grupo de Tecnologías de la Información.
- Los funcionarios y contratistas de la UAEOS 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 UAEOS. 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 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 password 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 UAEOS 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 UAEOS 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 UAEOS.

- La información producida por la UAEOS debe ser respaldada de forma frecuente y segura, debe ser almacenada en lugares apropiados que garantice que la información este resguardada y pueda ser recuperada en caso de desastre, pérdida o incidente con los equipos.

- Los funcionarios y contratistas de la UAEOS 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 UAEOS 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 UAEOS; exceptuando los equipos utilizados en la modalidad de Teletrabajo.

- Los documentos que se impriman en las impresoras de la UAEOS deben ser de carácter institucional.

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.

POLÍTICA DE CONTROL DE ACCESO A LA PLATAFORMA TECNOLÓGICA

- El grupo de TIC restringe el acceso a los servicios de red y sistemas de información mediante el uso de usuarios y contraseñas. Para el acceso a los servicios de red, la restricción se implementa mediante la configuración de seguridad del directorio activo. En lo posible los sistemas de información están integrados con el directorio activo para unificar los criterios de seguridad; de no ser posible, cada sistema de información debe contar con un módulo de seguridad que permita la implementación de perfiles, usuarios y contraseñas.

- La conexión remota a la red de área local de la UAEOS debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por el Grupo de Tecnologías de la Información.

- El grupo de Gestión Administrativa asigna los puestos de trabajo y el grupo TIC instala y configura a los funcionarios y contratistas los equipos, accesos y recursos tecnológicos necesarios para que puedan desempeñar las funciones u obligaciones para las cuales fueron vinculados o contratados.

- Por defecto los usuarios creados no tienen permisos de administrador. En caso de requerirlo deben realizar la solicitud a la mesa de ayuda. Sólo se otorgan los privilegios

para la administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que cumplan dichas actividades.

- La infraestructura tecnológica de la UAEOS que soporta aplicaciones está separada en segmentos de red físicos, lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La separación de estos segmentos está implementada por medio del dispositivo de seguridad perimetral y los switches y enrutadores.

- El acceso a los servidores de la UAEOS será permitido únicamente a los funcionarios del Grupo de Tecnologías de la Información.

- 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 UAEOS será permitido únicamente por personal autorizado por la Coordinación del Grupo de Tecnologías de la Información.

POLÍTICA DE CONTROL DE ACCESO A USUARIOS

- Se prohíbe entrar a las instalaciones en horario nocturno, días feriados y fines de semanas, sin la previa autorización del coordinador (a) del área involucrada, Director Técnico y el Director General.

- Cuando las personas requieran ingresar a las instalaciones con algún tipo de equipos electrónicos como computadores portátiles, cámaras fotográficas o de video, deben realizar su registro en la portería principal, con la previa autorización del coordinador del área.

- Los elementos tecnológicos de la entidad están bajo la responsabilidad y cuidado del funcionario asignado. Igualmente, la entidad no es responsable de los dispositivos de tecnología u otros de propiedad personal que se extravíen dentro de las Instalaciones de la Entidad

- La salida de bienes de propiedad de la entidad para trámite de mantenimiento, reparación y/o garantía debe ser previamente autorizada por el Coordinador del Grupo de Tecnologías y el grupo de Gestión Administrativa

- Todos los funcionarios deben garantizar que ninguna persona ajena a la entidad se quede en las instalaciones sin acompañamiento o supervisión.

- Todo ingreso de funcionarios y personal externo en horario no hábil deberá ser autorizada previamente por el Coordinador del área, coordinador de Gestión Administrativa o el Director General cuando corresponda, para lo cual, debe remitirse un correo electrónico por el funcionario o por el coordinador del área quien deberá ser informado al respecto.

- Las puertas de acceso a la entidad deberán permanecer cerradas durante la jornada laboral y debidamente aseguradas en horario no laboral.

POLÍTICA DE 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 UAEOS deberá ser gestionado por el Grupo de Tecnologías de la Información de la entidad.

- El Grupo de Tecnologías de la Información debe 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.

- El Grupo de Tecnologías de la Información con ayuda del Grupo de Planeación y estadística deberá registrar ante el sistema de información llamado Registro Nacional de Base de Datos (RNBD) las bases de datos identificadas que contengan información personal en el sistema de la Superintendencia de Industria y Comercio.

POLÍTICA DE PROTECCIÓN CONTRA MALWARE

- Todos los equipos de cómputo, servidores y portátiles de la UAEOS están protegidos con un software de antivirus.

- Los programas de antivirus son instalados por el Grupo TIC en los servidores y en las estaciones de trabajo de modo residente para que estén activados durante su uso.

- Los servicios de información y tecnología que se emplean para servir a una finalidad operativa y administrativa en relación con la entidad y que intercambien información o los sistemas que la procesan, redes y demás infraestructura de la UAEOS se consideran bajo el control de la entidad y están bajo la supervisión del Grupo TIC para verificar la existencia de programas de protección contra código malicioso.

- El usuario puede ejecutar la verificación de existencia de virus o código malicioso con las herramientas antivirus provistos cada vez que detecte que algún equipo o dispositivo informático está funcionando de manera irregular o se sospeche de la presencia de virus en equipos, dispositivos, archivos o correos electrónicos.

- Todo usuario es responsable de reportar toda información cuyo origen le sea desconocido y asume la responsabilidad de las consecuencias que puede ocasionar la apertura o ejecución de cualquier archivo de origen desconocido.

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 TIC no será responsable de la pérdida.

- 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.

- Para los funcionarios que adopten la modalidad de trabajo en casa deberán respaldar la información a través del uso de la licencia de office 365 usando OneDrive institucional,

para aquellos que tienen asignada este tipo de licencia, y para los funcionarios que no deberán respaldar la información en medios USB o Discos Externos y asegurarla en las carpetas compartidas de la entidad.

POLÍTICA DE GESTIÓN DE CONTRASEÑAS

- El Grupo TIC, suministrará a los usuarios las contraseñas respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados.

- Las credenciales de acceso a los servicios de red y sistemas de información son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las contraseñas asignadas. Ningún usuario deberá acceder a la red o a los servicios TIC de la entidad, utilizando una cuenta de usuario o clave de otro usuario.

- El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato.

- Cada vez que se cambien estas deben ser distintas a las anteriores.

- Las contraseñas serán renovadas cada 6 meses por política en el directorio activo, y de acuerdo a solicitud de los usuarios.
- La contraseña debe cumplir con los siguientes requisitos:

  - Tener mínimo ocho (8) caracteres alfanuméricos
  - Caracteres en mayúsculas
  - Caracteres en minúsculas
  - Base de 10 dígitos (0 a 9)
  - Caracteres no alfabéticos (Ejemplo: ¡,$, %, &)

- Las cuentas de los usuarios que hagan más de 6 intentos fallidos de acceso quedarán deshabilitadas y los usuarios deberán solicitar su desbloqueo.

- El Grupo de Tecnologías de la información, es la encargada de realizar la asignación, modificación e inactivación de usuarios en el dominio y en todas las aplicaciones que maneje la entidad.

POLÍTICA DE SEGURIDAD DE EQUIPOS TECNOLÓGICOS

- El acceso a los servidores de la UAEOS 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 UAEOS.
- 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 UAEOS 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.

POLÍTICA DE USO DE CORREO ELECTRÓNICO

- Cualquier información o documentación relacionada con la UAEOS 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 UAEOS.

- Los usuarios son responsables de todas las actividades que se realicen desde su cuenta de correo institucional.

- 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 es el encargado de gestionar internamente la distribución y asignación de licencias de office 365 según necesidad y requerimientos que manejen los funcionarios.

- 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 funcionario 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 seguridaddigital@uaeos.gov.co.

- Los remitentes de correos electrónicos maliciosos o sospechosos de virus serán bloqueados desde la administración de la consola de Office 365 la cual es administrada por el Grupo de Tecnologías de la Información.

- La consola de Office 365 solicitará a los funcionarios el cambio de contraseña cada 121 días, el cambio de contraseña es obligatorio.

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.

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 UAEOS 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 UAEOS 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 UAEOS
  - Alterar, cambiar, transformar o adaptar cualquier software de propiedad de la UAEOS.
  - Copiar o distribuir software de propiedad de la UAEOS.
- Los usuarios serán responsables de todas las acciones realizadas con su “cuenta de usuario”.

POLÍTICA DE SEGURIDAD EN EL SISTEMA DE VIDEOVIGILANCIA (SV)

- El sistema de video vigilancia de la UAEOS, es el conjunto de herramientas tecnológicas y operadores que permiten llevar a cabo la función de captar imágenes de video, con el

fin de garantizar la seguridad de los datos personales, evitar la adulteración, pérdida, deterioro, consulta, uso o acceso no autorizado o fraudulento.

- El Grupo de Tecnologías de la información debe mantener la integridad de la información obtenida del sistema de video vigilancia y garantizar los derechos de los titulares de los datos personales.

- El Grupo de Tecnologías de la información deberá informar a los titulares acerca de la recolección y demás formas de tratamiento de las imágenes, así como la finalidad del mismo.

- El Grupo de Tecnologías de la información no instalará cámaras de vigilancia en lugares donde la recolección de imágenes y en general el tratamiento de estos datos pueda afectar la imagen o la vida privada de las personas.

- La instalación de las cámaras de video se realizará en las áreas comunes tales como: pasillos internos, entradas y salidas de los pisos de la entidad.

- El Grupo de Tecnologías de la información garantizará que las imágenes grabadas se reproducirán en un área de acceso restringido que garantice la seguridad de las mismas.

- La divulgación de las imágenes grabadas del sistema de video vigilancia (SV) es de carácter restringido.

- El sistema y los equipos de videocámaras deberán mantenerse en operación según la configuración por el Grupo de Tecnologías y aprobada por el Director General.

- Las grabaciones de las cámaras se almacenarán en el NVR por un tiempo de 30 días, solo podrán ser respaldadas en caso que se requiera la revisión en una situación indicada por la mesa de ayuda y aprobado por el coordinador del Grupo TIC.

- Se considera situaciones que ameriten la revisión de videos las siguientes:
  - Conductas que puedan ser constituidas como delitos.
  - Eventos o incidentes naturales o provocados por el hombre, que pongan en riesgo la seguridad de los funcionarios de la entidad.

- La información contenida en el sistema de video vigilancia, solo podrá ser realizada o consultada por los funcionarios del Grupo TIC y por la Dirección Nacional.

- El sistema y equipos deberá manejarse en forma adecuada y responsable, debiendo proteger y respetar en todo momento los derechos humanos y a la privacidad, el honor, la imagen o cualquier otro derecho fundamental.

- Sera atribuciones del responsable del sistema:

  - Resguardar las contraseñas del administrador de los NVR instalados en la entidad.
  - Asignar el administrador y usuarios de consulta
  - Cambiar por lo menos cada tres meses su contraseña de acceso.

- Está prohibido:

  - La adición de dispositivos para la grabación de audio
  - Alterar o manipular de manera total o parcial las imágenes obtenidas.
  - Permitir el acceso al sistema a persona no autorizadas
  - Colocar cámaras del sistema en ligares como baños, vestidores, oficinas en otros espacios donde exista la necesidad de privacidad de los funcionarios de la entidad
  - Utilizar las imágenes o video para fines distintos las los de la política.

POLÍTICA PARA EL USO DE MEDIOS REMOVIBLES

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

- La información que se considere pública reservada y pública clasificada de la UAEOS 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 UAEOS, 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 (Smartphone, tabletas entre otros), son una herramienta de trabajo que se debe utilizar únicamente para facilitar las comunicaciones entre los funcionarios de la entidad.

POLÍTICA DE SEGURIDAD DEL ARCHIVO DE GESTIÓN DOCUMENTAL

- Se contará con video vigilancia las 24 horas en el archivo de gestión de la UAEOS.

- Se permitirá el acceso al archivo de gestión de la entidad solo a personal autorizado y designado por la Coordinación de Gestión Administrativa obedeciendo a la seguridad y protección de datos personales y conservación de archivos.

POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

- Los funcionarios y contratistas de la UAEOS 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 UAEOS 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.

- Las sesiones de usuario se deben cerrar y proteger con contraseña cuando el usuario se ausente en forma temporal o por largos períodos de tiempo.

- Al finalizar sus actividades los usuarios deben verificar que en sus puestos de trabajo no quede expuesta información crítica o sensible para la entidad.

- Los usuarios deben concientizarse de ahorro del consumo de energía y uso racional, apagando el computador y dispositivos electrónicos a su cargo una vez termine la jornada de trabajo.

POLÍTICA DE TELETRABAJO – TRABAJO EN CASA

- 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.

- Los funcionarios de la UAEOS que adopten la modalidad de teletrabajo realizarán sus funciones en equipos o dispositivos suministrados por la entidad o de su propiedad, de acuerdo a las indicaciones del Director General.

- El grupo de Tecnologías de la Información debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos, contratistas de la UAEOS garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

- Toda la información gestionada por la UAEOS, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.

- 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.

POLÍTICA DE SEGURIDAD DIGITAL

- El Grupo de Tecnologías de la Información deberá implementar medidas para garantizar la seguridad digital y mitigar los riesgos e incidentes cibernéticos que afecten la filtración de datos personales o sensibles.

- Es deber del Grupo de Tecnologías de la Información adoptar buenas prácticas en materia de seguridad digital que ayuden a fortalecer el modelo de seguridad y privacidad de la información de la entidad.

- En caso de presentarse un incidente cibernético grave o muy grave este deberá reportarse dentro de las 24 horas siguientes al CSIRT-Gobierno.

- El Grupo de Tecnologías de la Información debe exigir al proveedor del hosting políticas de seguridad más robustas y un nivel de madurez de seguridad optimizado.

- El Grupo de Tecnologías de la Información deberá aplicar mecanismos de *hardening* para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace entre otros.

- El Grupo de Tecnologías de la Información debe ejecutar monitoreos de seguridad sobre los sitios web que considere, considerando las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios.

- El Grupo de Tecnologías de la Información debe exigir mecanismos de autenticación dentro de los sitios web a través de la creación de contraseñas fuertes y solicitar renovaciones periódicas de las mismas.

- Es obligación del Grupo de Tecnologías de la información mantener actualizado el software, frameworks y plugins de los sitios web.

- Se debe ocultar o restringir páginas de acceso administrativo.

- Se debe restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.

- El Grupo de Tecnologías de la Información debe garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de los usuarios).

- El Grupo de Tecnologías de la Información debe habilitar cabeceras de seguridad tales como: Content-Security-Policy (CSP), X-Content-Type- Options, X-Frame-Options, X-XSS-Protection, Strict-Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature-Policy.

- El Grupo de Tecnologías de la Información debe implementar mensajes genéricos de error, que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico, los cuales deberán ser comprensibles por parte de las personas.

- Es obligación del Grupo de Tecnologías de la Información proteger los archivos del aplicativo por medio de los métodos de ofuscación que consiste en alterar la estructura de los mismos de tal forma que estando en producción el software, la lectura de los archivos para personas externas sea incomprensible y así evitar modificaciones no deseadas.

- Es responsabilidad del Grupo de Tecnologías de la Información implementar en los servidores los controles necesarios (hardware, software) de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.

POLÍTICA DE SEGURIDAD PARA EL DESARROLLO DE SOFTWARE

- Se debe proteger la integridad de los códigos fuente mediante los siguientes aspectos:

    - Validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y cabeceras HTTP.
    - La sanitización de los parámetros de entrada: es decir que cuando se reciba la información de dichas variables se eliminen etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente forman un script, además de la restricción de formatos y tamaños de subidas de archivos.
    - La sanitización y escape de variables en el código.
    - Revisión y verificación de las políticas de origen de las cabeceras.

- Los desarrolladores del Grupo de Tecnologías de la Información deben revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y servicios Web seguros de la Open Web Application Security Project (OWASP).

- Los desarrolladores deben realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentran en la programación de las aplicaciones.

- Cumplir con la estandarización del código fuente para portales web, siguiendo las buenas prácticas del W3C (World Web Wide Consortium) de forma que permita la correcta visualización de la información a los usuarios.

- Implementar un sistema de control de versiones (Git), que permitan planear y controlar la vida de la aplicación.

VI. RESPONSABLE DE IMPLEMENTACION

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.

VII. 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.

VIII. 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%

IX. 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, o desde que esta sea aprobado en el comité administrativo.

X. ANEXOS

CONPES 3854 de 2016
CONPES 3701 de 2011
MODELO DE SEGURIDAD DE TI del Ministerio de Tecnologías de la Información.

XI . HISTORIAL DE CAMBIOS

Control	Responsable
Elaboró	Carlos Julio Vargas Gomez - Contratista Grupo de Planeación y Estadística
Revisó	Edna Lizeth Villarreal Duarte - Profesional Grupo Tecnologías de la Información
Aprobó	Laura Lizeth Malaver Botia - Profesional Grupo Tecnologías de la Información
Validó	Marisol Viveros Zambrano - Coordinadora de Planeación y Estadística

XII, CONTROL DE ACTUALIZACIÓN Y MEJORAS

Fecha de Actualización	Descripción del Cambio Realizado	Nombre y Cargo del responsable del Último Cambio	Versión
26/11/2020	Se crea Política en cumplimiento Seguridad de la Información y el marco normativo vigente.	Juan David Diaz Profesional Grupo Tecnologías de la Información	**1**
28/10/2021	Se incluye política de seguridad para el desarrollo de software, política de seguridad digital, política de seguridad en el sistema de videovigilancia (sv) en cumplimiento Seguridad de la Información y el marco normativo vigente.	Laura Lizeth Malaver Botia Profesional Grupo Tecnologías de la Información	**2**