U.A.E. CUERPO OFICIAL
BOMBEROS
BOGOTÁ D.C.

(Honor, Valor, Disciplina)

# MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TIC-MN01

## TABLA DE CONTENIDO

## 1. INTRODUCCIÓN

La posibilidad de interconectarse a través de redes, la utilización de aplicaciones, y el manejo de la información por parte de los funcionarios, contratistas, proveedores, terceros, ha abierto nuevos horizontes a las instituciones para mejorar su productividad y ofrecer sus servicios más allá de las fronteras institucionales e, incluso, nacionales, lo cual, lógicamente ha traído la aparición de nuevas amenazas para los sistemas de información, como son:

- Ataques cibernéticos internos y externos.
- Pérdida de información ante la migración de datos.
- Navegación imprudente por parte de los funcionarios y contratistas.
- Correos electrónicos maliciosos.
- Explotación automática de vulnerabilidades conocidas.
- Manipulación inadecuada de la información por parte de funcionarios y contratistas.
- Fuga de información por parte de funcionarios y contratistas.

Es así que estas políticas están orientadas a preservar la confidencialidad, integridad y disponibilidad de la información, a través de los lineamientos y controles que se adoptan en cumplimiento a los requisitos exigidos por la norma técnica Internacional ISO/IEC 27001:2013,para la seguridad y privacidad de sus activos de información, con el propósito de minimizar posibles impactos no deseados que puedan comprometer los principios esenciales del Sistema de Gestión de Seguridad de la Información.

La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), es prioridad para la UAECOB, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas y pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital.

El Modelo de Seguridad y Privacidad debe estar acorde con las buenas prácticas de seguridad y debe ser actualizado periódicamente, reuniendo los cambios técnicos de la norma ISO 27001 del 2013, la legislación de la Ley de Protección de Datos Personales (Ley 1581 de 2012), Transparencia y Acceso a la Información Pública (Ley 1712 de 2014), entre otras, las cuales se deben tener en cuenta para la gestión de la información.

La implementación del MSPI de la Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá (UAECOB) determinada por las necesidades de privacidad de los datos personales

de los ciudadanos, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos personales.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de la Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá se busca contribuir al incremento de la transparencia en la gestión pública, promoviendo el uso de las mejores prácticas de seguridad de la Información como base de la aplicación del concepto de Seguridad Digital aumentando la confianza en la ciudadanía.

## 2. MARCO LEGAL

| Marco Normativo | Descripción |
|---|---|
| **Ley 322 de 1996.** | Por la cual se crea el Sistema Nacional de Bomberos de Colombia y se dictan otras disposiciones |
| **Ley 962 de 2005** | El artículo 14 modificó el artículo 16 del Decreto-ley 2150 de 1995, que establece lo siguiente: "Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá al usuario.<br>Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. El envío de la información por fax o por cualquier otro medio de transmisión electrónica, proveniente de una entidad pública, prestará mérito suficiente y servirá de prueba en la actuación de que se trate, siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite.<br>Cuando una entidad pública requiera información de otra entidad de la Administración Pública, esta dará prioridad a la atención de dichas peticiones, debiendo resolverlas en un término no mayor de diez (10) días, para lo cual deben proceder a establecer sistemas telemáticos compatibles que permitan |

| | |
|---|---|
| | integrar y compartir información de uso frecuente por otras autoridades.” |
| **Ley 1273 de 2009** | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones |
| **Ley 1341 de 2009** | Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. |
| **Ley 1978 de 2019** | Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones. |
| **Ley 1581 de 2012** | Por la cual se dictan disposiciones generales para la protección de datos personales. |
| **Ley 1712 de 2014** | Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. |
| **Ley 1753 de 2015** | Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. |
| **Ley 1955 del 2019** | Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) |
| **Decreto 2150 de 1995** | Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública |
| **Decreto 680 de 2001** alcalde Mayor de Bogotá. | Por el cual se modifica la Comisión Distrital de Sistemas. |
| **Decreto 397 de 2002** | Delegar en el secretario general de la Alcaldía Mayor de Bogotá las atribuciones conferidas al Alcalde Mayor en el Acuerdo 57 |

| | |
|---|---|
| | de 2002 como presidente de la Comisión Distrital de Sistemas, y las demás funciones que se requieran en el ejercicio de esta atribución. |
| **Decreto 541 de 2006** | Por el cual se determina el objeto, la estructura organizacional y las funciones de la Unidad administrativa Especial Cuerpo Oficial de Bomberos |
| **Decreto 542 de 2006** | Por el cual se establece la Planta de cargos de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos |
| **Decreto 221 de 2007** | Por el cual se modifica la Estructura Organizacional y algunas funciones de las dependencias de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos |
| **Decreto 514 de 2007** | Por el cual se establece que toda entidad pública a nivel Distrital debe tener un Subsistema Interno de Gestión Documental y Archivos (SIGA) como parte del Sistema de Información Administrativa del Sector Público |
| **Decreto 619 de 2007.** | Se establece la Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital y se dictan otras disposiciones. |
| **Decreto 185 de 2008** | Por el cual se prorroga el plazo para formular la Estrategia Distrital de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital. |
| **Decreto 296 de 2008** | Por el cual se le asignan las funciones relacionadas con el Comité de Gobierno en Línea a la Comisión Distrital de Sistemas y se dictan otras disposiciones en la materia |
| **Decreto 316 de 2008** | Por medio del cual se modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico. |
| **Decreto 1151 de 2008** | Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones |
| **Decreto 4485 de 2009** | Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública. |
| **Decreto 235 de 2010** | Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas. |
| **Decreto 2364 de 2012** | Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. |

| | |
|---|---|
| **Decreto 2693 de 2012** | Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones. |
| **Decreto 1377 de 2013** | Por el cual se reglamenta parcialmente la Ley 1581 de 2012 o Ley de Datos Personales. |
| **Decreto 2573 de 2014** | Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones |
| **Decreto 2433 de 2015** | Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. |
| **Decreto 103 de 2015** | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones |
| **Decreto 1078 de 2015** | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones |
| **Decreto 415 de 2016** | Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones. |
| **Decreto 728 2016** | Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico |
| **Decreto 728 de 2017** | Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico. |
| **Decreto 1413 de 2017** | En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales |

| | |
|---|---|
| **Decreto 1499 de 2017** | Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. |
| **Decreto 612 de 2018** | Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. |
| **Decreto 1008 de 2018** | Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. |
| **Decreto 2106 del 2019** | Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública |
| | Cap. II Transformación Digital para una Gestión Publica Efectiva |
| **Decreto 620 de 2020** | Que conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones. |
| **Resolución 001 de 2003, de la secretaria general Alcaldía Mayor de Bogotá.** | Por la cual se establece el reglamento interno de la Comisión Distrital de Sistemas. |
| **Resolución 185 de 2007, de la secretaria general Alcaldía Mayor de Bogotá.** | Políticas de Conectividad para las Entidades del Distrito Capital. |
| **Resolución 355 de 2007, de la secretaria general Alcaldía Mayor de Bogotá.** | Política específica de la Infraestructura de Datos Espaciales IDEC@. |

| | |
|---|---|
| **Resolución 256 de 2008, de la secretaria general Alcaldía Mayor de Bogotá.** | Por la cual se establece el reglamento interno de la Comisión Distrital de Sistemas – C.D.S. deroga la resolución 001 de 2003 |
| **Resolución 305 de 2008, de la secretaria general Alcaldía Mayor de Bogotá.** | Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre |
| **Resolución 378 de 2008, de la secretaria general Alcaldía Mayor de Bogotá.** | Por la cual se adopta la Guía para el diseño y desarrollo de sitios Web de las entidades y organismos del Distrito Capital |
| **Resolución 383 del 2011 de la UAECOB** | Por la cual se adoptan las políticas de seguridad para el manejo de la información y la Administración y uso de los recursos tecnológicos de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos y se deroga la Resolución 345 de 2008. |
| **Resolución 473 de 2011 de la UAECOB** | Por la cual se reestructura el Sistema y el comité del sistema Integrado de Gestión de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos |
| **Resolución 580 de 2012 de la UAECOB** | Por la cual se crea el Comité de Tecnología de la Información y Comunicaciones de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá. |
| **Resolución 366 del 2014** | Por la cual se adoptan las políticas de seguridad para el manejo de la información y la Administración y uso de los recursos tecnológicos de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos y se deroga la Resolución 366 de 2014. |
| **Resolución 3564 2015; ministerio de tecnologías de la información y las comunicaciones.** | Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados) |
| **Resolución 2710 de 2017; ministerio de tecnologías de la información y las comunicaciones.** | Por la cual se establecen los lineamientos para la adopción del protocolo IPv6. |

| | |
|---|---|
| **Norma Técnica Colombiana NTC 5854 de 2012** | El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA. |
| **Norma Técnica ISO/IEC 27001-2013** | Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) |
| **CONPES 3292 de 2004** | Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos. |
| **CONPES 3854 Política Nacional de Seguridad Digital de Colombia, de 11 de abril de 2016** | El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo |
| **CONPES 3920 de Big Data, de 17 de abril de 2018** | La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales. |

| | |
|---|---|
| **CONPES 3975 de 2019** | Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema. |
| **Circular 02 de 2019** | Se establecerá El Portal Único del Estado Colombiano con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad. |
| **Directiva Distrital 002 de 2002** | Reglamenta la formulación de proyectos informáticos y de comunicaciones. El Alcalde Mayor asignó a la Comisión Distrital de Sistemas la función de evaluar la viabilidad técnica y la pertinencia de la ejecución de los proyectos informáticos y de comunicaciones de impacto interinstitucional o de costo igual o mayor a 500 SMLV, previa a la inscripción de los mismos ante el Departamento Administrativo de Planeación Distrital. |
| **Directiva Distrital 005 de 2005** | Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital. |
| **Directiva Distrital 02 2019** | Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones |
| **Acuerdo 057 de 2002.** Alta Consejería Distrital TIC | Por el cual se dictan disposiciones generales para la implementación del sistema Distrital de Información -SDI-, se organiza la Comisión Distrital de Sistemas, y se dictan otras disposiciones. |
| **Acuerdo 130 de 2004.** Alta Consejería Distrital TIC | Por medio del cual se establece la infraestructura integrada de datos espaciales para el Distrito Capital y se dictan otras disposiciones. |
| **Acuerdo 279 de 2007.** Alta Consejería Distrital TIC | Dicta los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital. |
| **Acuerdo 409 de 2009.** Alta Consejería Distrital TIC | Por el cual se modifica la integración de la Comisión Distrital de Sistemas |
| **Resolución 500 de 2021**. Del Ministerio | Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de |

| | |
|---|---|
| de Tecnologías de la Información y las Comunicaciones (MinTIC) | seguridad y privacidad como habilitador de la Política de Gobierno Digital |
| **Resolución 386 de 2021.** De la UAECOB | Por la cual se adoptan los instrumentos de Gestión de la Información de la Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá |
| **Resolución 306 de 2019.** De la UAECOB | «Para la cual se crea el Comité Institucional de Gestión y Desempeño de la Unidad Administrativa Especial Cuerpo Oficial Bombero de Bogotá» |
| **Resolución 1519 de 2020.** Del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) | «Tiene por objeto expedir los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 del 2014, estableciendo los criterios para la estandarización de contenidos e información, accesibilidad web, seguridad digital, datos abiertos y formulario electrónico para Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD). |
| Demás normas y/o jurisprudencia que complementen, modifiquen, deroguen o sustituyan las anteriores. | |

## 3. OBJETIVO DEL MANUAL Y POLÍTICA GENERAL

### 3.1. OBJETIVO DEL MANUAL

Establecer las políticas específicas de seguridad y privacidad de la información que permitan reducir amenazas y vulnerabilidades de los activos de información de la **Unidad Administrativa Especial Cuerpo Oficial Bomberos de Bogotá (UAECOB)**, enfocadas en afianzar los principios de confidencialidad, disponibilidad e integridad de la información, con el fin de asegurar la continuidad del negocio y gestionar los riesgos asociados interpretado conforme los términos de la norma ISO 22301 sobre las buenas prácticas.

Para asegurar la implementación de la política de seguridad y privacidad de la información, la UAECOB establece los siguientes objetivos:

1. Establecer los lineamientos, e instructivos en materia de seguridad y privacidad de la información.
2. Implementar y mejorar continuamente el Sistema de Gestión de Seguridad de la información (SGSI) de la entidad.

3. Cumplir con la normatividad relacionada con la protección de datos personales, adoptando las medidas de control y de seguridad de la información que minimicen el riesgo de exposición, difusión, adulteración o perdida de esta.
4. Proteger sus activos de información, preservando su integridad, confidencialidad y disponibilidad.
5. Gestionar los riesgos de seguridad digital y de privacidad de la información mediante la aplicación de estrategias de control efectivos.
6. Fortalecer la cultura de seguridad y privacidad de la información en los servidores, contratistas y terceros.
7. Apoyar la innovación tecnológica, el uso y aprovechamiento de las tecnologías de la información a través de servicios seguros, con calidad y transparencia.
8. Establecer los mecanismos de monitoreo de la seguridad sobre las vulnerabilidades en la infraestructura tecnológica, los sistemas de información y las áreas o zonas seguras.
9. Gestionar los incidentes de seguridad y privacidad de la información.

## 3.2. POLÍTICA GENERAL

En el cumplimiento de sus funciones institucionales de proteger la vida, el ambiente y el patrimonio de la población de Bogotá D. C., mediante la atención y gestión del riesgo en incendios, rescates, incidentes con materiales peligrosos y otras emergencias, la UAECOB implementará las medidas que estén a su alcance para salvaguardar la integridad, la disponibilidad, la confidencialidad y privacidad de la información necesaria para el cumplimiento de su misión, gestionando los riesgos de manera integral con criterios de efectividad, eficiencia y transparencia en todos sus procesos, y fortaleciendo sus capacidades en materia de seguridad de la información.

En este sentido, se declara como prioritaria la seguridad y privacidad de la información en la ejecución de las labores de la UAECOB, mediante la protección de los activos de información, la infraestructura crítica y de soporte, con el fin de garantizar la continuidad del negocio y sus servicios relacionados; contribuyendo por tanto al cumplimiento de su misión y los objetivos estratégicos institucionales.

## 4. ALCANCE

El alcance de esta política abarca todos los procesos y procedimientos donde la **UAECOB** realice recolección, procesamiento, almacenamiento, supresión, recuperación, intercambio, uso, circulación, transferencia y consulta de información, en el desarrollo de su misión institucional y cumplimiento de sus objetivos estratégicos.

Las políticas de seguridad y privacidad de la información, deben ser cumplidas por servidores, contratistas y terceros que laboren o tengan relación contractual vigente con la **UAECOB**, para alcanzar un adecuado nivel de protección en cuanto a confidencialidad, integridad y disponibilidad de la información.

Este documento debe ser conocido por los servidores y contratistas de la **UAECOB**. Su cumplimiento se debe establecer desde el inicio de los procesos de contratación de la entidad.

## 5. TÉRMINOS Y DEFINICIONES

**Activo:** Recurso del sistema de información o cualquier elemento que tenga valor para la entidad.

**Activo de Información:** Es el elemento de información que cada entidad territorial recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo, incluyendo datos contenidos en registros, archivos, bases de datos, videos e imágenes.

**Administrador del sistema:** Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está dirigida por la Oficina Asesora de Planeación.

**Análisis de riesgos:** Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos específicos y la magnitud de sus consecuencias.

**Ataque cibernético:** Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado, por lo general con intenciones insanas y perjudiciales.

**Auditor interno:** Persona encargada de auditar la entidad en nombre de ella misma. Es el encargado de llevar a cabo los procesos que permiten obtener evidencias y evaluarlas con el fin de determinar si se cumplen los requisitos de un sistema de gestión en una determinada organización.

**Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

**Brecha de seguridad:** deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

**Centro de Datos:** Es una instalación que se encarga del procesamiento de datos e información de manera sistematizada. También conocido como Centro de Procesamiento de Datos, o Data Center. El procesamiento se lleva a cabo con la utilización de computadoras (hardware) y programas (software) necesarios para cumplir con dicha tarea.

**Confidencialidad:** Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo para las personas autorizadas.

**Control:** Mecanismo para reducir el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal. También se denominan salvaguardas o contramedidas.

**Control correctivo:** Conjunto de acciones tomadas para eliminar las causas de una no conformidad detectada u otra situación no deseable.

**Control preventivo:** Conjunto de acciones tomadas para eliminar las causas de una no conformidad potencial u otra situación potencial no deseable.

**Contraseña:** Forma de autenticación privada compuesta por un conjunto de números, letras y caracteres que permiten al usuario tener acceso a un equipo de cómputo, a un archivo y/o a un programa.

**Cracker:** Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

**Custodio de los activos de información:** Parte designada de la entidad, un cargo, encargado de administrar y hacer efectivos los controles de seguridad que el responsable de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

**Datos sensibles:** Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

**Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

**Disponibilidad:** Garantía que tiene el personal autorizado de poder acceder a los activos de la información cuando sea necesario.

**Evento de seguridad de la información:** Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

**Incidente de seguridad de la información:** Identificación de la ocurrencia de un hecho que está relacionado con los activos de información, que indica una posible brecha en las políticas de seguridad o falla en los controles y/o protecciones establecidas.

**Información clasificada:** Se refiere a información que, al ser divulgada, puede causar daño a ciertos derechos de personas naturales o jurídicas, relacionados especialmente con la privacidad de estas. El artículo 18 de la Ley 1712 señala cuáles son esos derechos.

**Información reservada:** Se refiere a casos en los que la entrega de la información al público puede causar daño a bienes o intereses públicos. Estas temáticas están en el artículo 19 de la Ley 1712 de 2014.

**Información pública**: Es toda información que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

**Infraestructura de procesamiento de información:** Cualquier sistema de procesamiento de información, servicio, plataforma tecnológica o instalación física que los contenga.

**Firewall:** Dispositivo que permite bloquear o filtrar el acceso en redes de comunicación.

**Hacker:** Persona que realiza entradas no autorizadas a los sistemas por medio de redes de comunicación como internet, con el objeto de encontrar vulnerabilidades en los sistemas.

**Host:** Término usado en informática para referirse a los computadores conectados a la red que proveen y/o utilizan servicios de ella. Los usuarios deben utilizar hosts para tener acceso a la red.

**Integridad:** Propiedad de salvaguardar la exactitud y completitud de los activos de información.

**Internet:** Conjunto de redes conectadas entre sí que utilizan el protocolo TCP/IP para comunicarse.

**Intranet:** Red privada de uso interno en una empresa o entidad que utiliza el mismo software y protocolos servidores en la internet global.

**LAN:** sigla que hace referencia a Local Área Network, en español Red de Área Local. Red de computadoras ubicadas en el mismo ambiente, piso o edificación.

**Malware:** Código malicioso o cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.

**MSPI:** Modelo de Seguridad y Privacidad de la Información.

**Política:** Lineamientos que fijan la forma en que la entidad previene, protege y administra los riesgos de diferentes daños.

**Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

**Programas utilitarios:** Software que resuelve problemas relacionados con la administración de sistemas de información.

**Red:** Es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

**Responsable de los activos de información:** Conforme el artículo 3° de la Ley 1581 de 2012 es "Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos". En este sentido ese considera como una parte designada de la entidad, rol o cargo, para garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifique adecuadamente, de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables.

**Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

**Seguridad:** Mecanismos de control que evitan el uso no autorizado de recursos.

**Seguridad de la información:** Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información.

**Servidor:** Computadora que comparte recursos con otras computadoras conectadas con ella a través de una red.

**Sistema operativo:** Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora, servidor o dispositivo móvil.

**Terceros:** Toda persona jurídica o natural ajena a la UAECOB, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

**Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.

**Usuario:** Cualquier persona, entidad, cargo, proceso o sistema automatizado que genere, obtenga, transforme, conserve o utilice información en medio físico, o digital a través de las redes de datos y los sistemas de información de la entidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

**Virus:** Software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así programas ejecutables sin la autorización ni el conocimiento del usuario.

**VPN:** Una red privada virtual (RPV) (en inglés, Virtual Private Network, VPN) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

## 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La UEACOB define una estructura organizacional de la seguridad de la información con roles y responsabilidades, lo cual permite contar con un gobierno de seguridad alineado a las necesidades y objetivos estratégicos de seguridad de la información y seguridad digital.

### 6.1. ORGANIZACIÓN INTERNA

**Estructura orgánica**

Está basada en las responsabilidades generales en relación con el organigrama de la entidad.


La responsabilidad de la implementación, desarrollo, operación, control y mejora del Sistema de Gestión de Seguridad de la Información y Seguridad Digital, y su marco de referencia, el Modelo de Seguridad y Privacidad de la Información -MSPI-, en la UAECOB se encuentra a cargo de las siguientes dependencias y roles:

1. La **Dirección General y el Comité Institucional de Gestión y Desempeño** son los responsables a nivel estratégico de articular los esfuerzos y realizar el control y monitoreo a la implementación del Sistema de Gestión de Seguridad de la Información y su marco de referencia, el Modelo de Seguridad de Seguridad y Privacidad de la Información -MSPI y de gestionar los medios y recursos necesarios para tal fin.

2. La **Oficina Asesora de Planeación** es la encargada de coordinar, orientar y promover las actividades requeridas para el mantenimiento y mejora continua del Subsistema de Seguridad de la Información y Seguridad Digital.
3. La **Oficina de Control Interno** será responsable de evaluar el estado del diseño, implementación, funcionamiento y mejoramiento del Subsistema de Seguridad de la Información, de realizar la evaluación independiente y proponer las recomendaciones para el mejoramiento de la gestión institucional.
4. El **Equipo de Seguridad de la Información** asume las responsabilidades a nivel táctico, operativo y de apoyo para armonizar la adecuada implementación, operación y mejora del Subsistema de Gestión de Seguridad de la Información en el marco del Modelo de Seguridad y Privacidad -MSPI-.
5. El **Oficial de Seguridad de la información** es el responsable de administrar y operar adecuadamente el Subsistema de Gestión de Seguridad de la Información con el objeto de dar cumplimiento a los lineamientos de seguridad de la información y seguridad digital que establece la UAECOB.
6. El **líder de tecnología** es responsable de la implementación y gestión de los controles tecnológicos relacionados con la seguridad de la información que afecten sistemas de información, aplicaciones, plataformas de apoyo o infraestructura de comunicaciones y seguridad.
7. Los **líderes de proceso** apoyarán la implementación del Subsistema de Gestión de Seguridad de la información y tendrán a cargo la planificación o actualización de las guías, instructivos, manuales y demás documentos del MSPI que afecten los procesos a cargo.
8. **Los servidores públicos, contratistas, proveedores, estudiantes en pasantía, visitantes y terceros** que interactúen con los Sistemas de Información y demás recursos informáticos de la **UAECOB**:
    i) Cumplir las políticas, manuales, procedimiento, estándares, lineamientos y controles en cumplimiento de los establecido en el Sistema de Gestión de Seguridad de la Información y su marco de referencia el MSPI en el desarrollo de sus funciones u obligaciones a su cargo.
    ii) Ejecutar las actividades requeridas que permitan la implementación del MSPI.

### 6.1.1. Roles y responsabilidades del Sistema de Gestión de Seguridad de la Información

A continuación, se establece un marco de referencia en cuanto a roles y responsabilidades para la gestión, implementación y operación del Sistema de Gestión de Seguridad de la Información -SGSI- en la UAECOB.

| RESPONSABLE | RESPONSABILIDADES |
|---|---|
| Dirección General y Comité Institucional de Gestión y Desempeño | 1. Aprobar la estrategia de seguridad y privacidad de la información.<br>2. Aprobar las políticas de seguridad y privacidad de la información.<br>3. Establecer la visión, decisiones estratégicas y apoyo gerencial para la coordinación de las actividades para dirigir y controlar la seguridad de la información y seguridad digital.<br>4. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad y privacidad de la información.<br>5. Controlar y verificar periódicamente el avance en la implementación y desarrollo del Modelo de Seguridad y Privacidad de la Información -MPSI-.<br>6. Establecer los roles y responsabilidades para gestionar la seguridad y privacidad de la información.<br>7. Controlar y supervisar los riesgos de seguridad de la información con el fin de evidenciar cambios significativos que puedan llegar a impactar el cumplimiento de los objetivos estratégicos de la entidad.<br>8. Aprobar los niveles de aceptación y de tratamiento de los riesgos en seguridad de la información.<br>9. Promover campañas de sensibilización y comunicación al interior de la entidad del Subsistema de Gestión de Seguridad de Información.<br>10. Supervisar la investigación y monitorear los incidentes de seguridad de la información.<br>11. Controlar y monitorear los indicadores de seguridad de la información. |
| Jefe de la Oficina Asesora de Planeación | 1. Coordinar, orientar y promover las actividades requeridas para el mantenimiento y mejora continua del Subsistema de Seguridad de la Información.<br>2. Liderar e impartir lineamientos para implementar la estrategia de seguridad de la información. |
| Equipo de Seguridad de la Información | Asumir las responsabilidades a nivel táctico, operativo y de apoyo para efectos de garantizar la adecuada implementación, operación y mejora del Subsistema de Gestión de Seguridad de la Información en el marco del Modelo de Seguridad y Privacidad -MSPI-.<br><br>El Equipo de Seguridad de la Información de la **UAECOB** está conformado por las oficinas asesoras y subdirecciones o un delegado de los siguientes funcionarios:<br><br>• El jefe de la Oficina Asesora de Planeación<br>• El jefe de la Oficina Asesora Jurídica |

| | |
|---|---|
| | • El jefe de la Oficina de Control Interno<br>• El subdirector de Gestión del Riesgo<br>• El subdirector de Gestión Corporativa<br>• El subdirector de Operativa<br>• El subdirector de Gestión Humana<br>• El subdirector de Logística<br>• El responsable del área de Gestión de Recursos Tecnológicos<br>• El responsable del área de comunicaciones o prensa<br>• El responsable de Seguridad Informática<br>• El oficial de Seguridad de la Información<br><br>El jefe de la Oficina de Control Interno o el delegado será invitado permanente con voz, pero sin voto.<br><br>Serán responsabilidades del Equipo de Seguridad de la Información las siguientes:<br><br>1. Dirigir la implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información y Seguridad Digital e impartir las políticas y directrices de acuerdo con las normas establecidas.<br>2. Impulsar la implementación de la estrategia de seguridad de la información y seguridad digital y la implementación del modelo de Seguridad y Privacidad de la Información -MSPI- al interior de la entidad y participar en la evaluación de planes de acción que se formulen al respecto.<br>3. Evaluar periódicamente el avance en la implementación y desarrollo del Subsistema de Seguridad de la Información y del Modelo de Seguridad y Privacidad de la Información -MPSI- y, según los resultados de esta revisión, definir las acciones pertinentes.<br>4. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.<br>5. Proponer al Equipo Institucional de Gestión y Desempeño, para su aprobación, los cambios en la Política de Seguridad de la Información y las responsabilidades generales en materia de seguridad de la información.<br>6. Evaluar y proponer al Equipo Institucional de Gestión y Desempeño, para su aprobación, iniciativas de inversión para incrementar la seguridad de la información.<br>7. Acompañar e impulsar el desarrollo de proyectos de seguridad.<br>8. Verificar que la seguridad sea parte del proceso de clasificación de la información. |

| | |
|---|---|
| | 9. Validar que la seguridad sea parte del desarrollo de sistemas de información o aplicaciones de software desde sus etapas tempranas.<br>10. Evaluar la eficacia de la gestión de riesgos de seguridad de la información y seguridad digital y de los respectivos planes de tratamiento para mitigar y/o eliminar riesgos.<br>11. Hacer seguimiento a los indicadores de gestión de la seguridad de la información.<br>12. Aprobar programas de sensibilización, concientización y entrenamiento de los funcionarios, contratistas y proveedores.<br>13. Hacer seguimiento a los indicadores de gestión de la seguridad de la información.<br><br>El Equipo de Seguridad de la Información de la **UAECOB** sesionará de manera ordinaria trimestralmente, y extraordinariamente cuando se estime pertinente, previa convocatoria a través de correo electrónico, de sus integrantes. Sesionarán de manera virtual o presencial con la mitad de sus miembros y sus decisiones se tomarán por consenso.<br><br>El Equipo de Seguridad de la Información podrá invitar a cada sesión, con voz y sin voto, los funcionarios o contratistas que considere necesarios por la naturaleza de los temas a tratar.<br><br>De lo debatido en las sesiones se dejará constancia en el acta correspondiente. |
| Líder de Tecnología y Comunicaciones | Responsable de la implementación y gestión de los controles tecnológicos relacionados con la Seguridad de la Información que afecten servicios, sistemas de información, aplicaciones, plataformas de apoyo o infraestructura de comunicaciones y seguridad.<br><br>1. Identificar las necesidades y recursos necesarios (tecnológicos, humanos, de capacitación, financieros, entre otros) para el mantenimiento de la infraestructura de seguridad Informática.<br>2. Definir políticas y procedimientos de gestión de accesos lógicos, esquema y metodología de construcción de roles y perfiles para los accesos a plataformas e infraestructura de la Entidad.<br>3. Definir procedimientos de gestión de logs (registro de actividades sobre sistemas de cómputo).<br>4. Definir líneas base, guías de aseguramiento, etc. para hardening (procesos de aseguramiento) de sistemas.<br>5. Definir la metodología y procedimientos del ciclo de vida de desarrollo de software incluyendo requerimientos de seguridad en cada etapa. |

| | |
|---|---|
| | 6. Definición de la estrategia de respaldo de información.<br>7. Definir políticas y procedimientos de gestión de cambios.<br>8. Definir el diseño de red y plataformas tecnológicas teniendo en cuenta las necesidades de la entidad.<br>9. Implementación de planes de remediación de vulnerabilidades.<br>10. Adquirir e implementar herramientas de gestión de logs y correlación de eventos respecto de los sistemas de cómputo.<br>11. Adquirir e implementar tecnologías de seguridad.<br>12. Adquirir, implementar y configurar la red y las plataformas tecnológicas con el fin de garantizar los aspectos de seguridad.<br>13. Realizar los ajustes y mejoras necesarias en el proceso de desarrollo de software.<br>14. Adquirir e implementar mecanismos de seguridad física.<br>15. Definir los mecanismos de actualización de la plataforma tecnológica por obsolescencia. |
| Oficial de Seguridad de la Información | Administrar y operar el Subsistema de Gestión de Seguridad de la Información y su marco de referencia, el MSPI.<br><br>1. Asesorar a la Oficina Asesora de Planeación y dependencias de la **UAECOB** en materia de seguridad de la información.<br>2. Coordinar la implementación y operación del Sistema de Seguridad de la Información -SGSI- y de las políticas de seguridad de la información, con la participación de las dependencias de la **UAECOB**.<br>3. Establecer la estrategia de seguridad de la información y presentarla para su aprobación.<br>4. Evaluar y sugerir la implementación de controles específicos de seguridad de la información para los sistemas de información o servicios informáticos.<br>5. Apoyar a las diferentes dependencias en la aplicación de las metodologías para la clasificación de la información y el análisis de riesgos de seguridad de la misma.<br>6. Velar por la adecuada actualización de las políticas y lineamientos de seguridad de la información establecidos en la entidad.<br>7. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.<br>8. Hacer seguimiento al comportamiento de los indicadores de gestión de la seguridad de la información que adopte el Equipo de Seguridad de la Información.<br>9. Realizar el diagnóstico de avance de implementación del Subsistema de Seguridad de la Información -SGSI- y su marco de trabajo el Modelo de Seguridad y Privacidad de la información -MSPI-. |

| | |
|---|---|
| | 10. Establecer un programa periódico, por lo menos una vez al año, de revisión de vulnerabilidades de la plataforma tecnológica de la entidad; y coordinar los planes de remediación y de aseguramientos, conforme con los resultados de las mencionadas pruebas.<br>11. Reportar al Equipo de Seguridad de la Información el estado de la investigación y monitoreo de los incidentes de seguridad de la información, los resultados de las auditorias periódicas, y la revisión y supervisión del Subsistema de Gestión de Seguridad de la Información -SGSI-.<br>12. Presentar al Equipo de Seguridad de la Información iniciativas e informes periódicos del estado de seguridad de la información de la entidad.<br>13. Proponer el plan de sensibilización y entrenamiento en aspectos de seguridad de la información.<br>14. Medir y revisar el cumplimiento de los indicadores del Sistema de Gestión de Seguridad de la Información. |
| Líderes de proceso | Apoyar la implementación del Sistema de Gestión de Seguridad de la Información y asumir las siguientes responsabilidades relacionadas con la seguridad de la información:<br>1. Planificar y actualizar las guías, instructivos, manuales y demás documentos del Modelo de Seguridad y Privacidad de la Información -MSPI- que afecten los procesos a cargo.<br>2. Identificar, valorar y clasificar los activos de información que tiene a cargo, con respecto a la confidencialidad, integridad y disponibilidad de la información.<br>3. Realizar el respectivo etiquetado de la información teniendo en cuenta la clasificación definida.<br>4. Mantener actualizada la matriz de activos de información validando los controles de acceso asignado a dichos activos.<br>5. Gestionar los activos de información bajo su responsabilidad, custodia o uso, de acuerdo con el nivel de clasificación y etiquetado definido.<br>6. Conocer, fomentar y dar cumplimiento a la normatividad establecida de seguridad de la información e informar sobre su incumplimiento.<br>7. Participar activamente en las actividades relacionadas con sensibilización y toma de conciencia en seguridad de la información.<br>8. Informar acerca de cualquier oportunidad de mejora para la seguridad de la información de los activos.<br>9. Identificar riesgos asociados con la seguridad de la información y ciberseguridad en los procesos de los cuales son responsables o tienen participación. |

| | |
|---|---|
| | 10. Reportar oportunamente eventos o incidentes de seguridad de la información y ciberseguridad.<br>11. Colaborar activamente en la implantación de los planes de contingencia y continuidad de su proceso relacionado con la información. |
| Los servidores públicos, contratistas, proveedores, visitantes y terceros | 1. Cumplir las políticas, manuales, procedimiento, estándares, lineamientos y controles en cumplimiento de lo establecido en el Subsistema de Gestión de Seguridad de la Información y su marco de referencia, el Modelo de Seguridad y Privacidad de la Información -MSPI- en el desarrollo de sus funciones y obligaciones.<br>2. Ejecutar las actividades requeridas que permitan la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI-. |
| Oficina de Control Interno | Realizar las auditorías internas al Sistema de Gestión de Seguridad de la Información de manera periódica o cada vez que ocurran cambios significativos (nuevos procesos, nuevo proveedor, nuevos usuarios) en la implementación de la seguridad, con el propósito de determinar si los objetivos de control, controles, procesos y procedimientos del Subsistema de Gestión de Seguridad de la Información -SGSI-:<br><br>1. Cumplen los requisitos de la norma NTC-ISO/IEC 27001 y de la legislación aplicable;<br>2. cumplen los requisitos identificados de seguridad de la información;<br>3. están implementados y se mantienen eficazmente; y<br>4. se están ejecutando en forma consistente y conforme con la Política de Seguridad de la Información de la **UAECOB.** |

### 6.1.2. Separación de deberes

a. Todo el personal que tenga acceso a la información de la UAECOB debe tener definidos sus deberes frente a la gestión de la seguridad de la información, con el fin de minimizar el uso no autorizado, indebido o accidental de los activos de información.

b. En todos los sistemas de información de la entidad se deben implementar controles de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, cuando se tenga la posibilidad de acceder a los sistemas de información.

### 6.1.3. Contacto con las autoridades

La UAECOB, debe mantener contacto actualizado con las autoridades competentes para el cumplimiento de la ley, como los organismos de control (Procuraduría General de la Nación, Contraloría General de la República, Defensoría del Pueblo y Fiscalía general de la Nación) y las Fuerzas Militares (Fuerza Pública, Comando Conjunto Cibernético).

La Oficina de Control Interno de la UAECOB debe definir, actualizar y publicar el listado de autoridades a contactar en caso de que se sospeche de la violación de la Ley (Normograma), para mantener contacto con organismos de control y autoridades; los funcionarios y contratistas pueden consultar el marco legal aplicable en el Normograma de la UAECOB.

### 6.1.4. Contactos con grupos de interés

La UAECOB, a través de la Oficina de Tecnología y Comunicaciones, debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior, con el fin de estar al día con la información relacionada con la seguridad de la información, recibiendo comunicados de actualizaciones de software, notificaciones de ataques de vulnerabilidad día cero (o vulnerabilidades nuevas no identificadas por fabricantes de antivirus, por lo cual no está registrada por estos en sus bases de datos como virus, luego no será detectado como virus en las entidades que tengan este herramienta de antivirus), avisos de ciberataques o ataques cibernéticos, reporte de vulnerabilidades y amenazas nuevas.

### 6.1.5. Seguridad de la información en la gestión de proyectos

La seguridad de la información se debe integrar al procedimiento de gestión de proyectos de la UAECOB, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Esto debe aplicar a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los líderes de proyectos, de los dueños de procesos y de los funcionarios y contratistas de la Oficina de Tecnología y Comunicaciones, asegurar que se cumplan las siguientes directrices:

a. Realizar la valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto para identificar los controles necesarios.

b. Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos durante todas las fases del proyecto.

## 6.2. DISPOSITIVOS MÓVILES Y TELETRABAJO

Los dispositivos móviles corporativos (teléfonos inteligentes, tabletas, portátiles, etc.) son herramientas de trabajo que se deben utilizar únicamente para el desarrollo de actividades relacionadas con los procesos de la entidad.

### 6.2.1. Política de Dispositivos Móviles

#### 6.2.1.1. Política para Dispositivos Móviles Corporativos

a. **Conexión a redes de la UAECOB:** la Oficina de Tecnología debe controlar la conexión de dispositivos móviles tales como teléfonos inteligentes, tabletas y computadores personales de los contratistas a la red corporativa, a excepción de los dispositivos que sean propiedad de la UAECOB, con el fin de minimizar los riesgos de seguridad de la información que implica el uso de dispositivos móviles.

b. **Software y protección:** las estaciones de trabajo y equipos portátiles que son propiedad de la UAECOB cuentan con software licenciado y protección contra código malicioso. Solo el personal de soporte de la Oficina de Tecnología está autorizado a instalar softwares específicos en los dispositivos móviles de propiedad de la UAECOB.

c. **Auditoría:** la UAECOB se reserva el derecho de revisar, cuando se requiera, el software instalado y utilizado en equipos de cómputo y servidores; además, para los portátiles de los contratistas que se conecten a la red corporativa, se deben validar algunos aspectos de seguridad, entre estos: antimalware activo y actualizado, sistema operativo legalizado y actualizado y no permitir que se conecten a internet desde la red de los funcionarios, etc.

d. **Registro de equipos:** el grupo de servicios administrativos encargado de inventarios debe mantener un registro de los dispositivos móviles asignados (qué dispositivo y a quién se le asigna).

e. **Mantenimiento de dispositivos:** el mantenimiento de dispositivos que son propiedad de la UAECOB queda restringido al área responsable de su mantenimiento (área de tecnología). Por tanto, debe controlar que el usuario no haga cambios en el hardware, instale software o modifique la configuración del equipo sin autorización de la Oficina de Tecnología.

f. **Almacenamiento de la información:** la información de la UAECOB que no sea estrictamente necesaria para el desarrollo de las tareas del usuario no debe almacenarse en el dispositivo. Si se accede a la información desde varios dispositivos,

esta tiene que estar sincronizada para evitar duplicidades y errores en las versiones. Los funcionarios autorizados por su respectivo superior deben solicitar a la Oficina de Tecnología la creación de los almacenamientos de datos para el intercambio de información al interior de la Entidad.

g. **Notificación en caso de infección:** Si un funcionario o contratista sospecha la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible al personal de mesa de ayuda.

h. **Transporte y custodia**: los computadores de la UAECOB no deben quedar expuestos a altas temperaturas que puedan dañar sus componentes. El usuario debe evitar que se pueda acceder a la información almacenada en el mismo.

   En ningún caso se debe descuidar el portátil, celular o tableta si se viaja en transporte público. También deben estar protegidos físicamente contra hurtos, especialmente cuando se dejan en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reuniones, es recomendable el uso de guayas de seguridad. En caso de hurto del equipo se debe notificar de manera inmediata al personal de servicios administrativos grupo de inventarios y realizar la denuncia respectiva ante la Policía Nacional.

   Los dispositivos que contienen información clasificada o reservada para la UAECOB no se deben dejar sin supervisión y, donde sea posible, deben estar protegidos bajo llave o se debe usar guayas para asegurarlos; adicionalmente, los computadores portátiles que habiéndose extraídos de la UAECOB posteriormente sean hurtados, se debe comunicar inmediatamente al Oficial de Seguridad de la Información, para seguir los pasos de reporte del incidente y comunicarlo a la entidad judicial competente.

   La información sensible o crítica para la UAECOB no debe reposar o ser almacenada en los equipos personales de los contratistas, para esto se deben usar los repositorios corporativos.

i. **Uso del puesto de trabajo:** el usuario debe aplicar las buenas prácticas de uso del puesto de trabajo que sean relativas al uso de un equipo móvil (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, definir un patrón de seguridad o contraseña de acceso al iniciar el sistema, contar con antivirus actualizado de manera permanente para su dispositivo y mantener las ultimas actualizaciones de seguridad en el sistema operativo).

j. **Responsabilidades:** el usuario es el responsable del equipo portátil o móvil que se le facilite para el desempeño de sus tareas fuera de las instalaciones de la UAECOB. Por

tanto, es el funcionario el que debe garantizar la seguridad tanto del equipo como de la información que contiene. Esta normativa es de obligatorio cumplimiento y debe ser objeto a los acuerdos que se firmen al aceptar el uso de estos dispositivos. En caso de incumplimiento o develamiento de información indebida y de tratarse de un funcionario se iniciará un proceso disciplinario y en caso de ser un contratista o proveedor se podrá declarar incumplimiento del acuerdo de confidencialidad e iniciar procesos legales pertinentes.

k. **Viajes de trabajo:** Los funcionarios o contratistas que viajan por asuntos de la entidad son responsables de la seguridad de la información propiedad de la UAECOB.

#### 6.2.1.2. Política de uso de dispositivos móviles no corporativos

a. **Acceso a contratistas:** el contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato en lo posible debe:

- Tener y usar solo software legal instalado en su equipo.
- Contar con software antivirus licenciado.

b. **Información en dispositivos propios:** los contratistas no deben tener información corporativa en sus dispositivos móviles personales.

c. **Antivirus en dispositivo móvil:** es recomendable contar con un software antivirus en su dispositivo móvil.

d. **Apps en dispositivos móviles:** se recomienda solo descargar aplicaciones de sitios oficiales.

e. **Almacenamiento de información:** En lo posible se debe evitar almacenar información de la UAECOB en los dispositivos móviles personales.

### 6.2.2. TELETRABAJO

La implementación del teletrabajo en la UAECOB supone una transformación organizacional, desde sus formas de planear y hacer, hasta sus formas de realizar seguimiento y evaluación. La adopción de esta modalidad y organización laboral requiere del liderazgo del equipo directivo y la participación de un equipo de trabajo coordinado, la utilización de recursos y la movilización hacia un cambio cultural y de procedimientos, que son posibles de alcanzar con el apoyo de las directivas que respalden las iniciativas de aplicar el teletrabajo. Talento Humano es la dependencia que lidera las alternativas y

lineamientos que buscan un compromiso institucional y realiza las acciones para la adopción e implementación del teletrabajo, buscando que se generen beneficios para sus funcionarios.

#### 6.2.2.1. Lineamientos para la UAECOB

a. Garantizar que los equipos de trabajo en caso de ser suministrados a los teletrabajadores tengan los medios de protección adecuados para la tarea a realizar.

#### 6.2.2.2. Lineamientos para el teletrabajador

a. Utilizar los equipos y herramientas en caso de ser suministrados en forma adecuada.

b. Cumplir, en la medida de lo posible, que la información procesada y almacenada se consolide en la infraestructura tecnológica de la entidad.

c. Verificar, en la medida de lo posible, que sus dispositivos, incluido el enrutador de internet, estén actualizados.

d. Evitar acceder a redes wifi-públicas y procurar conectarse a redes de conexiones a internet seguras y protegidas con contraseña.

e. Asegurar la comunicación a través de herramientas seguras de mensajes de datos, de modo que, si los sistemas de información no funcionan y el correo electrónico no se encuentra disponible, no se pierda la comunicación.

f. Cumplir con las políticas definidas por la entidad respecto al uso de equipos, aplicaciones y programas informáticos, protección de datos personales, propiedad intelectual y seguridad de la información que se encuentren señaladas en la ley.

g. Utilizar los datos de carácter personal, privado o sensible a los que tenga acceso, única y exclusivamente, para cumplir con las funciones propias en la UAECOB, así como garantizar que ningún tercero tenga acceso por cualquier medio a los datos de carácter personal, privado o sensible de la entidad.

h. Informar a la Oficina de Tecnologías, según la ruta establecida, sobre conflictos de red o problemas tecnológicos o del equipo que requieran ser solucionados para el cumplimiento de las funciones.

i. El teletrabajador se compromete a guardar la máxima reserva y confidencialidad sobre las actividades laborales que desarrolle. Se considera información confidencial la información de propiedad de la entidad y la información que genere el Teletrabajador en virtud de su vinculación laboral.

#### 6.2.2.3. Lineamientos para la Oficina de Tecnologías e Información

a. Fortalecer las capacidades de monitoreo para la operación remota, con el fin de detectar accesos indebidos o situaciones anormales.

b. Contar con las capacidades y disponibilidad de los servicios de VPN, seguridad en los servicios de correo electrónico y el acceso a la información de la entidad, realizando un análisis de riesgos.

c. Fortalecer el monitoreo en el uso de los datos personales e información confidencial.

d. Realizar oportunamente copias de seguridad de los datos tanto en las plataformas físicas como en la nube.

e. Disponer de protocolos para contar con una clara identificación de roles y responsabilidades del personal de la Oficina de Tecnología.

f. Contemplar herramientas para la gestión remota en la entidad.

g. Preparar al personal de mesa de ayuda que prestan el soporte para la instalación y la configuración de los equipos para trabajo remoto.

h. Contemplar las políticas y procedimientos para evitar disputas acerca de derechos de propiedad intelectual desarrollados en equipos de propiedad privada de los funcionarios y contratistas.

i. Verificar el uso de software licenciado, de tal forma que la UAECOB quede eximida de responsabilidades por el no licenciamiento de software en las estaciones de trabajo de propiedad de los funcionarios y contratistas.

j. Determinar requisitos de seguridad sobre el firewall, y de protección contra software malicioso.

#### 6.2.2.4. Directrices y acuerdos por incluir

a. La UAECOB podrá, eventualmente, suministrar un equipo adecuado para las actividades de teletrabajo.

b. La UAECOB podrá eventualmente suministrar equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto.

c. El equipo de la UAECOB en el hogar del teletrabajador debe ser utilizado solo por el funcionario de la UAECOB.

d. La UAECOB debe suministrar soporte y mantenimiento del hardware y el software a los equipos de su propiedad asignados al teletrabajador.

e. Se debe realizar, ocasionalmente, auditoría y seguimiento de la seguridad en los sitios de teletrabajo.

f. La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos de propiedad de la UAECOB asignados al teletrabajador cuando las actividades del teletrabajo finalicen.

#### 6.2.2.5. Método de conexión de la modalidad de acceso remoto en la UAECOB

Actualmente la UAECOB aplica el trabajo en casa (Circular 041 del 2020 expedida por el Ministerio de Trabajo) tanto para funcionarios como para contratistas; a su vez, se están estableciendo los lineamientos para cumplir con el marco regulatorio de teletrabajo únicamente para los funcionarios.

La siguiente es la forma de conectarse a las plataformas de la UAECOB en la modalidad de acceso remoto y trabajo en casa:

a. Cuando se requiera realizar labores de trabajo en casa el líder del proceso debe solicitar a La Oficina de Tecnología la creación de una VPN de acceso en los recursos tecnológicos que se hayan definido para trabajo fuera de oficina, indicando el tiempo de acceso por el cual se requiere la conexión.

b. El funcionario o contratista debe haber instalado el cliente de VPN en el computador personal de su hogar, con el fin de conectarse vía remota a los servicios tecnológicos de la UAECOB. Por otro lado, es posible omitir el cliente VPN si al funcionario se le ha asignado un escritorio virtual.

c. Una vez ejecute el cliente de VPN en el equipo de su casa debe autenticarse con las credenciales otorgadas por la Oficina de Tecnología de manera individual y personal.

d. Establecida la conectividad a través de la IP (es una dirección única que identifica a un dispositivo en Internet o en una red local) del computador de escritorio en las oficinas de la UAECOB el usuario debe autenticarse con las credenciales normales de acceso brindadas por el Directorio Activo (Active Directory (AD) es una base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo.). Esto permite que el usuario ingrese a los sistemas de información y recursos compartidos como si estuviera dentro de las oficinas de la UAECOB.

e. El usuario no debe copiar archivos desde el sistema de archivos del computador de la casa hacia el computador al cual está conectado por la VPN y que es propiedad de la UAECOB.

f. Todos los archivos que gestione el usuario mientras esté conectado por VPN en la estación de trabajo propiedad de la UAECOB no deben ser descargados a las unidades locales o escritorio del computador de la casa.

g. Es importante que el usuario no se conecte a internet a sitios web como YouTube, plataformas de streaming, redes sociales, entre otras a través de la VPN y desde la estación de trabajo de la UAECOB.

h. Adquirir la rutina de desconexión y conexión continua mientras se realizan labores que no requieren de conectividad.

i. Identificar la forma adecuada de desconexión de su estación de trabajo de la UAECOB para no cometer el error de apagar esta estación de trabajo. En caso de apagar esta estación de trabajo de la UAECOB en forma remota no le permitirá establecer conexiones futuras y deberá acudir a la línea de soporte de la Oficina de Tecnología.

j. El usuario de dispositivos móviles debe usar su carpeta virtual de office 365 (One Drive) para garantizar copias de respaldo de su información a través de esquemas de backups automáticos.

k. La Oficina de Tecnología debe asegurarse de incorporar en la póliza de seguro de equipos de cómputo los dispositivos móviles de la UAECOB.

## 7. SEGURIDAD DE LOS RECURSOS HUMANOS

### 7.1. Antes de asumir el empleo.

#### 7.1.1. Previa vinculación de un funcionario es importante considerar

Es importante que el Grupo de Gestión de Talento Humano, proporcional a las responsabilidades o al manejo de información sensible de la entidad, establezca un proceso de verificación de los antecedentes de los candidatos que aspiran a un cargo, el cual se debe llevar a cabo de acuerdo con las leyes y reglamentos, siendo proporcionales a los requisitos dentro de la UAECOB, a la clasificación de la información que va a tener acceso y a los riesgos percibidos.

La modalidad de teletrabajo en la UAECOB únicamente aplica a funcionarios nombrados en carrera administrativa.

#### 7.1.2. Previa vinculación de un contratista se debe considerar

La verificación está a cargo del Grupo de Contratación, la cual debe tener en cuenta toda la privacidad pertinente y la protección de la información de datos personales y cuando se permita, debe incluir lo siguiente:

- Una verificación (completa y precisa) de la hoja de vida del solicitante;
- Confirmación de las certificaciones y títulos brindados.
- Una verificación más detallada, como la información de antecedentes penales.
- Establecer acuerdos o compromisos contractuales con el personal contratista donde se indiquen las responsabilidades en cuanto a la seguridad de la información.
- Firma del formato de autorización de tratamiento de datos personales por parte del contratista.

### 7.2. Durante la ejecución del empleo.

#### 7.2.1. Inicio de ejecución del contrato

El cumplimiento de las Políticas de Seguridad de la Información por parte de todos los funcionarios, contratistas, proveedores, o cualquier persona que tenga una relación contractual o situacional con la entidad o que tenga acceso a los activos de información de la UAECOB debe ser informado en el momento que inicie sus actividades contractuales, desde Talento Humano, para los funcionarios de planta, y desde el supervisor del contrato,

para los demás colaboradores de la entidad, con apoyo del Oficial de Seguridad de la Información y, además:

a. Todo funcionario, contratista, proveedor o tercero que desde su gestión o alcance del contrato requiera del acceso a un sistema de información, por ejemplo, SIM, FUOCO, CONTROLDOC, etc. o a la red corporativa de la UAECOB, debe hacer la solicitud a través del formato de acceso lógico y físico, el cual será autorizado por el líder del grupo o supervisor del contrato.

b. La solicitud a través del formato de acceso lógico y físico debe especificar claramente los permisos que el funcionario, contratista, proveedor o tercero, requiere para sus actividades y acceso a los sistemas de información u otro componente tecnológico, especificando los privilegios a ser asignados en el sistema de información.

c. Desde la Oficina de Tecnología se debe gestionar el requerimiento descrito desde el formato de acceso lógico y físico dando alcance a cada solicitud con el especialista del sistema de información o componente tecnológico que corresponda.

d. Desde la Oficina de Tecnología se debe notificar el alcance dado desde la solicitud del formato de acceso lógico y físico, con el fin de que el funcionario, contratista, proveedor o tercero, sea notificado y dé inicio a sus labores o actividades contractuales.

### 7.2.2. Durante la ejecución del empleo de funcionario o contratista

Todos los funcionarios o contratistas a los que se brinde acceso a información confidencial deben firmar un acuerdo de confidencialidad y no divulgación de información, antes de tener acceso a las instalaciones de procesamiento de información. Además:

a. Los dueños de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades y derechos legales con relación a leyes sobre derecho de autor o legislación sobre protección de datos personales.

b. Los dueños de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades para la clasificación de la información y la gestión de activos institucionales asociados con información, instalaciones de procesamiento de información y servicios de información que deben ser manejados por el funcionario o contratista.

c. Los líderes de proceso deben asegurarse de que los funcionarios y contratistas

conozcan las responsabilidades del funcionario o contratista para el manejo de la información recibida de otras entidades o partes externas.

d. Talento Humano y el Grupo de Contratación deben asegurar que los funcionarios y contratistas conozcan y acepten la política de seguridad de la información, para esto deben informar al Oficial de Seguridad de la Información para que les indique las medidas a seguir para el acceso a esta política.

e. Talento Humano debe establecer los mecanismos para asegurar que los funcionarios tomen las charlas de sensibilización en seguridad de la información brindadas por la Ofician Asesora de Planeación. Se debe tener en cuenta el manejo de datos personales, clasificación de la información, solicitud de recursos tecnológicos, incidentes de seguridad de la información y puntos de atención para asesoría sobre seguridad de la información.

f. El Grupo de Contratación debe establecer los mecanismos para asegurar que los funcionarios tomen las charlas de sensibilización en seguridad de la información brindadas por la Oficina de Tecnología. Se debe tener en cuenta el manejo de datos personales, clasificación de la información, solicitud de recursos tecnológicos, incidentes de seguridad de la información y puntos de información para asesoría sobre seguridad de la información.

g. Talento Humano, o el supervisor del contrato para los contratistas y/o terceros, debe comunicar a la Oficina de Tecnología los cambios de cargo de personal, indicando los cambios en los recursos tecnológicos asignados, especialmente actualizaciones sobre los accesos a carpetas compartidas y sistemas de información.

### 7.3. Terminación o cambio de empleo.

#### 7.3.1. Terminación o cambio de responsabilidades de empleo

Se debe informar al personal los deberes y responsabilidades después de la terminación del empleo o contrato.

Previa emisión de paz y salvo para el funcionario o contratista se debe considerar:

a. Tener formato de paz y salvo firmado por la Oficina de Tecnología, el cual asegura que se retiraron los accesos lógicos y físicos de acuerdo con el procedimiento de control de acceso.

b. Tener formato de paz y salvo igualmente firmado por el jefe inmediato o supervisor de contrato donde se aseguró de la transferencia apropiada de información al sucesor del cargo, informe de gestión que indica el estado de las actividades realizadas (en desarrollo, finalizadas o pendientes) y la aceptación del jefe inmediato o supervisor de contrato.

c. Para el caso de contratistas, los accesos lógicos se deben mantener únicamente durante el tiempo del contrato. En caso de presentarse tareas pendientes estas deben realizarse con el usuario supervisor del contrato, por lo cual, las tareas pendientes en controldoc deben ser trasladadas al supervisor del contrato o a quien este delegue.

d. Mantener las responsabilidades frente a la confidencialidad de la información de la entidad en caso de desvinculación del funcionario o contratista.

e. El responsable de la dependencia debe notificar por medio de la Mesa de Ayuda acerca de la necesidad de bloquear provisionalmente los accesos a cargo del funcionario, cuando se produzca ausencia temporal o vacaciones.

### 7.3.2. Procesos Disciplinarios

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la Ley 734 de 2002 (Código Único Disciplinario) y la Ley 1952 de 2019 (Por medio de la cual se expide el código general disciplinario) y demás legislación aplicable con relación a los procesos disciplinarios, la UAECOB sigue los lineamientos de los procedimientos establecidos a su interior.

## 8. GESTIÓN DE ACTIVOS

Si bien es cierto que los sistemas de información y la información digital están sujetos a amenazas graves desde el ciberespacio, que pueden tener impactos adversos a la operación comprometiendo los activos de información, tales impactos adversos también pueden llegar a comprometer la confidencialidad, integridad y disponibilidad de la información procesada, almacenada y transmitida.

Es así como se deben proporcionar niveles de protección a todos los activos de información de la entidad. Todas estas medidas o lineamientos están destinadas a mitigar los posibles riesgos.

### 8.1. Inventario de activos

Cada área debe ser responsable de mantener actualizado el inventario de activos de seguridad de la información con el acompañamiento del Oficial de Seguridad de la Información de acuerdo con las directrices del Procedimiento de Gestión de Activos.

### 8.2. Uso aceptable de los activos

a. La información, archivos físicos, sistemas, servicios, y los equipos (estaciones de trabajo, portátiles, impresoras, redes, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, faxes, entre otros) propiedad de la UAECOB son activos de la entidad y se proporcionan a los funcionarios, contratistas y proveedores o terceros autorizados para cumplir con los propósitos de su trabajo.

b. Los funcionarios, contratistas, proveedores o terceros y todo aquel que cuente con acceso a la información de la UAECOB debe reportar los eventos de seguridad de la información identificados, de acuerdo con el Procedimiento de Gestión de Incidentes.

### 8.3. Uso de equipos de cómputo de propiedad de la UAECOB

a. Está prohibido que personal ajeno a la Oficina de Tecnología destape o retire partes de los equipos de cómputo de propiedad de la UAECOB.

b. La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad de la Oficina de Tecnología y, por tanto, se debe solicitar soporte a ella para la realización de estas labores.

c. Los equipos de cómputo no deben ser trasladados del sitio asignado inicialmente, ni cambiar el funcionario al que le fue asignado, sin previo aviso a la Oficina de Tecnología.

d. Debe respetarse y no modificarse la configuración de hardware y software establecido por la Oficina de Tecnología.

e. No se autoriza el uso de medios extraíbles para almacenamiento de información institucional (USB, celulares, tarjetas de memoria, etc.) en las estaciones de trabajo de la entidad, con excepción de aquellos funcionarios que, por sus funciones y actividades propias institucionales, sean autorizados por directivos o jefes de oficina mediante el formato de acceso lógico y físico debidamente diligenciado. Las tabletas institucionales no requieren autorización y se hará uso de ellas sin restricción alguna.

f. Toda actividad informática (escaneos de seguridad, ataques de autenticación o de

denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información de la UAECOB están prohibidas.

g. Durante la permanencia en las instalaciones de la UAECOB, los equipos de cómputo externos deben estar conectados únicamente a la red de datos corporativos configurada por la oficina de Tecnología.

h. Todas las estaciones de trabajo deben apagarse o hibernarse al finalizar la jornada laboral.

i. Los equipos de cómputo (CPU y monitor), servidores, teléfonos, IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados, con el fin de evitar picos alto que puedan dañar el componente tecnológico.

j. La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de la UAECOB y que no son propiedad de la entidad, es responsabilidad única y exclusiva de sus propietarios. La UAECOB no es la responsable por estos equipos en ningún caso.

k. Los dueños de procesos deben clasificar la información tanto física como digital como: información pública, información pública clasificada e información pública reservada.

l. Los dueños de procesos deben identificar los riesgos digitales y reportarlos al área de seguridad de la información. Para esto, es importante que los funcionarios y contratistas de las diferentes dependencias asistan a las capacitaciones en riesgos digitales brindadas por la Oficina Asesora de Planeación.

### 8.4. Uso de internet

a. No se autoriza a los funcionarios y contratistas acceder a cualquier sitio web o dirección que contenga material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de la entidad como violencia, terrorismo, grupos al margen de la Ley, discriminación, entre otras.

b. No se autoriza el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o institucional.

c. Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones

no autorizadas y errores en la red de la UAECOB, no se permite el envío o descarga de información masiva como música, videos y software no autorizado.

d. Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta de acceso.

e. Todas las actividades realizadas en los sistemas de información de la UAECOB deben ser monitoreadas con el fin de preservar la seguridad informática de la entidad.

f. Ningún usuario está autorizado para asignar claves de administrador sobre los computadores de la entidad. Esto es competencia de la Oficina de Tecnología.

g. Los usuarios no deben intentar burlar los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la entidad.

### 8.5. Uso del Correo Institucional

a. La Entidad debe proveer a los usuarios un correo electrónico institucional con el dominio bomberosbogota.gov.co.

b. El estándar para la creación de buzón del correo es: primera letra del nombre + primer apellido; por ejemplo, el correo de Pablo González Roa sería: pgonzalez. En caso de que exista un homónimo se debe agregar a la fórmula anterior la primera letra del segundo apellido: pgonzalezr. Si continúa la homonimia la Oficina de Tecnología debe asignar un correo basado en el nombre completo del colaborador.

c. La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y el buzón asociado a la entidad.

d. El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la entidad, esto es, para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo desempeñadas.

e. El correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo, no es una herramienta de difusión masiva de información y no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.

f. Cuando se reciban correos desde una cuenta de divulgación se debe evitar dar una respuesta utilizando la opción responder a todos.

g. El servidor de correo debe bloquear archivos adjuntos o información nociva como archivos .exe o de ejecución de comandos.

h. Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener un código malicioso (virus, troyanos, keyloggers, gusanos, etc.) que eventualmente podría atentar contra los sistemas, programas y datos de la entidad.

i. Se recomienda no usar o revisar indebidamente la cuenta de correo electrónico de otro usuario como si fuera propia; sin embargo, es responsabilidad de cada usuario el manejo de sus credenciales de acceso, mantener sus sesiones atendidas, entiéndase no dejar los equipos sin cerrar sesión al alcance de cualquier intruso.

j. El usuario debe notificar cualquier recibo de correo sospechoso a la cuenta mesadeayuda@bomberosbogota.gov.co, el correo sospechoso no debe ser abierto ni reenviado a ningún usuario.

### 8.6. Clasificación de la información

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la ley 1712 de 2014 y la Ley 1581 de 2012 de protección de datos personales la UAECOB clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con el Procedimiento de Gestión de Activos y, además:

a. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que el activo está inventariado en la Matriz de Activos de Información o informar al Oficial de Seguridad de la Información para su debido registro.

b. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que los activos están clasificados y protegidos apropiadamente.

c. El funcionario, contratista, proveedor y/o tercero responsable del activo de información, debe definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables.

d. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

### 8.7. Gestión de medios removibles

Los medios removibles en los que se almacene información clasificada como información pública clasificada e información pública reservada deben estar cifrados, de acuerdo con las directrices del procedimiento de gestión de activos. La Oficina de Tecnología debe establecer herramientas tecnológicas para el cifrado de la información y, además:

a. La Oficina de Tecnología debe proveer el uso de carpetas compartidas en lugar de medios removibles para el intercambio de información al interior de la entidad.

b. Las unidades de medios removibles de las estaciones de trabajo, equipos portátiles y servidores se deben bloquear mediante la herramienta endpoint; quien requiera hacer uso de estas unidades debe solicitar la activación a la Oficina de Tecnología, previa autorización del coordinador de grupo, indicando el tiempo por el cual se requiere la activación.

c. Los funcionarios o contratistas que requieran los medios removibles habilitados de forma permanente deben tener una autorización firmada por el jefe de oficina o coordinador de grupo.

d. Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la entidad se debe remover y luego de ello formatear el dispositivo.

e. Los medios removibles no deben ser utilizados en sitios públicos y deben tratarse bajo cuidado alejado de daños externos como agua, polvo o fuego.

### 8.8. Disposición de los medios

a. Los medios que contienen información confidencial se deben disponer en forma segura, mediante incineración, destrucción o el borrado de datos antes de ser reutilizados o dados de baja.

b. La información en las cintas de backups que contienen información pública clasificada o información pública reservada se debe cifrar y, además, debe estar protegida en un lugar seguro y bajo llave en el lugar que disponga la Oficina de Tecnología.

c. La información almacenada en medios removibles debe ser transferida a medios nuevos antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos.

d. Se debe guardar al menos una copia de datos valiosos para la UAECOB en medios separados, con el fin de evitar la pérdida de información por daño o hurto de los medios

removibles.

e. Las cintas de backups se deben guardar en una ubicación alterna a la localización de los datos o aplicaciones para aumentar la seguridad ante posibles impactos de desastres ambientales, accidentes, incendios, etc.

f. Se debe realizar pruebas a las copias de datos para validar la integridad de la información.

### 8.9. Transferencia de medios físicos

a. Para la transferencia de medios físicos (información en carpetas selladas, computadores, dispositivos móviles, tabletas, etc.) se debe seguir las directrices del Procedimiento de Gestión de Activos y sus documentos relacionados (mensajería externa o interna - tabla controles según clasificación de información).

b. El embalaje de la información debe ser apropiada para que mitigue los daños físicos que se puedan presentar en el transporte de la misma, protegiendo la exposición al calor, humedad o campos electromagnéticos.

c. Se debe llevar un registro que identifique el contenido de los medios, la protección aplicada, los tiempos de transferencia a los responsables durante el transporte y el recibo en su destino.

## 9. CONTROL DE ACCESO

### 9.1. Lineamientos sobre control de acceso

La oficina de tecnología debe controlar el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:

a. **Lo que necesita conocer:** solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).

b. **Lo que necesita usar:** solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.

### 9.2. Acceso a redes y servicios en red

a. El acceso a redes Wi-Fi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK.

b. La Oficina de Tecnología provee un servicio de conectividad a todos los funcionarios y contratistas de la entidad para la navegación en internet, dicho acceso es controlado por usuario mediante la autorización previa de las direcciones, jefes o coordinadores de grupo, mediante el formato de acceso lógico y físico.

c. Para los usuarios que requieran contar con servicios especiales de mensajería instantánea, sitios web de encuentro o descargas, deben ser autorizados por el jefe inmediato o supervisor del contrato, mediante formato de acceso lógico y físico dirigido a la Oficina de Tecnología, justificando la necesidad del acceso.

d. La conexión remota a la red de área local de la UAECOB debe ser realizada a través de una conexión VPN segura, suministrada por la Oficina de Tecnología, la cual debe ser aprobada por los jefes de oficina mediante el formato de acceso lógico y físico dirigido al jefe de la Oficina de Tecnología.

e. La conexión a servicios en red se controla mediante el directorio activo, a excepción del control de acceso físico el cual se controla a través de acceso biométrico y el servicio de impresión.

f. La conexión a redes públicas abiertas desde equipos corporativos de la UAECOB está prohibida, así como la conexión a redes Wi-Fi públicas.

g. Todo acceso o privilegio a sistemas, redes, aplicaciones o información de la UAECOB debe estar aprobado por los líderes de las áreas y los propietarios de información según aplique.

h. El acceso a la red Wi-Fi de la UAECOB para los visitantes debe realizarse por la red destinada para estos accesos a visitantes, de no conocer este acceso se debe solicitar a la Mesa de Ayuda para su debida activación.

i. Es responsabilidad del Oficial de Seguridad de la Información definir los lineamientos a seguir para garantizar accesos seguros y confiables a los sistemas y plataformas de la UAECOB.

### 9.3. Solicitud o inicio de acceso

Los procedimientos definidos por la UAECOB para administrar los privilegios de acceso de los usuarios a la información de la UAECOB deben comprender la asignación, la modificación y la revocación de los permisos. Todos los sistemas, recursos y aplicaciones, que procesen cualquier información propietaria deben requerir autenticación y debe tener en cuenta por lo menos, que:

a. Los líderes de grupo son los únicos funcionarios autorizados para realizar las solicitudes de acceso a los sistemas de información mediante el formato de acceso lógico y físico.

b. Ningún colaborador autorizado puede realizar solicitudes de acceso para sí mismo. Por ejemplo, la jefatura de la Oficina Asesora de Planeación no puede realizar una solicitud para tener nuevos privilegios en un sistema de información como por ejemplo Controldoc, debe solicitar la aprobación de la Dirección.

c. Los jefes o delegados deben realizar las solicitudes de acceso a los sistemas de información requeridos por los funcionarios o colaboradores a su cargo en las herramientas establecidas por la UAECOB. Para tal fin, se debe tener en cuenta las matrices de accesos previamente definidas y gestionadas por cada especialista funcional de la Oficina de Tecnología.

d. La Oficina de Tecnología asigna a los usuarios los permisos de acceso a la información con base en los roles y perfiles del usuario aprobados por los responsables de cada grupo y/o proceso.

e. La confirmación de la gestión del requerimiento y el envío de los datos de autenticación deben ser enviados usando un canal seguro. Esta entrega debe estar controlada por un proceso de administración formal que permita informar a los usuarios sobre el compromiso de cumplir con los lineamientos de seguridad establecidos para el buen uso de los datos de acceso (usuarios y contraseña) otorgados.

f. La reutilización de nombres de cuentas no está permitida, aun cuando la cuenta de usuario ya se encuentre eliminada/inactiva. Para evitar esto la Oficina de Tecnología debe aplicar el procedimiento definido para la creación de cuentas de usuario y correo electrónico.

g. Asignar identificaciones únicas a todos los funcionarios y colaboradores, es decir, que no debe existir cuentas genéricas para el acceso o gestión sobre los sistemas tecnológicos de la entidad (equipos, aplicaciones, bases de datos, sistemas operativos, entre otros). En el Directorio Activo se debe detallar el responsable de cada cuenta de servicio.

h. La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar, es decir, el uso de las claves de usuarios administradores tales como: «root», «adm» y «system», entre otros, debe ser controlado por la Oficina de Tecnología, quienes son los responsables de dichos accesos y de esta gestión existirá un registro que permita identificar al funcionario o colaborador que está haciendo uso de estos accesos.

i. Todo usuario del sistema debe tener un mecanismo de autenticación privado.

j. En caso de ser necesario, se debe utilizar métodos de autenticación fuertes como sensores biométricos, huellas dactilares o tokens de hardware.

k. El acceso de un usuario debe ser limitado a la información requerida para el desarrollo de sus funciones.

l. Para los equipos de cómputo se debe establecer bloqueos o terminación de sesiones automáticas en caso de que queden desatendidos, con el propósito de proteger la información.

m. La utilización de información compartida, como unidades de red, debe estar restringida mediante controles ejecutados por la Oficina de Tecnología. El responsable y/o dueño de la información debe definir los accesos a la información únicamente al personal autorizado.

n. Todos los usuarios creados en ambiente de producción de los sistemas de información o servicio de la UAECOB deben ser solicitados según el procedimiento establecido en el formato de acceso lógico y físico, con el fin de mantener un registro formal o la trazabilidad de los privilegios otorgados a los colaboradores autorizados para cumplir con las labores asignadas.

o. Los accesos a la información o sistemas de información no deben otorgarse por los administradores de base de datos y de aplicaciones del servicio hasta que se hayan completado los procedimientos de autorización.

p. Se debe considerar la inclusión, en los contratos del personal y contratos de servicio con terceros, de cláusulas que especifiquen las sanciones si los colaboradores o terceros intentan un acceso no autorizado.

### 9.4. Suspensión o terminación de acceso

El acceso a los sistemas debe ser suspendido para todo funcionario o colaborador de la UAECOB que se encuentre en licencia, permisos, vacacione u otras situaciones administrativas que impliquen la separación temporal o definitiva del servicio estipuladas en el Decreto 1083 de 2015, además:

a. La Oficina de Tecnología debe mantener actualizado el Directorio Activo con la información de los usuarios de funcionarios y colaboradores, de acuerdo con el último formato de acceso lógico y físico solicitado para la gestión de los usuarios de la UAECOB, en el cual debe registrarse las novedades de estos para que se realice la suspensión o eliminación según corresponda.

b. Se debe definir y aplicar reglas para deshabilitar las cuentas de usuarios de red que no han cambiado la contraseña durante 60 días; igualmente, se debe definir qué cuentas deben quedar bloqueadas porque no fueron reactivadas y eliminar aquellas cuentas que no presentan ninguna actividad desde su creación.

c. Los usuarios creados con acceso a las bases de datos que no hayan sido utilizados en un período mayor o igual a 3 meses deben ser inhabilitados por los administradores de base de datos; asimismo, si estas no han sido utilizadas en un periodo igual o mayor a 6 meses debe ser eliminadas.

d. La Oficina de Tecnología debe disponer de mecanismos documentados para desactivar el acceso a los usuarios en las siguientes situaciones:

    - Desvinculación por parte de los funcionarios a la UAECOB.
    - Desvinculación por parte de contratistas de la UAECOB.
    - Ausencias temporales de los colaboradores por motivo de vacaciones, viajes o licencias.
    - Los funcionarios de la Entidad que no han accedido a los recursos tecnológicos por un período determinado.
    - Número de intentos fallidos durante el ingreso de la contraseña a un recurso tecnológico o aplicativo o cuando se presente algún tipo de incidente de seguridad de la información sobre el código de usuario.
    - Cuando el responsable de la información lo solicite.

### 9.5. Revisión o validación de accesos

Las autorizaciones de acceso a sistemas y/o aplicaciones deben ser revisadas periódicamente por los coordinadores de área y/o propietarios de la información.

El Oficial de Seguridad de la Información debe revisar o monitorear en intervalos de tiempo regulares los privilegios asignados a los usuarios, para asegurar que no tengan accesos no autorizados, teniendo en cuenta los siguientes aspectos:

a. Validar solicitudes de accesos especiales como USB y VPN, administrador de máquina y acceso remoto.

e. Los derechos de acceso de un usuario se deben revisar y reasignar, bien sea por cambio de cargo o traslado de área dentro de la misma Entidad, teniendo en cuenta:

- El nuevo jefe debe realizar los requerimientos de acceso a los sistemas de información que el colaborador requiera según las funciones que le sean asignadas en el área.

- Se asignan los permisos autorizados por el nuevo jefe y se eliminan los demás permisos y privilegios del cargo anterior.

### 9.6. Identificación de los usuarios

Todos los usuarios deben tener un identificador único (ID de usuario) para uso personal y se debe seleccionar una técnica de autenticación adecuada para garantizar la identidad del usuario. Este control se aplica a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de redes, proveedores, programadores de sistemas y administradores de bases de datos, etc.).

### 9.7. Normas para la creación de contraseñas

Los usuarios y contraseñas son de uso personal e intransferible, cualquier utilización indebida y/o irregularidad debe ser responsabilidad del colaborador. Como medida de seguridad los usuarios deben crear y administrar sus contraseñas siguiendo las siguientes normas para la creación y el uso:

a. Las contraseñas se consideran como información confidencial y deben ser protegidas como tal.

b. La contraseña debe tener al menos ocho (8) caracteres, donde se tengan letras en mayúscula, minúscula y números o caracteres especiales.

c. Las contraseñas deben cambiarse mínimo cada 60 días y no se pueden repetir las ultimas 10 contraseñas.

d. Si se digita más de 3 veces la contraseña de forma inválida la cuenta del usuario debe ser bloqueada. El desbloqueo se debe solicitar a través de un requerimiento desde Mesa de Ayuda.

e. La contraseña no debe incluir un nombre o palabra en algún lenguaje común (español, inglés, etc. evitando que estas sean vulnerables a los ataques de diccionarios.) u otra información pública como números de tarjeta de crédito, nombres de calles o números telefónicos. Una contraseña debe incluir información que solo sea conocida por el usuario.

f. No utilizar contraseñas por defecto, éstas se deben cambiar una vez se adquieran componentes tecnológicos nuevos o sistemas de información que las puedan incluir.

g. No es permitido compartir usuarios, contraseñas y cualquier mecanismo de autenticación asignado (ej. tokens).

h. Dispositivos como los tokens que permitan el acceso a un sistema de información en la entidad o entidades externas deben ser almacenados y salvaguardados en lugares seguros, donde solamente el dueño del token tenga acceso.

i. En los casos que se sospeche del compromiso de una contraseña en un posible incidente de seguridad esta debe ser cambiada inmediatamente por el administrador de la aplicación y debe reportarse la situación al Oficial de Seguridad de la Información.

j. Los usuarios no deben incluir las claves en ningún proceso de registro automatizado; por ejemplo, almacenado en una macro o sistema de información.

### 9.8. Segregación de funciones

La segregación de funciones en la UAECOB representa una actividad de control clave para separar las responsabilidades de las diversas actividades que intervienen en la ejecución de los procesos, una adecuada segregación de funciones permite mantener la confidencialidad, integridad y disponibilidad de la información.

a. La segregación de funciones permite reducir el riesgo de un mal uso accidental o deliberado del sistema, razón por la cual se deben definir lineamientos para evitar accesos no autorizados que permitan modificar o utilizar los activos sin autorización o detección.

b. La segregación de funciones en cada uno de los procesos de la entidad debe garantizar como mínimo la independencia de las siguientes actividades:

- Operación de equipos de cómputo
- Administración de red
- Administración de sistemas operativos
- Administración de bases de datos
- Administración de aplicaciones (administradores funcionales)
- Desarrollo de software
- Gestor de cambios
- Administración de seguridad informática

Teniendo en cuenta lo anterior, los líderes de cada proceso tienen la responsabilidad de generar las respectivas matrices de segregación de funciones las cuales deben ser validadas periódicamente.

### 9.9. REQUERIMIENTOS DE LA ENTIDAD PARA EL ACCESO LÓGICO

Las directivas, jefaturas o líderes de procesos deben definir los privilegios de los colaboradores a su cargo, siempre bajo los conceptos de menor privilegio y necesidad de saber. Es responsabilidad de la Oficina de Tecnología establecer procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios previamente definidos por los responsables del proceso. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación.

### 9.10. Control de acceso a las aplicaciones y recursos tecnológicos

a. Los accesos a las aplicaciones y recursos tecnológicos deben ser restringidos y monitoreados de acuerdo con las necesidades de la UAECOB.

b. El oficial de Seguridad de la Información debe definir y mantener los lineamientos para controlar el acceso de los colaboradores a las aplicaciones o recursos tecnológicos.

c. El oficial de Seguridad de la Información debe implementar mecanismos de monitoreo de accesos, control de privilegios con el fin de identificar posibles incumplimientos a las políticas de seguridad de la información.

d. La selección de los mecanismos de control de acceso a las aplicaciones se define de acuerdo con la criticidad y/o sensibilidad de la información (procesada, almacenada, usada) utilizada por el proceso.

e. Se deben utilizar medidas de seguridad para restringir el acceso a los aplicativos, bases de datos y en general a los recursos tecnológicos.

f. Las aplicaciones de la entidad deben contar con mecanismos para el manejo de contraseñas, los cuales sean interactivos y cumplan con los parámetros de seguridad definidos; para ello debe tener en cuenta:

- Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación.
- En los aplicativos y/o sistemas de información, tener en cuenta los lineamientos de contraseñas robustas.
- Los aplicativos deben obligar a los usuarios a cambiar las contraseñas temporales en su primer ingreso o registro.
- Mantener un registro de claves de usuario previas y evitar la reutilización.
- No mostrar las contraseñas en la pantalla en el momento de ingresarlas.
- Almacenar las contraseñas cifradas con algoritmos fuertes, mediante uso de funciones hash.
- Validar el nivel de seguridad de las contraseñas de acceso creadas por los colaboradores, permitiendo solamente el uso de contraseñas fuertes.
- Solicitar la modificación, en un periodo definido, de las contraseñas de ingreso a los aplicativos de la UAECOB.
- Implementar políticas de bloqueo automático del usuario cuando la contraseña se haya ingresado de manera errónea por tres veces, igualmente definir e implementar mecanismos que permitan su desbloqueo incluyendo: un tiempo de desbloqueo

automático de 15 minutos, asignación de nueva contraseña haciendo uso del sistema de control de acceso, entre otras alternativas.

### 9.11. Restricción del acceso a la información

a. El acceso de los usuarios a la información y las funciones del sistema de la aplicación debe limitarse de acuerdo con la política de control de acceso definida.

b. La extensión de la fecha de vencimiento de un contratista en lo posible debe evitarse. El bloqueo de las credenciales es automático en el sistema de gestión de cuentas de usuarios (Directorio Activo). De requerirse, por fuerza mayor, una extensión debe estar autorizada por el supervisor del contrato a través de un correo electrónico al líder de tecnología y con copia a Mesa de Ayuda.

c. Las restricciones para el acceso a las aplicaciones se deben basar en el rol que el usuario desempeñará, para ello se debe cumplir con los siguientes aspectos:

- Generar menús para controlar el acceso a las funciones del sistema de aplicación.
- Controlar los permisos de acceso de los usuarios: lectura, escritura, modificación y eliminación.
- Controlar y definir la interacción e intercambio de datos entre sistemas (internos y externos).
- Asegurar que las salidas de información de los sistemas, aplicaciones o plataformas que manejan información confidencial solo contengan la información requerida para el cumplimiento de las labores y solamente el personal autorizado tenga acceso a esta.

d. Restricciones de uso sobre los sistemas operativos.

e. Dentro de los aspectos para tener en cuenta por parte de los usuarios para un buen uso de los sistemas operativos están:

- El administrador de la plataforma es el responsable de otorgar los accesos a los recursos del sistema operativo.
- Las autorizaciones a las rutinas del sistema operativo no deben permitir modificaciones; en caso de requerirse, estas deben ser autorizadas y documentadas.

- El uso de herramientas o utilitarios propios de los sistemas operativos debe ser limitado a personal autorizado y su uso está restringido a casos específicos, asimismo, debe disponerse de la trazabilidad de las operaciones realizadas en los casos que son autorizados.

- Los administradores y operadores de plataformas no deben tener acceso a aplicaciones en producción, archivos y transacciones en línea.

- Está prohibido el uso de herramientas intrusivas con fines de vulnerar la seguridad del sistema operativo, bases de datos, redes etc.; solamente el oficial de seguridad de la información o quien este delegue podrá utilizarlas en la realización de pruebas de hacking ético.

- Las sesiones que no han presentado ningún tipo de actividad por un período de determinado deben finalizar automáticamente de acuerdo con la configuración definida; esto mismo aplica para los accesos remotos.

- Todos los colaboradores de la UAECOB deben cumplir con los lineamientos sobre contraseñas.

- Todas las estaciones de trabajo deben estar plenamente identificadas para garantizar la conexión de equipos confiables, esto debe venir acompañado de correctas configuraciones de red que restrinjan la conexión a los equipos de la granja de servidores (servidores de red) permitiendo solamente las conexiones necesarias.

- Se deben registrar los intentos exitosos y fallidos de autenticación del sistema.

### 9.12. Uso de las utilidades del sistema

El jefe de la Oficina de Tecnología debe implementar procedimientos para restringir y controlar el uso de los programas de utilidad que podrían ser capaces de vulnerar los controles del sistema y/o aplicación y mantener un inventario de estos. Se debe tener en cuenta, entre otros aspectos, los siguientes:

- Limitar el uso de los programas utilitarios a un número práctico mínimo de usuarios autorizados y confiables.
- Registro de todo uso de los programas de utilitarios.
- Definir y documentar los niveles de autorización de los programas de utilitarios.

### 9.13. Control de acceso a la red

El jefe de la Oficina de Tecnología debe implementar procedimientos para controlar el acceso a la red de la UAECOB, proporcionando a los funcionarios o colaboradores autorizados para su uso el acceso a los servicios. Se deben considerar, entre otros, los siguientes lineamientos:

a. La utilización de recursos de red debe ser limitada a usuarios autorizados.

b. Para acceder a las redes de datos de la UAECOB se requiere autenticación individual.

c. Las contraseñas de red de usuario y las contraseñas de usuarios privilegiados deben ser cambiadas periódicamente (mínimo una vez por mes).

d. Cuando se requiera realizar transferencia de información de la entidad, en especial la clasificada como publica confidencial o publica reservada, se deben utilizar mecanismos de cifrado o canales seguros.

e. La UAECOB permite a usuarios externos (proveedores o terceros) acceder a las redes institucionales desde redes externas bajo ciertas condiciones de seguridad. Dicha autorización debe ser tramitada por el líder del proceso ante la Oficina de Tecnología; en caso de ser aprobada, no se deben utilizar identificadores genéricos.

f. Los líderes de procesos que tienen acuerdos contractuales con proveedores o terceros que requieran acceso a los recursos tecnológicos de la entidad, se debe contar con autorización previa de parte de la Oficina de Tecnología. De igual manera se debe asegurar que los proveedores o terceros conozcan y acepten las políticas de seguridad de la información y que las normas o acuerdos específicos de seguridad que apliquen para la actividad contractual queden registrados en el documento de acuerdo contractual.

g. Los administradores de sistemas deben identificar y documentar los niveles máximos de servicio. Así mismo, se debe asegurar que el acceso y utilización de los recursos informáticos cumplan con los requerimientos de seguridad.

h. Se deben definir validaciones o revisiones teniendo en cuenta la criticidad de los proveedores o terceros ante el cumplimiento de la política de seguridad de la información, como los acuerdos específicos de seguridad para el desarrollo de las labores con los terceros. Este cumplimiento podrá ser validado por entes de control.

i. Cuando los usuarios accedan a datos en redes locales y remotas vía VPN, deben utilizar mecanismos de seguridad para autenticarse ante tales redes. Las solicitudes deben ser realizadas ante la Oficina de Tecnología, quienes deben realizar el trámite respectivo, para lo cual es requisito contar con usuario de red asignado y posteriormente se remite al jefe de la Oficina de Tecnología para asignar el acceso.

j. El jefe de la Oficina de Tecnología debe mantener las redes de datos internas segmentadas por VLANS (redes de área local virtuales), grupos de servicios, usuarios y sistemas de información.

k. Todas las estaciones de trabajo conectadas a la red de la UAECOB deben contar con herramientas de seguridad, como firewalls, HIDS (Host Intrusion Detection System o sistema de detección de intrusos), filtros de contenido, antivirus, Endpoint, entre otros.

l. El servicio de correo externo no debe ser habilitado para proveedores o terceros y temporales, salvo casos excepcionales por funcionalidad de un servicio.

### 9.14. CONEXIONES REMOTAS

Se define como acceso remoto cualquier conexión establecida desde fuera de la entidad que requiere acceso a la red o aplicaciones internas de la UAECOB por parte de funcionarios, proveedores entre otros.

Para dichos accesos se deben tener en cuenta las siguientes consideraciones:

a. Iniciar la conexión remota de red desde computadores y sitios seguros, evitar conexiones remotas desde computadores públicos o desconocidos como cafés internet, aeropuertos, hoteles o redes inalámbricas públicas.

b. Las conexiones remotas a los recursos de la plataforma tecnológica deben estar restringidas, únicamente se deben permitir estos accesos a personal autorizado y por periodos establecidos, de acuerdo con las labores desempeñadas.

c. La autenticación para los accesos remotos debe complementarse con doble factor de autenticación.

d. Si es el caso se debe aprobar o aceptar del lado de la entidad para que el proveedor tome el control remoto. No debe permitirse el acceso y control total de manera automática, sino cuando la UAECOB lo autorice y, en este caso, se deben monitorear las actividades realizadas por estos proveedores.

e. El trabajo remoto por VPN lo debe solicitar el superior o el supervisor del contrato, conforme con el procedimiento definido de solicitud de requerimientos. La Oficina de Tecnología gestiona dicha solicitud y otorga el privilegio, evaluando y aplicando las medidas de protección adecuadas que garanticen una conexión segura.

f. El acceso remoto a los servidores debe estar controlado por las políticas del Directorio Activo para el ingreso por este servicio, es decir, quién puede o no ingresar por este servicio, teniendo presente que el mismo debe ser autorizado únicamente para los administradores de los servidores; los usuarios o proveedores fuera de la oficina no deben tener estos accesos o llamado a este servicio.

g. Las aplicaciones críticas de la UAECOB deben forzar la autenticación mediante el protocolo HTTPS.

## 10. CONTROLES CRIPTOGRÁFICOS

### 10.1. La Oficina de Tecnología debe:

a. Determinar los algoritmos criptográficos y protocolos autorizados para su uso en la UAECOB y configurar los sistemas para permitir únicamente aquellos autorizados, teniendo en cuenta la información de los grupos de interés con el fin de descartar algoritmos de cifrado débil.

b. Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad.

c. La administración de llaves criptográficas y certificados digitales está a cargo de La Oficina de Tecnología; sin embargo, la administración de tokens bancarios, tokens para acceso al Sistema Integrado de Información Financiera (SIIF) y firmas digitales está a cargo de cada uno de los funcionarios o contratistas a quienes les fueron asignados para el desempeño de sus labores.

d. Los administradores de bases de datos de La Oficina de Tecnología deben establecer una estrategia para cifrar las bases de datos críticas de la UAECOB, velando por no afectar el desempeño del sistema de información.

e. La Oficina de Tecnología, donde aplique debe dar a conocer y capacitar a los funcionarios, contratistas, proveedores y terceros, cuando sea del caso, en el uso de las herramientas de uso criptográfico.

f. Realizar revisiones periódicas a las herramientas de uso criptográfico (tokens, firma digital, etc.), con el fin de detectar fallas o vulnerabilidades.

g. La Oficina de Tecnología debe notificar con anterioridad a los dueños de la información, aplicaciones y software que requieran de certificados digitales, la fecha de caducidad de estos para su renovación.

h. Realizar la entrega de los certificados digitales generados con el debido procedimiento para su aplicación y uso.

i. Realizar las configuraciones requeridas para el uso y administración de los certificados de firma digital.

j. Prestar soporte técnico para la configuración de los usuarios y soluciones adoptadas para controles criptográficos.

k. Velar por que la información clasificada y reservada (en reposo y transmisión) y donde aplique por el riesgo de exposición este siempre cifrada por los métodos que la UAECOB haya adoptado.

l. Comunicar al Comité Institucional de Gestión y Desempeño los eventos o incidentes que conlleven el incumplimiento de los objetivos institucionales por el no uso de controles criptográficos para la información clasificada y reservada.

m. Proporcionar los recursos necesarios para la administración y monitoreo en el uso de controles criptográficos a través de herramientas o softwares de seguridad.

n. Identificar e inventariar los puertos USB para quienes estén autorizados para la firma digital, con el fin de dar seguimiento al buen uso de la información.

**10.2. Los funcionarios y colaboradores de la UAECOB deben:**

a. Conocer y cumplir la política de uso de controles criptográficos.

b. A quienes les fueron asignados tokens bancarios y tokens de acceso a SIIF deben almacenarlos bajo llave cuando no hagan uso de estos, o cuando se van a retirar de sus puestos de trabajo.

c. Informar a los líderes de todos los procesos misionales (manejo, reducción y conocimiento) y de apoyo (gestión del talento humano, servicio a la ciudadanía, gestión

de recursos), las desviaciones que se presenten por el no uso de los controles criptográficos para la información clasificada y reservada.

d. Administrar los riesgos que se presenten por el no uso de controles criptográficos para la protección de la información clasificada y reservada.

e. Mantener bajo custodia la clave, llave o token, que le ha sido suministrada desde la Oficina de Tecnología.

f. Responder por el manejo de la información clasificada y reservada para que esté protegida con las medidas de seguridad necesarias.

g. En caso de pérdida o daño de un token, comunicar este incidente a la Oficina de Tecnología a través de la Mesa de Ayuda para su respectiva reposición; se debe proceder de igual forma si la clave secreta o llave de cifrado ha sido vulnerada.

h. Devolver a la Oficina de Tecnología, el token y las llaves de cifrado en caso de situaciones administrativas que lo desvinculen laboral o temporalmente como vacaciones, licencias, permisos, etc. Esta verificación se debe dar a través del Paz y Salvo de entrega del cargo aceptado por la Oficina de Tecnología.

### 10.3. Firma digital

El uso de firma digital es seguro por el hecho de usar mecanismos y algoritmos de cifrado bastantes robustos. Sin embargo, la seguridad puede ser comprometida si el funcionario que hace uso de la firma digital no toma las medidas necesarias para proteger la clave, llave o token que le ha sido asignado para su uso.

a. Los funcionarios autorizados para hacer uso de la firma digital son: jefes de oficina, coordinadores de grupo o directivos.

b. La firma digital se utilizará para cumplir con las normativas legales, para identificar al firmante de manera inequívoca, para certificar la integridad del documento o cuando se requiera proteger un documento o la información (autenticidad e integridad) con un riesgo asociado resultado de una evaluación de riesgos.

c. Para el uso de firma digital dentro de la UAECOB se ha establecido que deben ser individuales, es decir, cada funcionario que esté autorizado para el uso de la firma digital es responsable único de la firma del documento.

d. La firma digital individual se da mediante un token personalizado, con estampado

cronológico e incorporando la identificación de las características de identificación (la fecha y hora de la firma, el correo y la dirección IP del firmante) del creador del documento.

e. Por ser una firma individual, la UAECOB debe adquirir los tokens que se requieran para el uso de la firma digital y su asignación a cada funcionario que adopte esta responsabilidad.

f. La firma digital debe ser verificada a través de una llave pública incluida en un certificado válido emitido por una entidad certificadora, a la cual se le debe exigir acuerdos de niveles de respuesta para el servicio de certificación o verificación.

g. Se debe realizar mantenimiento anual a todas las firmas digitales, así como las API (interfaz de programación de aplicaciones) correspondientes.

h. Una vez firmados los documentos con la firma digital deben conservarse en su estado electrónico para garantizar su validez.

i. Una vez firmados digitalmente los documentos se deben convertir en formato PDF y deben visualizarse a través del sistema de Gestión Documental.

j. Los certificados digitales, firmas digitales, llaves de cifrado de la información, token criptográfico (físico o lógico) son de uso personal e intransferible.

k. Si el documento que se firma tiene información clasificada o información reservada, es importante conocer que la firma digital no da privacidad a la información, por lo que su tratamiento requiere de otro control criptográfico, como podría ser una herramienta de cifrado de información para su transporte o almacenamiento.

l. Los funcionarios autorizados para el uso de firma digital en la UAECOB, antes de firmar un documento que tiene otras firmas digitales, deben asegurarse de que estas firmas previas no han sido alteradas.

m. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:

- Es única a la persona que la usa.
- Es susceptible de ser verificada.
- Está bajo el control exclusivo de la persona que la usa.
- Está ligada a la información o mensaje de datos de tal manera que si estos son

cambiados la firma digital es invalidada.
- Está conforme con las reglamentaciones adoptadas por el Gobierno nacional.

El uso de firma digital, según la Ley 527 de 1999, posee tres atributos fundamentales en el aseguramiento jurídico, por lo que es necesario que los funcionarios autorizados para su uso velen por que estos atributos se cumplan en su implementación.

a. **Autenticidad:** Es la medida que permite verificar en un mensaje de datos firmado digitalmente que quién es su autor, es quién se compromete jurídicamente.

b. **Integridad:** El destinario de ese mensaje de datos podrá verificar si la información ha sido o no alterada en el proceso de comunicación electrónica, lo que es muy útil para determinar la originalidad electrónica del mensaje de datos, especialmente a la luz de los artículos 8 y 9 de la Ley 527 de 1999.

c. **No repudio:** Quien firma digitalmente se compromete con la suscripción respectiva y posteriormente no le es dado retractarse o refutar dicho acto.

### 10.4. Firma electrónica

Todos los funcionarios y contratistas que desde el directorio activo se autentiquen a un sistema de información de la UAECOB pueden hacer uso de la firma electrónica, enviando el contenido del mensaje a través de un medio electrónico válido, por ejemplo, una solicitud a través del formato de acceso lógico y físico. Para el envío de información externa, será con base en su clasificación y será autorizada por el dueño del proceso.

En la UAECOB se contempla la firma electrónica bajo las siguientes circunstancias:

- Permitir la identificación de quien firma con el fin de determinar que la persona es quien dice ser.
- La firma electrónica solo puede ser generada por el emisor del documento.
- La firma electrónica podrá ser validada (que consiste en mostrar certificado del firmante para verificar los datos de la firma digital que asocian la identidad de una persona o entidad), pero no falsificada.
- La firma electrónica está creada de un modo que solo está bajo el control de quien firma.
- La firma electrónica está vinculada a los datos de tal forma que si los datos son alterados la firma dejará de ser válida.
- La firma electrónica debe servir para indicar que el contenido cuenta con su aprobación.

- Debe ser confiable y apropiada para el propósito por el cual el mensaje fue generado o comunicado.

### 10.5. Cifrado de la información

La UAECOB debe contar con controles que permitan definir y administrar los mecanismos de cifrado de información que permitan el intercambio de información cifrada, para minimizar los riesgos en este proceso de intercambio o transporte de la información y brindar seguridad, confianza y, además:

a. Se debe hacer uso de cifrado para la protección de claves de acceso, llaves criptográficas a datos, información clasificada y reservada, y todos aquellos servicios que estén expuestos a internet.

b. Cifrado en la transmisión de información clasificada y reservada por los diferentes canales de comunicación que se utilicen en la entidad.

c. Cifrado en el resguardo de información clasificada y reservada en cualquier medio físico o componente tecnológico, o cuando así surja de la evaluación de riesgos realizada por el dueño de la información y el oficial de seguridad de la información.

### 10.6. Llaves criptográficas

Con el fin de garantizar la confidencialidad e integridad de los datos o la información de un documento, la UAECOB debe garantizar la protección de la información tanto en reposo como en tránsito, para lo cual ha adoptado el uso de algoritmos de seguridad que cumplan con la reglamentación legal, la protección y privacidad de la información.

Por tanto, es importante, además de la información, proteger las claves secretas o llaves criptográficas para que no sean vulneradas ni modificadas sin autorización. Por consiguiente, la Oficina de Tecnología debe velar por la custodia de estas y todo su ciclo de vida, que se relaciona a continuación:

a. **Generación:** Es la selección del valor que se va a utilizar para ser usado por un algoritmo criptográfico específico o aleatorio. La llave debe ser elegida de tal manera que no sea previsible y que en el proceso no se presente un acceso no autorizado.

b. **Distribución:** Es el proceso de traslado de una llave desde el punto de su generación hasta el punto donde va a ser usada, siendo la mayor exigencia en los algoritmos simétricos. En la UAECOB, se exige el uso de cifrado para las llaves.

c. **Instalación:** Es el proceso de almacenamiento de la llave en el dispositivo o proceso que se va a usar y debe mantener en todo momento la protección para evitar el acceso no autorizado. En la UAECOB se exige el uso de cifrado para las llaves.

d. **Almacenamiento:** Las llaves solo pueden ser almacenadas en forma cifrada, con el fin de evitar su manipulación o intento de acceso no autorizado.

e. **Cambio:** Establece la vigencia de una llave, a mayor tiempo de vigencia de una llave mayor será la probabilidad de acceso no autorizado. El periodo se define en cada caso particular dependiendo del nivel de riesgo identificado en el activo de información.

f. **Eliminación:** Las llaves deben ser eliminadas para evitar su divulgación, esto aplica para los valores de las llaves que en algún momento puedan encontrarse en forma clara o sin cifrado en algún medio de almacenamiento.

g. **Protección:** Se deben usar mecanismos que protejan las llaves de accesos y modificaciones no autorizadas.

h. **Revocación:** Hace referencia a la invalidez de una llave antes de cumplir el periodo de vigencia establecido y el responsable de esta acción es el funcionario al que le fue asignada la llave correspondiente.

Las razones por las cuales un funcionario debe solicitar a la Oficina de Tecnología la revocación de una llave, clave secreta o token bajo su responsabilidad son las siguientes:

- Pérdida del dispositivo en el cual se encuentra almacenada la llave.
- Se evidencia alguna circunstancia en la cual se ha dado acceso no autorizado a la llave, clave secreta o token.
- Reporte de ataques informáticos o acción de algún tipo de programa maligno.
- Cuando el funcionario responsable de la gestión de la llave termina su relación laboral o contractual con la entidad.

### 10.7. Certificados digitales

Los responsables de los sistemas de información deben ser conscientes en el uso y caducidad que pueda tener un certificado digital, esto, con el fin de comunicar a la Oficina de Tecnología para la emisión e implementación de los mismos.

El responsable de la solicitud ante la entidad certificadora para la emisión de los certificados también debe velar por la no caducidad de estos, teniendo como control un listado de todos los certificados emitidos con la fecha de caducidad y la asignación de estos en los sistemas de información. En la UAECOB, se establece el uso de certificados digitales para:

a. Garantizar la autenticidad del sitio, servicio o aplicativo web.

b. Evitar el riesgo de ataques de suplantación de identidad o phishing de los sitios Web.

c. Proteger la confidencialidad de la información intercambiada entre la entidad y sus ciudadanos a través del sitio web.

d. Establecer conexiones seguras cifrando la información intercambiada entre los aplicativos y los ciudadanos.

e. Mantener la integridad de la información intercambiada, porque el certificado presenta las características de la entidad, algoritmo de cifrado, fecha de emisión del certificado, etc.

## 11. SEGURIDAD FÍSICA Y DEL ENTORNO

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales. Toda área donde se soliciten o capturen datos personales debe contar con anuncio al público de dicha actividad, a su vez esta información debe ser conservada de acuerdo con la Ley 1581 de 2012 de Protección de Datos Personales.

### 11.1.1. Áreas seguras

La UAECOB cuenta con una recepción donde se controla el ingreso y salida de terceros, y el ingreso y salida de elementos, tanto de funcionarios como de terceros. La UAECOB exige a los proveedores que gestionen o procesen información por fuera de las instalaciones de la UAECOB cumplir con las políticas de seguridad de Unidad y las que disponga el proveedor en sus instalaciones.

El datacenter o centros de cableado deben contar con mecanismos que cumplan los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los

fabricantes de los servidores y equipos de comunicaciones que alberga, igualmente debe contar con sistemas mecánicos para control de incendios, impedir el acceso a personal no autorizado, consumo de alimentos, bebidas o cigarrillos tradicionales o electrónicos.

La UAECOB cuenta con un sistema de seguridad CCTV (Circuito Cerrado de Televisión) para otorgar la mayor seguridad posible tanto a los ciudadanos como a los funcionarios que ingresan a sus instalaciones. El sistema de seguridad CCTV opera bajo las siguientes directrices:

a. La Oficina de Tecnologías es la responsable del mantenimiento y soporte de la plataforma tecnológica que soporta el sistema CCTV.

b. La Oficina de Tecnologías debe garantizar el funcionamiento del sistema CCTV las 24 horas del día de los 365 días del año. La Oficina de Servicios Administrativos garantizará la operación y monitoreo.

c. El acceso al centro de monitoreo es de carácter restringido. Las únicas personas que tienen permiso de acceder son los operadores o aquellos funcionarios que autorice la Oficina de Servicios Administrativos.

d. El operador de medios tecnológicos del CCTV debe registrar en la bitácora diaria cualquier evento ocurrido durante su turno.

e. El operador de medios tecnológicos del CCTV debe notificar vía telefónica o electrónica a la Oficina de Tecnología acerca de las fallas o ausencias de video que se presenten en las cámaras del sistema CCTV de la UAECOB. Lo anterior con el fin de restablecer dicho servicio y mantener su correcto funcionamiento.

f. Cuando el operador de medios tecnológicos del CCTV detecte anomalías o incidentes en las zonas de monitoreo las debe reportar inmediatamente al supervisor de contrato de vigilancia y seguridad privada.

g. Toda solicitud de copias de video debe hacerse por escrito a la Oficina de Servicios Administrativos.

h. Todas las grabaciones tienen una duración mínima de 30 días y después se reescriben.

i. Está prohibido dar información de especificaciones técnicas y ubicaciones de cámaras.

j. Toda copia de video generada debe ser entregada mediante oficio o mediante cadena de custodia.

k. La Oficina de Tecnologías e Información debe brindar un repositorio para el almacenamiento de videos históricos garantizado la confidencialidad y disponibilidad de esta información.

### 11.1.2. Ubicación y protección de los equipos

El datacenter está ubicado de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado por la Oficina de Tecnología.

Se hace seguimiento a las condiciones de temperatura, humedad, voltaje, apertura y cierre de puertas que pueden llegar a afectar adversamente al datacenter.

### 11.1.3. Servicios de suministro

La UAECOB cuenta con aire acondicionado de contingencia, UPS (sistema de alimentación ininterrumpida, en inglés [Uninterruptible Power Supply]) que asegura el tiempo necesario de autonomía para que la planta eléctrica entre a soportar la carga o mientras regresa la energía eléctrica, ante una falla en el suministro de energía. También cuenta con un enlace de red redundante y un sistema de monitoreo de las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) del datacenter.

### 11.1.4. Seguridad del cableado

El datacenter de la UAECOB cumple con la normatividad de cableado estructurado y está debidamente certificado. Así mismo la UAECOB debe exigir a los proveedores de servicios informáticos cumplir con las políticas de seguridad de la Unidad.

### 11.1.5. Mantenimiento de equipos

La Oficina de Tecnología debe establecer y ejecutar planes anuales de mantenimiento de la infraestructura tecnológica de la UAECOB.

### 11.1.6. Seguridad de equipos y activos fuera de las instalaciones

a. Los equipos y medios removibles que son retirados de las instalaciones de la UAECOB deben estar debidamente cifrados.

b. Los funcionarios y contratistas que retiren equipos o medios removibles de las instalaciones de la UAECOB deben seguir las siguientes directrices:

- En ninguna circunstancia los equipos de cómputo pueden ser desatendidos o separados en la órbita de custodia en lugares públicos, o a la vista en caso que esté siendo transportado en un vehículo.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos (como rayos X de escáner similares a los de aeropuerto).

- En caso de pérdida o hurto de un equipo de la UAECOB, se debe interponer la denuncia ante la autoridad competente e informar inmediatamente al jefe de grupo y al grupo de servicios administrativos para que se inicie el trámite interno correspondiente.

### 11.1.7. Disposición segura o reutilización de equipos

Cuando una estación de trabajo o equipo portátil vaya a ser reasignado o dado de baja se debe realizar una copia de respaldo de la información de la UAECOB que allí se encuentre almacenada (en caso de ser necesario). Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobreescritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.

### 11.1.8. Política de equipo desatendido, escritorio limpio y pantalla limpia

Todos los colaboradores de la UAECOB deben conservar su escritorio libre de información propiedad de la entidad que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento. Cada vez que se vayan a retirar de sus puestos de trabajo se deben contemplar los siguientes lineamientos:

a. Al imprimir documentos de carácter confidencial (información pública clasificada e información pública reservada), estos deben ser enviados y retirados de la impresora inmediatamente.

b. Los computadores deben cargar por defecto el fondo de pantalla de la UAECOB el cual no debe ser modificado y debe permanecer activo.

c. Los funcionarios y contratistas de la UAECOB deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo (aplicando el comando de bloqueo oprimiendo simultáneamente las teclas Windows + L), a su vez, la Oficina de Tecnología debe implementar mecanismos para cierres de sesión

automáticos no superior a cinco minutos.

d. Los usuarios son responsables y asumen las consecuencias por la pérdida de información que esté bajo su custodia. Se prohíbe el almacenamiento de información personal en los computadores de la UAECOB. El escritorio lógico (del computador) debe estar libre de información pública clasificada e información pública reservada.

e. La información de gestión del área debe ser almacenada por los usuarios en carpetas compartidas del área y la información de gestión del usuario en el almacenamiento virtual de One Drive corporativo de Office 365.

## 12. SEGURIDAD DE LAS OPERACIONES

### 12.1. Documentación de procedimientos operativos

Se debe contar con procedimientos documentados de trabajo debidamente documentados para las actividades operativas asociadas con las instalaciones de procesamiento y comunicación.

### 12.2. Control de cambios

Los cambios en los procesos de la entidad, en las instalaciones y en los sistemas de procesamiento de información se deben realizar de acuerdo con los lineamientos del Procedimiento de Gestión de Cambios Tecnológicos.

### 12.3. Gestión de capacidad

La UAECOB debe gestionar la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones del Procedimiento de Gestión de Capacidad.

### 12.4. Separación de los ambientes

La UAECOB debe contar con ambientes de desarrollo, pruebas y producción separados por máquinas físicas y virtuales.

La UAECOB debe controlar el acceso al ambiente de pruebas de la misma forma que controla el acceso al ambiente de producción. Un ambiente de prueba es un término utilizado en el campo del software y desarrollo de sitios web previo a la producción (es el espacio donde operará el sistema o aplicación, es decir, es donde se hace uso del servicio por parte de los usuarios finales).

### 12.5. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

a. Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de la UAECOB contra códigos maliciosos.

b. Los contratistas que hagan uso de sus equipos portátiles personales en lo posible deben contar con un software antivirus licenciado.

c. El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.

d. El único servicio de antivirus autorizado en la UAECOB es el asignado directamente por la Oficina de Tecnología, el cual cumple con todos los requisitos técnicos y de seguridad. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

e. El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.

f. El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.

g. Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus y que han sido establecidos por la Oficina de Tecnología.

h. El programa de antivirus debe ser instalado única y exclusivamente por la Oficina de Tecnología en los servidores y estaciones de trabajo.

### 12.6. COPIAS DE RESPALDO

La UAECOB debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello, la Oficina de Tecnología define el Procedimiento de Copias de Respaldo e Instructivo, que describe las actividades para la estrategia de backup requeridas; además:

a. La Oficina de Tecnología debe establecer las políticas de copias de seguridad desde la herramienta de backups para los sistemas de información y bases de datos.

b. Todos los administradores de base de datos, aplicaciones y servicios deben cumplir con las políticas de backup establecidas por la Oficina de Tecnología.

c. La Oficina de Tecnología debe realizar copias de respaldo a las carpetas compartidas

definidas en el servidor de archivos de la UAECOB.

d. Todas las copias de respaldo deben ser almacenadas en un área adecuada, con control de acceso y donde se apliquen los controles para la protección de los medios de respaldo.

e. Todas las copias de respaldo deben contemplar un plan de continuidad de la entidad, destinando un sitio secundario para su preservación orientado a evitar la pérdida de la información.

f. Las copias de respaldo deben ser guardadas únicamente con el objetivo de restaurar el sistema cuando sea necesario recuperar la información por situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o computadores o por requerimientos legales.

g. Toda la información institucional que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la entidad, motivo por el cual no debe ser divulgada a terceros, salvo autorización expresa de la UAECOB.

### 12.7. REGISTRO Y SUPERVISIÓN DE EVENTOS

#### 12.7.1. Registro de eventos

Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones de la UAECOB deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

#### 12.7.2. Protección de la información de registro

La Oficina de Tecnología, con el fin de proteger la información de registro de modificación no autorizada por parte de usuarios no autorizados, administradores u operadores de los sistemas de información, debe implementar mecanismos de copiado de logs en «tiempo real» a un sistema por fuera del control de administradores y operadores de los sistemas.

#### 12.7.3. Sincronización de relojes

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por la

UAECOB deben estar sincronizados utilizando como referencia la hora oficial de Colombia de Instituto Nacional de Metrología que está disponible en el sitio web horalegal.inm.gov.co

## 12.8. CONTROL DE SOFTWARE OPERACIONAL

### 12.8.1. Instalación de software en sistemas operativos

El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de la Mesa de Ayuda de la Oficina de Tecnología. Por lo tanto, a los funcionarios o contratistas no le es permitido realizar esta labor.

Para la instalación de software se deben seguir las siguientes directrices:

- El software licenciado debe contar con su respectiva documentación (licencia) y, en el caso del software libre, debe estar permitido el uso comercial.
- El instalador debe ser descargado de la página oficial del fabricante.
- Debe dejarse evidencia documentada de que las directrices anteriores fueron seguidas a cabalidad.

Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de las nuevas adquisiciones de software o mejoras al software existente antes de su puesta en producción.

Todo el software nuevo y mejorado debe estar completamente soportado por una documentación suficientemente amplia y actualizada y no debe ser puesto en el ambiente de producción sin contar con la debida documentación.

- **Documento de licencia del software:** representa el permiso que le da el fabricante para la instalación y uso de su producto.

- **Manual de instalación del software**: para determinar que el software ha sido instalado apropiadamente.

- **Manual del usuario para uso del software:** para guiar al usuario en su uso y apropiación.

La Oficina de Tecnología debe realizar revisiones periódicas del uso del software instalado en las estaciones de trabajo y servidores de la entidad, con el fin de validar el cumplimiento de la Ley 603 de 2000 "*Por la cual se modifica el artículo 47 de la Ley 222 de 1995*" y

Ley 23 de 1982 sobre los Derechos de Autor, y conjuntamente debe identificar los activos de información que se encuentran afectados por derechos de propiedad intelectual.

Todo software que viole los acuerdos de licenciamiento debe ser desinstalado inmediatamente y debe ser reportado el hecho como incidente de seguridad por incumplimiento de la política, de los términos y condiciones de uso, poniendo en riesgo la seguridad de la información y quizás generando sanciones económicas por incumplimiento a la Ley 603 de 2000 de derechos de autor.

Para contar con una trazabilidad del software instalado en los componentes tecnológicos de la UAECOB (sistemas operativos, programas ofimáticos, sistemas de información, entre otros) se debe contar con un sistema de control de la configuración, en donde se observen los cambios ejecutados en dicho software, como instalación de parches, cambios de versionamiento (control de versiones), actualizaciones, etc., con el fin de mantener el historial y el control del software operacional en la UAECOB.

La Oficina de Tecnología debe comunicar a los funcionarios y contratistas sobre las consecuencias por el uso ilegal de software, y conjuntamente con la Oficina Asesora Jurídica deben definir y establecer las cláusulas de los contratos para cumplir con la legislación vigente relacionada con los derechos de autor y datos personales.

El software que desde Fábricas de Software o proveedores de desarrollo de software se contemple y, los desarrollos Inhouse o realizados por funcionarios o contratistas directos de la UAECOB deben anexar un certificado de uso y cesión de derechos según sea el caso, cuando de adquisición se trate.

Es importante que la Oficina Asesora Jurídica haga parte de esta adquisición en cuanto a la comprensión que se haga lectura del documento de la licencia, derechos de autor y propiedad intelectual del software adquirido y que será propiedad de la UAECOB, cuando de desarrollos de Fábrica de Software y Desarrollos Inhouse se trate.

### 12.9. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

La Oficina de Tecnología es responsable de verificar de manera periódica la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la entidad. Adicionalmente, debe contar con un procedimiento y un análisis de vulnerabilidades que permitan la identificación y mitigación de las vulnerabilidades identificadas en toda la plataforma tecnológica de la UAECOB.

### 12.9.1. Gestión de las vulnerabilidades técnicas

a. Se debe generar y ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y/o hacking ético para las plataformas críticas de la entidad cuya viabilidad técnica y administrativa lo permitan.

b. Una vez se lleve a cabo la ejecución de escaneos de vulnerabilidad en la plataforma tecnológica de la entidad, las vulnerabilidades o hallazgos identificados se deben remediar de acuerdo con los lineamientos establecidos por los Procedimientos de Gestión de Vulnerabilidades.

c. Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de la Oficina de Tecnología; para estas remediaciones se debe tener en cuenta las directrices establecidas en el Procedimiento de Gestión de Cambios cuando su aplicación se lleve al ambiente de producción.

## 12.10. AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

### 12.10.1. Controles sobre auditorias de sistemas de información

Para la ejecución de auditorías a los sistemas de información se deben tener en cuenta las siguientes consideraciones:

a. Los requisitos de auditoría para acceso a sistemas y a datos se deberían acordar con los jefes de las Dependencias involucradas.

b. El alcance de las pruebas técnicas de auditoría se debería acordar y controlar.

c. Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistema se deben realizar en horario no laboral en un ambiente controlado.

d. Se debe hacer seguimiento de todos los accesos y logs (registro de eventos en los sistemas) para producir un rastro de referencia.

e. Las pruebas de auditoría se deben limitar a acceso a software y datos únicamente para lectura.

## 13. SEGURIDAD EN LAS COMUNICACIONES

La Oficina de Tecnología debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de la información en las redes definidas en la entidad, la disponibilidad de los servicios en red y la seguridad en sí de la información.

### 13.1.1. Gestión de la seguridad en las redes

La Oficina de Tecnología debe definir e implementar mecanismos de separación de las redes de la UAECOB con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de computador de escritorio y dominio de servidor), por dependencias (Oficina de Talento Humano, Oficina de Servicios Administrativos, Oficina de Gestión Financiera y Oficina de Tecnología e Información) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples dependencias) y, además:

a. La Oficina de Tecnología debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de alguna de las dos redes.

b. El acceso remoto a las redes de la UAECOB se controla mediante conexiones VPN, las cuales deben estar monitoreadas para evidenciar la desactivación de estas en el tiempo que se ha definido.

### 13.1.2. Transferencia de información

La UAECOB debe firmar acuerdos o compromisos de confidencialidad con los servidores públicos y debe incluir una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información clasificada o información reservada. En este acuerdo deben quedar especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se debe firmar antes de permitir el acceso o uso de dicha información.

Todos los lineamientos para la transferencia de información deben aplicarse en toda la entidad, proveedores y terceros que dentro de sus funciones se establezca la necesidad de intercambio de información física y/o digital.

## 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La Oficina de Tecnología debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en la UAECOB. Las dependencias que contraten el desarrollo de software o los adquieran de terceros deben apoyarse en la Oficina de

Tecnología para definir los requisitos de seguridad de la información. Para ello, debe tener en cuenta los lineamientos establecidos en el Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de información y, además, los siguientes:

### 14.1.1. Requisitos de seguridad de los sistemas de información.

a. El nivel de confianza requerido con relación a la identificación declarada de los usuarios para obtener los requisitos de autenticación de usuario. Por ejemplo, la implementación de segundos factores de autenticación y un sistema de gestión de contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar su reutilización.

b. Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datos de acceso por correo electrónico.

c. Las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad e integridad. Por ejemplo, cifrado de información almacenada y el envío de información por canales cifrados.

d. Los requisitos obtenidos de los procesos de la entidad, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación mediante HTTPS (Protocolo seguro de transferencia de hipertexto es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.), cifrado de contraseñas almacenadas y uso de firmas digitales.

e. Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.

f. La necesidad de exigir la implementación de metodologías de desarrollo seguro.

### 14.1.2. Seguridad en los procesos de desarrollo y soporte

La Oficina de Tecnología debe definir e implementar principios de desarrollo seguro en actividades de construcción de sistemas de información internos.

Los principios de desarrollo establecidos se deben revisar con regularidad (al menos anualmente) para asegurar que están contribuyendo a mejorar los estándares de seguridad dentro del proceso de construcción; también se deben revisar regularmente para que

permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Los lineamientos para el desarrollo seguro deben aplicarse también para los sistemas de información existentes en la UAECOB y a los de uso externo con los proveedores (Fábrica de desarrollo), teniendo en cuenta el Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información y, además, lo siguiente:

a. La UAECOB (Oficina de Tecnología y supervisor del contrato) debe velar por el desarrollo interno y externo de los sistemas de información, para que cumplan con los requisitos de seguridad esperados, así como con pruebas de aceptación y seguridad al software desarrollado. Además, la UAECOB debe asegurar que todo software desarrollado o adquirido, interna o externamente, cuenta con el nivel de soporte requerido por la entidad.

b. Los cambios en sistemas deben realizarse de acuerdo con el Procedimiento de Gestión de Cambios.

c. En todo desarrollo interno, externo y/o a través de la Fábrica de Desarrollo, se debe hacer uso de metodologías de desarrollo seguro que contemplen lineamientos de seguridad en todas las etapas del desarrollo.

### 14.1.3. Ambiente de desarrollo seguro

a. La Oficina de tecnología debe aplicar los mismos controles en al ambiente de producción y ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).

b. La Oficina de Tecnología debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas, de acuerdo con el Procedimiento de Cambios Tecnológicos.

c. La Oficina de Tecnología debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la UAECOB.

### 14.1.4. Desarrollo contratado externamente

Cuando se contrata un desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por la UAECOB. Adicionalmente, se debe acordar la entrega de manuales técnicos que describan la estructura interna del sistema, así como el diccionario de datos, librerías ejecutables, modelo entidad relación de la base de datos, manuales

funcionales, manual del usuario y manual de instalación y, además, se debe cumplir con lo siguiente:

a. Las dependencias deben asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

b. Las dependencias deben exigir el suministro de evidencia sobre la realización de pruebas de seguridad al software desarrollado por terceros.

c. Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.

d. Las dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

e. Las dependencias deben incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.

f. Las dependencias deben incluir en los acuerdos contractuales, en donde sea posible, el derecho de la UAECOB a realizar auditorías durante el desarrollo del contrato.

#### 14.1.5. Pruebas de seguridad de sistemas

Se debe exigir tanto para desarrollos internos como externos la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

#### 14.1.6. Pruebas de aceptación de sistemas

Independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable), en estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido las brechas de seguridad. Además, se debe acreditar lo siguiente:

a. Se deben realizar pruebas de aceptación del software por parte de una persona diferente de quien lo ha desarrollado; estas pruebas deben reposar en un documento,

certificar que el software desarrollado cumple con los lineamientos y funcionalidades para su uso y estar firmadas por quienes las realizaron. Para mayor detalle se debe dirigir al Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

b. De ser posible, las pruebas se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente productivo de la UAECOB, y que las pruebas son confiables.

c. En donde la funcionalidad de la seguridad no satisface el requisito especificado por la Oficina de Tecnología, antes de comprar el software se debe reconsiderar el riesgo introducido y los controles asociados.

#### 14.1.7. Datos de prueba

La Oficina de Tecnología debe establecer que la información entregada a los desarrolladores (tanto internos como externos) para sus pruebas debe ser enmascarada y los datos sensibles deben ser eliminados una vez culminada las pruebas con el fin de no revelar información confidencial de los ambientes de producción, dando cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales), Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública) y la Ley 1437 de 2011.

## 15. RELACIÓN CON LOS PROVEEDORES

### 15.1.1. Seguridad de la información en las relaciones con los proveedores.

La UAECOB debe establecer mecanismos de verificación de lineamientos de seguridad en sus relaciones con todos los proveedores, especialmente aquellos proveedores críticos para la Unidad por el manejo de información clasificada o reservada, con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que cumplan con las políticas de seguridad de la información. Es fundamental que se lleven a cabo visitas a los proveedores con el fin de identificar situaciones que puedan comprometer la información de la UAECOB por el no cumplimiento de los lineamientos establecidos en este manual. Para estas visitas se ha establecido el Procedimiento de Gestión de Proveedores.

### 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores.

a. Los supervisores de contratos deben asegurar que se comuniquen las políticas y procedimientos de seguridad de la información a los proveedores y/o contratistas.

b. El Grupo de Contratación debe incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información**:**

- Cláusula de confidencialidad.
- Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).
- Cumplimiento de las políticas de seguridad de la información de la UAECOB.
- Reporte de eventos de seguridad de la información a través de los canales definidos en el Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Etiquetado y manejo de la información de acuerdo con las directrices del procedimiento de gestión de activos.
- Cláusula de seguimiento y revisión de los servicios de los proveedores o terceros para asegurar que los términos y condiciones de seguridad de la información de los acuerdos contractuales se cumplan.

c. Los supervisores de contratos deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos y monitoreando la aparición de nuevos riesgos.

d. Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la Oficina de Tecnología utilizando el formato Acceso Lógico y Físico.

## 16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad debe estar armonizada con los lineamientos del Procedimiento de Gestión de Incidentes, donde se debe establecer, como mínimo, quiénes deben reportar, los canales de comunicación, tipo de situaciones que se deben reportar, decisiones sobre las situaciones reportadas, respuesta a incidentes, aprendizaje de estos y recolección de evidencias digitales.

Es deber de todo funcionario, contratista o colaborador informar el incumplimiento de los lineamientos descritos en este manual.

Cualquier incumplimiento identificado debe remitirse al Oficial de Seguridad de la información, quien debe determinar si el evento se considera como incidente de seguridad de la información, teniendo en cuenta las categorías y criterios de clasificación.

**Categorías de incidentes de seguridad de la información:** Se debe considerar como incidente de seguridad de la información:

a. **Fuga de información:** Se evidencia divulgación no autorizada de información de la UAECOB.

b. **Acceso no autorizado:**

- Se evidencia que una persona ingresa a un sistema de información sin credenciales de acceso.
- Se evidencia que una persona (interna o externa) tiene credenciales de acceso asignadas a otro usuario.
- Personal no autorizado ingresa a las instalaciones de la UAECOB.

c. **Ataque:**

- Se evidencia intención de afectar un recurso específico.
- Se modifica la imagen institucional en aplicaciones de la UAECOB.
- No se cuenta con la disponibilidad de un sistema de información por ataques de denegación de servicio.
- Se evidencia caso de suplantación ya sea en correo electrónico o en sitios web.

d. **Código dañino:**

- El daño (modificación o indisponibilidad de la información) se manifiesta en memorias USB que alteran la información.

- El daño (modificación o indisponibilidad de la información) se manifiesta en un equipo y el vector de propagación fue por medio de USB contaminada o correo malicioso.

e. **Denegación de servicio:**

- El sistema de información no responde por alta cantidad de peticiones.
- El sistema de información se encuentra con latencia o degradación del servicio.

f. **Hurto o pérdida:**

- Se presenta hurto o pérdida de equipos portátiles, cargadores, periféricos de entrada y salida.

- Se presenta hurto o pérdida de elementos personales en las instalaciones de la UAECOB.

**Alarmas de sistemas de monitoreo:** Estos incidentes son reportados por dispositivos de seguridad según las reglas implementadas.

g. **Usos inadecuados:**

- Si se ingresa texto copiado de internet en documentación oficial de la UAECOB, a no ser que el texto es libre de derechos de autor, o sin registrar la fuente o registrarla de manera errónea. Existe una forma muy fácil de determinar si el texto es plagio, la cual es: se toma una frase del texto, se copia y se pega en el buscador de Google, pero entre comillas. Esto hace que el sistema busque dicha frase exacta y literal en Internet. Si aparecen textos con esa frase exacta, podrá determinar el plagio. De igual manera existen herramientas libres que permiten identificar plagio.

- Si se publican comunicados en nombre de la entidad sin revisión y aprobación del proceso de comunicación estratégica.

### 16.1. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Al incurrir en el incumplimiento de estas políticas se debe notificar inmediatamente a la Oficina de Tecnología a través de los siguientes canales:

- Correo electrónico: mesadeayuda@bomberosbogota.gov.co
- Mesa de Ayuda: PBX 3822500 Ext. 14300
- Mesa de Ayuda: WhatsApp: +57 3058908288
- A través de la herramienta de gestión de Mesa de Ayuda reportando el incidente de seguridad, en lo posible con copia al oficial de seguridad de la información.

Asimismo, se deben notificar situaciones tales como personas ajenas a la UAECOB en oficinas y centros de cómputo, correos maliciosos o sospechosos, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso ilegal de software, divulgación, alteración y hurto de información.

### 16.2. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DEL RIESGO

La gestión del riesgo de seguridad de la información y ciberseguridad se encuentra alineada con la Metodología del Sistema Integral para la Administración y Gestión de Riesgos de la UAECOB y con los lineamientos que desde la Norma ISO 31000:2018 - Sistema de Gestión de Riesgos se describen.

La matriz de riesgos definida en la Metodología de Riesgos de Seguridad incluye el análisis de los atributos generales de seguridad de la información y ciberseguridad, estos son, confidencialidad, integridad y disponibilidad, en otras palabras, se identifican y analizan para cada uno de los riesgos estos pilares.

#### 16.2.1. La gestión del riesgo para la confidencialidad

Se definen como riesgos que afectan este pilar aquellos que describen que la información puede ser conocida o utilizada sin autorización por cualquier colaborador, persona o ente dentro o fuera de la UAECOB. Asimismo, la información que pueda estar expuesta para ser utilizada por personas no autorizadas.

#### 16.2.2. La gestión del riesgo para la integridad

Se definen como riesgos que afectan este pilar los que hagan referencia a aquella información que puede ser manipulada o alterada, es decir, se tendrán en cuenta aquellas situaciones o escenarios en que la información no pueda mantener la exactitud y aquellas modificaciones indebidas que afecten el orden lógico de los datos cambiando su estructura o significado.

#### 16.2.3. La gestión del riesgo para la disponibilidad

Se definen como riesgos que afectan este pilar los que describan aquella información que no pueda ser accesible y utilizable en el momento que sea necesario o se requiera por las personas, sistemas o procesos operacionales.

## 17. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

### 17.1. Continuidad de la seguridad de la información

La UAECOB debe contemplar una estrategia de continuidad de negocio basada en los resultados del BIA (Bussines Impact Analisis por sus siglas en inglés) y demás documentación que se ha desarrollado que permita contar con lineamientos para la

continuidad de las operaciones de negocio; entre esta documentación se encuentra la Política de Continuidad de Negocio, el Manual de Continuidad de Negocio, el Análisis de brecha versus las buenas prácticas de la norma ISO 22301 y el Plan de Gestión de Crisis).

Planificar e implementar la continuidad de negocio en la UAECOB debe ser un aspecto fundamental teniendo en cuenta no solo los recursos tecnológicos, sino también activos de información críticos de los procesos, los cuales deben ser definidos y estructurados en el BIA; además:

a. Se deben realizar pruebas periódicas a los controles de continuidad de negocio y de continuidad de la seguridad de la información implementados, con el fin de asegurar que sean válidos y eficaces durante situaciones adversas.

b. Los responsables de los procesos e información deben asegurar que se actualicen los Planes de Continuidad de Negocio con posterioridad a los cambios en la infraestructura tecnológica con respaldo de la Oficina de Tecnología.

c. Contemplar un sitio alterno donde los controles implementados en el ambiente de producción deben ser consistentes.

d. Los cambios de seguridad en el ambiente de producción deben ser aplicados de la misma forma para el ambiente de contingencia.

e. El Plan de Continuidad de Negocio debe ser protegido contra accesos no autorizados, contemplando a su vez copias de respaldo y que estas sean resguardadas en un sitio externo con la protección adecuada tanto física como medioambientalmente.

### 17.2. Redundancias

a. La UAECOB debe establecer e implementar un Plan de Recuperación de Desastres (PRD) con el fin de asegurar la redundancia (Los sistemas redundantes, en ingeniería de computadores, son aquellos en los que se repiten aquellos datos o hardware de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuado) y continuidad de las instalaciones de procesamiento de información.

b. La UAECOB debe realizar pruebas periódicas al PRD, con el fin de asegurar que los controles tecnológicos implementados sean válidos y eficaces durante situaciones adversas.

## 18. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

### 18.1.1. Identificación de la legislación aplicable y requisitos contractuales

La Oficina Asesora Jurídica y el oficial de seguridad de la información deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la UAECOB relacionados con seguridad de la información. Para ello, se pueden apoyar en los jefes de grupo, tales como el Grupo de Gestión de Talento Humano y Gestión Documental.

### 18.1.2. Derechos de propiedad intelectual

a. La Oficina de Tecnología debe asegurarse de que todo el software que se ejecute en la UAECOB esté protegido por derechos de autor y requiera licencia de uso o, en su lugar, sea software de libre distribución y uso.

b. Los usuarios no deben instalar softwares o sistemas de información en sus estaciones de trabajo o equipos portátiles suministrados para el desarrollo de sus actividades.

c. Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de softwares, basados en el Procedimiento de Derechos de Propiedad Intelectual.

d. Es ilegal duplicar softwares o su documentación sin la autorización del propietario de los derechos de autor y su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

e. El Grupo de Contratación debe incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.

### 18.1.3. Protección de registros

La UAECOB se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de confidencialidad, integridad y disponibilidad, siguiendo las directrices del Procedimiento de Gestión de Activos.

### 18.1.4. Privacidad y protección de información de datos personales

La UAECOB, quien será «responsable del tratamiento de los datos personales», tal y como este término se define en la Ley 1581 de 2012, respeta la privacidad de cada uno de los terceros que le suministren sus datos personales a través de los diferentes puntos de recolección y captura de dicha información. Por lo tanto, la UAECOB debe implementar los

controles necesarios para su protección y en ningún momento divulgará esta información a terceras partes a menos que cuenten con la autorización formal de los titulares o en los casos en que la ley lo permita.

#### 18.1.5. Reglamentación de controles criptográficos

La UAECOB se regirá por la Ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y otras disposiciones” y sus decretos reglamentarios, según aplique.

### 18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

#### 18.2.1. Revisión de la seguridad de la información

El proceso de evaluación, control y mejora debe realizar auditorías internas de revisión independiente al menos anualmente. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la entidad para gestionar la seguridad de la información. Esta revisión, que es responsabilidad de Control Interno de la UAECOB, debe incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios en el enfoque hacia la seguridad, incluyendo la política y los objetivos de control.

#### 18.2.2. Revisión al cumplimiento técnico

El jefe de la Oficina de Tecnología debe coordinar la revisión periódica (al menos anualmente) de los sistemas de información para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información. Para ello, se debe determinar a qué sistemas de información se les hará revisión.

### 18.3. CUMPLIMIENTO

El incumplimiento de esta política está sujeto a las sanciones disciplinarias, fiscales y penales que se deriven de la conducta del implicado, incluso cuando se encuentre en situaciones administrativas como permisos, licencias, vacaciones, suspensiones en ejercicio del empleo o en comisión.

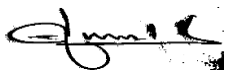
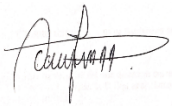
## 19. DOCUMENTOS RELACIONADOS

| CÓDIGO | DOCUMENTO |
|---|---|
| | |
| | |

## 20. CONTROL DE CAMBIOS

| VERSIÓN | FECHA | DESCRIPCIÓN DE LA MODIFICACIÓN |
|---|---|---|
| 01 | 28/12/2021 | Creación del documento |
| 02 | 07/06/2022 | Actualización del documento |

## 21. CONTROL DE FIRMAS

| **Elaboró**<br>José Hernán Morales<br>Alvaro Bernal Ruiz | **Cargo**<br>Contratista OAP<br>Contratista OAPG | Firma<br>  <br>  |
|---|---|---|
| **Revisó**<br>Camilo Escobar<br>**Revisó**<br>Oswaldo García Rincón | **Cargo**<br>Vo.Bo. de Mejora Continua - OAP<br>**Cargo**<br>Líder tic | Firma<br>  <br>  |
| **Aprobó**<br>Norma Cecilia Sánchez Sandino | **Cargo**<br>Jefe Oficina Asesora de Planeación | Firmado en original<br>  |