POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Unidad Administrativa
Especial de Servicios Públicos
–UAESP
Marzo 2024

ALCALDÍA MAYOR DE BOGOTÁ D.C.
UAESP Unidad Administrativa Especial de Servicios Públicos
BOGOTÁ

CONTENIDO

1. INTRODUCCIÓN 6
2. TÉRMINOS Y DEFINICIONES 6
3. OBJETIVOS 9
3.1. OBJETIVO GENERAL 9
3.2. OBJETIVOS ESPECIFICOS 9
4. ALCANCE 10
5. MARCO NORMATIVO 10
6. COMPROMISO DE LA DIRECCIÓN 14
7. PRINCIPIOS 14
8. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL 16
9. POLÍTICAS ESPECIFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 16
9.1. POLITICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ... 16
9.1.1. Organización Interna 16
9.2. POLÍTICA DE DISPOSITIVOS MÓVILES Y BYOD 17
9.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL TRABAJO REMOTO 20
9.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL RECURSO HUMANO 21
9.4.1. Antes de Asumir el Empleo o la Prestación del Servicio 21
9.4.2. Durante la ejecución del empleo o la prestación del servicio. 22
9.4.3. Finalización de la prestación del servicio o del empleo. 23

9.5. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN 24
9.5.1. Responsabilidad y Clasificación de Activos de Información 24
9.5.2. Medios Removibles 26
9.6. POLÍTICA DE CONTROL DE ACCESO.....27
9.6.1. Requisitos para el Control de Acceso.....27
9.6.2. Gestión de Acceso de Usuarios 28
9.6.3. Responsabilidades de los Usuarios para el Uso de Contraseñas. 31
9.6.4. Acceso a Sistemas y Aplicaciones. 32
9.7. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO 36
9.7.1. Áreas Seguras.....36
9.7.2. Seguridad de Equipos Tecnológicos.....39
9.8. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA 41
9.9. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS.....42
9.10. SEGURIDAD EN LAS OPERACIONES 44
9.10.1. Procedimientos y Responsabilidades Operacionales. 44
9.10.2. Directrices Contra Código Malicioso. 46
9.10.3. Registros y Supervisión.....47
9.10.4. Control de Software. 47
9.10.5. Gestión de Vulnerabilidades.....48
9.10.6. Auditoria de Sistemas de Información.....49
9.11. POLÍTICA DE BACKUPS.....49
9.12. POLÍTICA DEL BUEN USO DEL INTERNET Y HERRAMIENTAS COLABORATIVAS.....51
9.12.1. Buen Uso del Internet.....51

9.12.2. Buen Uso del Correo electrónico y Herramientas Colaborativas. 52

9.13. POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES.....54

9.13.1. Gestión de Seguridad en las Redes.....54

9.13.2. Intercambio de Información.....55

9.14. POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 57

9.14.1. Requisitos de Seguridad de los Sistemas de Información. 57

9.14.2. Seguridad en el desarrollo y soporte de sistemas de información 58

9.14.3. Datos de Prueba 61

9.15. POLÍTICA DE RELACIÓN CON PROVEEDORES.....62

9.16. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....63

9.17. POLÍTICA DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO.....65

9.17.1. Cumplimiento de Requisitos legales y Contractuales 65

9.17.2. Disponibilidad de Instalaciones de procesamiento de información 67

9.18. POLÍTICA DE CUMPLIMIENTO DE REQUISITOS LEGALES 67

9.18.1. Cumplimiento de Requisitos Legales. 67

9.18.2. Revisión de Seguridad de la Información. 69

10. OBLIGACIONES.....70

11. REVISIÓN.....70

12. COMUNICACIÓN 70

13. ROLES Y RESPONSABILIDADES 71

13.1. ROLES.....71

13.2. PERFILES 74

14. INCUMPLIMIENTO 75

15. CONTROL DE CAMBIOS 75

16. AUTORIZACIONES 76

ÍNDICE DE TABLAS

Tabla 1 Perfiles de los Oficiales 74

Tabla 2 Control de Cambios 75

Tabla 3 Revisión y Aprobación de las Políticas 76

1. INTRODUCCIÓN

La Unidad Administrativa Especial de Servicios Públicos - UAESP, en respeto de los Derechos Humanos y de los principios constitucionales y legales, entiende la información, como uno de los activos más importantes para el cumplimiento de su misionalidad y la toma de decisiones, por esta razón y como parte del proceso de mejora continua, se ha comprometido a definir, implementar, operar y actualizar las Políticas de Seguridad y Privacidad de la Información, con el fin de establecer un marco de confianza en el ejercicio de sus deberes, alineados a las necesidades del negocio y los requerimientos legales, reglamentarios, regulatorios y de normas colombianas en materia de seguridad y privacidad de la información.

De acuerdo con lo anterior, el presente documento establece el compromiso, los principios y directrices que buscan proteger y mantener la integridad, confidencialidad y disponibilidad de la información, implementando controles para el desarrollo de todas las actividades relacionadas con el tratamiento de la información en la Entidad, con el fin de mitigar los riesgos e incidentes de seguridad de la información; Así mismo, define los deberes, obligaciones y responsabilidades de los sujetos aplicables.

2. TÉRMINOS Y DEFINICIONES

Activos de información: Toda información o elemento relacionado con el tratamiento de esta (Documentos, hardware, software, servicios, edificios, personas, entre otros) que tenga valor para la organización y por lo tanto se debe proteger. Se puede considerar un activo de información los datos creados o utilizados por un proceso, pueden ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, equipos de cómputo relacionados al tratamiento o almacenamiento de información, software del sistema, servicios utilizados para la transmisión, recepción y control de la información, edificaciones, entre otros.

Amenaza: Causa potencial de un incidente no deseado que puede provocar daños o afectaciones a un activo de información.

Autoridad competente: Es la autoridad apta e idónea para tratar de un determinado procedimiento o proceso de acuerdo con la ley.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO 27000]

Continuidad del Negocio: Para propósitos de este documento, el término puede interpretarse en un sentido amplio para referirse a la capacidad de una organización para seguir funcionando y proporcionando sus productos o servicios en niveles aceptables luego de enfrentar un incidente significativo.

Contratista: Persona natural o jurídica que celebra un contrato con una entidad pública o privada para la ejecución de obras, la prestación de servicios, la realización de suministros o la realización de cualquier otro tipo de actividad contractual.

DAFP: Departamento Administrativo de la Función Pública (DAFP), es la entidad técnica, estratégica y transversal del Gobierno Nacional que contribuye al bienestar de los colombianos mediante el mejoramiento continuo de la gestión de los servidores públicos y las instituciones en todo el territorio nacional.

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Disponibilidad: La propiedad de tener la información cuando es requerida. Se relaciona con la facilidad y oportunidad de acceso a la información.

Evento de seguridad: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la Política de Seguridad de la Información o falla en los controles.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO 27000]

Integridad: Propiedad de la información relativa a su exactitud y completitud. [ISO 27000]

MSPI: Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MinTIC.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Es pertinente señalar que "seguridad de la información" no solo corresponde a Seguridad Informática, sino que su alcance se complementa con ciberseguridad, seguridad física, ambiental y del recurso humano entre otras, buscando mantener la confidencialidad, la disponibilidad e integridad de la información. [Directiva 002 de 2021 – Alcaldía Mayor de Bogotá]

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Servidor(a) Publico(a): Toda persona natural que mediante relación de trabajo y bajo continuada dependencia y subordinación ejerce funciones públicas en forma permanente o temporal a una entidad estatal, atribuidas al cargo o la relación laboral y que constan en la Constitución Política, la ley o el reglamento o le son señaladas por autoridad competente. También son servidores públicos los trabajadores oficiales, los de elección popular y periodo fijo. (Concepto 150801 de 2022 Departamento Administrativo de la Función Pública)

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Terceros: Para efectos de esta política, el termino hace referencia a entidades, organizaciones, proveedores, practicantes o individuos que no forman parte directa de la Entidad tenga un vínculo laboral con la Entidad y preste un servicio de forma directa o

indirecta bien sea en las instalaciones de la Entidad o en sus propias instalaciones y que emplea algunos de los recursos informáticos y de comunicaciones de la Entidad.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3)

Usuario: Cualquier persona que tiene acceso a la plataforma y a los activos de información, sea en calidad de usuario final, tercero o administrador de la plataforma.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Establecer las políticas y directrices orientadas a proteger y preservar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los activos de información gestionados por la Entidad, mediante una gestión integral de riesgos y la implementación de controles efectivos que prevengan la materialización de incidentes de seguridad y privacidad de la información, cumpliendo los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua, el uso efectivo y la apropiación de seguridad y privacidad de la Información.

3.2. OBJETIVOS ESPECIFICOS

I. Desarrollar y establecer políticas, procedimientos e instructivos claros y completos en materia de seguridad y privacidad de la información, que sean adecuados para las necesidades y requisitos de la Entidad.
II. Establecer un plan de respuesta a incidentes de seguridad y privacidad de la información que permita una identificación temprana, notificación oportuna, contención eficiente, recuperación efectiva y análisis de los incidentes.

III. Establecer un conjunto adecuado de controles que permitan fortalecer la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la Información, basado en mejores prácticas y estándares reconocidos.

IV. Fortalecer la cultura organizacional, a través de la concienciación, participación y apropiación de la seguridad y privacidad de la información, orientados a la mejora continua.

V. Asegurar el cumplimiento de los principios, requisitos legales, reglamentarios y regulatorios aplicables en materia de seguridad y privacidad de la información

VI. Garantizar la continuidad del negocio frente a posibles incidentes de seguridad y privacidad de la información.

VII. Establecer e implementar un sistema de gestión de seguridad de la información (SGSI) que promueva la confianza y la seguridad digital entre los grupos de interés de la organización.

4. ALCANCE

Aplica para todos los servidores (as) públicos (as), contratistas, proveedores, operadores, así como aquellas personas o terceros que utilicen, recolecten, procesen, intercambien, consulten y accedan a los activos de información de la Unidad Administrativa Especial de Servicios Públicos – UAESP. Así mismo, se extiende a todos los procesos de la entidad, dentro del marco de gestión establecido en el Modelo Integrado de Planeación y Gestión - MIPG propuesto por el DAFP y el Modelo de Seguridad y Privacidad de la Información - MSPI.

5. MARCO NORMATIVO

Teniendo en cuenta las disposiciones legales sobre seguridad de la información, el marco normativo en la materia, sin ser restringido, corresponde a:

CONSTITUCIÓN POLITICA: Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones

que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (…).

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Ley 23 de 1989: Sobre derechos de autor.

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 se dictan otras disposiciones.

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

Ley 603 DE 2000: Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Ley 962 de 2005: Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1341 de 2009: Por la cual se definen los 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 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 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 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Decreto 2106 DE 2019: Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

Decreto 2364 de 2012: Firma electrónica. Decreto 2609 de 2012 Expediente electrónico.

Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012, derogado parcialmente por el Decreto 1081 de 2015.

Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Compilado en el Decreto Único Reglamentario 1081 de 2015 del Sector Presidencia de la República.

Decreto 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo." Reglamenta parcialmente la Ley 1581 de 2012.

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 1081 de 2015: Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. Reglamenta parcialmente la ley 1581 de 2012 y compila el Decreto 103 de 2015.

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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Decreto 338 de 2022: "Por el cual se adiciona el Titulo 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".

Decreto 767 de 2022: "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

Acuerdo 002 de 2023: Por el cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.

Resolución 2710 del 2017: Por la cual se establecen lineamientos para la adopción del protocolo IPV6.

Directiva 002 de 2018 - Secretaría Jurídica Distrital: Tratamiento de Datos Personales.

Directiva 005 de 2018 - Secretaría Jurídica Distrital: Tratamiento de datos personales – Autorizaciones, datos sensibles, datos de niños, niñas y adolescentes, cámaras y videos de seguridad, sanciones y recomendaciones.

Resolución 1519 de 2020: Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

CONPES 3854 de 2016: Política Nacional de Seguridad Digital.

CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.

NTC-ISO-IEC 27001:2022: Sistema de Gestión de Seguridad de la Información.

6. COMPROMISO DE LA DIRECCIÓN

La Dirección de la Unidad Administrativa Especial de Servicios Públicos, entendiendo la importancia de una adecuada gestión de los activos de información, se compromete con la implementación, seguimiento y medición del Modelo de Seguridad y Privacidad de la Información MSPI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de los requerimientos legales, reglamentarios, regulatorios y de normas colombianas en materia de seguridad y privacidad de la información y en concordancia con la misión, visión, los objetivos y planes estratégicos de la Entidad.

7. PRINCIPIOS

Los principios están orientados a proteger los tres pilares de seguridad de la información, confidencialidad, integridad y disponibilidad, para garantizar que la información recibe los niveles de protección adecuados.

Principio de cumplimiento normativo:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, se ajustará a la normativa de aplicación legal vigente con relación a la seguridad y privacidad de la información, en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

Principio de Gestión de Riesgos:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, gestionará los riesgos hasta niveles aceptables implementando controles de seguridad adecuados y pertinentes.

Principio de concienciación y formación:

La Unidad Administrativa Especial de Servicios Públicos – UAESP, articulará programas de formación, sensibilización y campañas de concienciación para todos los servidores (as) públicos (as), contratistas y terceros que tengan acceso a los activos de información de la entidad en materia de seguridad de la información.

Principios de continuidad del negocio:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, asegurará la continuidad del negocio mediante planes de contingencia para los servicios de la información críticos y de procesos misionales, velando por la confidencialidad, integridad y disponibilidad de la información.

Principio de responsabilidad:

Todos los servidores (as) públicos (as), contratistas y terceros en relación con la Unidad Administrativa Especial de Servicios Públicos – UAESP, deben ser responsables de los activos de información y sus acciones relacionadas a la seguridad de la información, cumpliendo con las normas y controles establecidos.

Principio de gestión de incidentes:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, gestionará los incidentes de seguridad digital articulando las capacidades que permitan atender de forma oportuna y adecuada la materialización de riesgos.

Principio de mejora continua:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, revisará de manera periódica el grado de eficacia de los controles de seguridad implementados en la Entidad y velará por la disponibilidad de sus procesos estratégicos, misionales, de apoyo y de evaluación y la continuidad de su operación basada en la prevención de incidentes de seguridad de la información.

Lo anterior, con el fin de aumentar la capacidad de adaptación a la constante evolución del riesgo y del entorno tecnológico.

Principio de Confianza:

La unidad Administrativa Especial de Servicios Públicos, propenderá por la implementación, adecuación y uso de tecnologías, controles y lineamientos que permitan la protección de los activos de información.

8. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La Unidad Administrativa Especial de Servicios Públicos -UAESP- se compromete a implementar una gestión integral de riesgos para proteger la confidencialidad, integridad, disponibilidad y no repudio de la información en todo su ciclo de vida. Esta gestión estará alineada con la política de administración del riesgo de la UAESP y se basará en la identificación, evaluación y tratamiento de los riesgos asociados a la seguridad de la información. Además, se promoverá una cultura de seguridad y privacidad de la información entre los servidores(as) públicos(as), contratistas y terceros, enfatizando la conciencia y formación continua en seguridad de la información, la implementación de controles apropiados y el cumplimiento de requisitos legales y normativos.

Se realizarán revisiones periódicas de los controles de seguridad, auditorías internas y acciones correctivas y preventivas para lograr una mejora continua en la gestión de la seguridad y privacidad de la información.

9. POLÍTICAS ESPECIFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

9.1. POLITICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

9.1.1. Organización Interna

Directrices:

a) El Oficial de seguridad de la información, junto con la Oficina TIC, deben mantener y documentar los contactos con las autoridades en materia de ciberseguridad y otros entes especializados para que puedan ser contactados en caso de presentarse un incidente de seguridad de la información que requieran de asesoría,

acompañamiento o intercambiar conocimientos para mejorar el sistema de gestión de seguridad de la información y mejorar la respuesta ante incidentes.

b) Es responsabilidad de todos los procesos velar por que la seguridad y privacidad de la información sea parte integral de los proyectos o contratos gestionados, para lo cual contarán con el apoyo del Oficial de seguridad de la información.
c) Todos los proyectos deben contemplar un análisis de riesgos de seguridad de la información, si aplicase.

9.2. POLÍTICA DE DISPOSITIVOS MÓVILES Y BYOD (Bring Your Own Device)

Directrices:

a) La Oficina de Tecnologías de la Información y las Comunicaciones debe establecer las condiciones necesarias para la protección física y el uso seguro de los equipos móviles institucionales, como establecer contraseñas de acceso robustas, cifrar la información almacenada cuando el custodio del activo así lo requiera e identifique de acuerdo con la clasificación y criticidad del mismo, mecanismos de respaldo y demás necesarios para garantizar la seguridad y privacidad de la información, llevando el registro y control de los elementos entregados.
b) La Oficina de Tecnologías de la Información y las Comunicaciones debe proporcionar a los computadores institucionales las herramientas Ofimáticas, Antivirus y de Almacenamiento en nube licenciadas por la Entidad. De acuerdo con la disponibilidad de licencias, se deben proporcionar las mismas herramientas a otros dispositivos móviles con base a la criticidad de la información que se almacene en ellos, en caso de no ser posible, aplicar los controles de acceso y criptográficos necesarios.
c) Los dispositivos móviles personales, no deben estar dentro del dominio de la entidad y para su conexión se debe solicitar autorización a través de la mesa de servicios y cumplir los lineamientos en seguridad de la información establecidos por la Entidad.
d) Las personas que hagan uso del correo institucional en sus dispositivos móviles personales o cualquier otro aplicativo con acceso a información institucional deberán

contar con un mecanismo de bloqueo para prevenir el acceso no autorizado en caso de pérdida o robo, entre ellos:

- Protegerlo con una contraseña segura y cambiarla frecuentemente. La contraseña debe tener mínimo, 8 caracteres alfanuméricos, un patrón de seguridad al menos 7 puntos de contacto o huella dactilar.
- Si el dispositivo lo permite, deberá usarse un doble factor de autenticación.
- Configurar el bloqueo de pantalla para máximo 1 minuto de inactividad.

Si lo anterior no es posible, se deberá contar con doble factor de autenticación en el correo electrónico.

e) Las personas deben tomar medidas para asegurarse de que los correos electrónicos y los archivos adjuntos confidenciales no se guarden en el dispositivo móvil personal o en la nube pública y utilizar los recursos de almacenamiento institucionales para el manejo de datos sensibles.
f) Se debe implementar un mecanismo de cifrado en los dispositivos personales para proteger la información confidencial o sensible almacenada y transmitida.
g) Las personas que hagan uso de sus dispositivos móviles personales para acceder a los recursos de Entidad deben tener instalado un software de seguridad actualizado, asimismo, tener instalado los últimos parches de seguridad del sistema operativo respectivo.
h) Los dispositivos personales solo deben utilizarse para acceder a sistemas, aplicativos y recursos institucionales. Se prohíbe utilizar los dispositivos personales para actividades no laborales, como descargas ilegales de contenido multimedia, acceso a material inapropiado o cualquier otro uso no autorizado con los recursos de la entidad.
i) Todos los dispositivos móviles personales que hagan uso de los recursos de la Entidad o que almacenen información confidencial, deben tener habilitada la opción de borrado remoto para proteger los datos confidenciales en caso de robo o perdida.
j) Se debe notificar de inmediato cualquier pérdida, robo o compromiso de sus dispositivos personales a la Oficina TIC, jefe inmediato y seguir las instrucciones que se den para minimizar el impacto en la seguridad de la información.

k) Los servidores (as) públicos (as), contratistas o terceros, que tengan un dispositivo móvil institucional asignado, deben evitar conectarlos a equipos externos o redes inalámbricas (wifi, bluetooth, entre otros) públicas como Café Internet, Aeropuertos, Restaurantes, entre otros, o diferentes a las redes wifi del hogar para trabajo remoto. En caso de requerir la conexión a redes públicas utilizar herramientas de cifrado o de conexión segura como VPNs.

l) Los servidores (as) públicos (as), contratistas y terceros no están autorizados a cambiar la configuración, realizar instalaciones o desinstalación de las aplicaciones de los dispositivos móviles institucionales que se les entregue o sean asignados como recurso para la ejecución de sus funciones u obligaciones contractuales.

m) Está prohibido el uso de los computadores, dispositivos móviles y dispositivos de almacenamiento removibles de la Entidad por parte de personas no autorizadas.

n) Está prohibido realizar cualquier intervención al hardware o al software no autorizada por la Oficina TIC de cualquier dispositivo móvil institucional, para llevar a cabo mantenimientos de cualquier tipo.

o) Los servidores (as) públicos(as), contratistas o terceros deben configurar solo las cuentas institucionales en los dispositivos asignados.

p) En caso de pérdida o hurto, de cualquier dispositivo móvil asignado o bajo su custodia, se debe reportar oportunamente al jefe inmediato mediante correo electrónico con copia al jefe de la Oficina TIC y al Almacenista.

q) La Oficina de Tecnologías de la Información y las Comunicaciones definirá e implementará herramientas o métodos de borrado seguro y otros mecanismos de seguridad en medios removibles o dispositivos móviles de la Entidad que sean reutilizados o dados de baja.

r) La Oficina de Tecnologías de la Información y las Comunicaciones podrá hacer revisión del cumplimiento de esta política directamente en los dispositivos de la Entidad.

s) La UAESP se reserva el derecho de realizar auditorías y monitoreo periódico de los dispositivos personales utilizados en el entorno de trabajo para asegurar el cumplimiento de esta política y la seguridad de la información de la Entidad.

9.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL TRABAJO REMOTO

Directrices:

a) La Entidad brindará a los servidores (as) públicos (as) los equipos y herramientas necesarias para el cumplimiento de las funciones en las modalidades de trabajo remoto de acuerdo con los lineamientos o normatividad vigente que las regulen.
b) Los servidores (as) públicos (as) podrán disponer de sus propios equipos y demás herramientas, siempre que medie acuerdo con la Entidad. Si no se llega al mencionado acuerdo, la UAESP suministrará los equipos, sistemas de información, software o materiales necesarios para el desarrollo de las funciones.
c) Los servidores (as) públicos (as) deberán cumplir con las obligaciones y responsabilidades en materia de uso y cuidado de los activos de información asignados.
d) La Oficina de Tecnologías de la Información y las Comunicaciones establecerá mecanismos para el trabajo remoto en términos de seguridad y privacidad de la información, que consideren los siguientes aspectos:
   I. Uso de VPN entre el usuario y la UAESP.
   II. Uso de programas de acceso remoto autorizados por parte de la Oficina TIC.
   III. Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la Unidad, la criticidad de la información a la que se accederá y que pasará a través del canal de comunicación y la criticidad de los sistemas de información de la Entidad.
   IV. La amenaza de acceso no autorizado a información o recursos por parte de personas diferentes al servidor(a) publico, por ejemplo, familia y amigos.
   V. Configuración de servicios de redes domésticas y red inalámbrica que incluyan los controles de seguridad perimetral y antivirus.
   VI. Cuando se considere necesario, acuerdos para que la Entidad o el usuario sean responsables por el licenciamiento de software usado en estaciones de trabajo propias.
   VII. Desinstalación de software no autorizado por la UAESP.

d) La sesión remota establecida con la Entidad no debe ser usada por una persona diferente a la asignada.
e) El proceso de Gestión de Talento Humano definirá, documentará y mantendrá actualizados los procedimientos asociados a las modalidades de trabajo remoto, donde se tendrá en cuenta el concepto de la Oficina TIC en la evaluación de los requisitos técnicos o herramientas tecnológicas necesarias a fin de preservar la seguridad y privacidad de la información.
f) Los servidores (as) públicos (as) deben reportar, a través de la mesa de servicios y por los canales establecidos, cualquier evento anormal o incidente de seguridad de la información de acuerdo con la Política 9.16 Gestión de Incidentes de Seguridad y Privacidad de la información.
g) La Oficina de Tecnologías de la Información y las Comunicaciones debe establecer mecanismos de monitoreo sobre las conexiones que permitan verificar las actividades en la suite ofimática, el tiempo y horarios de conexión a los servicios tecnológicos a los que el servidor público o contratista tiene acceso.
h) Al finalizar la modalidad de trabajo remoto, se deberán devolver los activos de información asignados por parte de la Entidad y la Oficina TIC revocará los accesos remotos.

9.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL RECURSO HUMANO

9.4.1. Antes de Asumir el Empleo o la Prestación del Servicio

Directrices:

a) Previo al proceso de contratación o vinculación del personal, las áreas correspondientes deberán validar los antecedentes (procuraduría, contraloría, policía u otros que apliquen) de los candidatos, la formación académica, experiencia y demás información o aspectos que se requieran, de acuerdo con la normatividad vigente y reglamentos de la Entidad en la materia.
b) Las áreas encargadas de contratación o vinculación del personal deben tener autorización para el tratamiento de datos personales de acuerdo con la Política de

tratamiento de datos personales de la Entidad, y lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.

c) Se deberá incluir una cláusula en las minutas de contrato, o por medio del mecanismo que considere oportuno el área de Contratación, obligaciones en relación con el cumplimiento de la Política General de Seguridad y Privacidad de la Información.
d) Las áreas de Gestión Documental, Talento Humano y Contratación deben establecer los mecanismos y controles necesarios para proteger la información contenida en las historias laborales y expedientes contractuales.
e) Los servidores (as) públicos (as), contratistas y terceros que desarrollen funciones u obligaciones contractuales en la UAESP estarán sujetos a clausulas o acuerdos de confidencialidad dados por la criticidad de los activos de información bajo su custodia.

9.4.2. Durante la ejecución del empleo o la prestación del servicio.

Directrices:

a) La Oficina de las Tecnologías de la Información y las Comunicaciones, en articulación con el proceso de gestión talento humano, deben dar a conocer a los servidores (as) públicos (as), contratistas o terceras partes que desempeñen funciones en la Entidad, las políticas, roles, responsabilidades y obligaciones en materia de seguridad y privacidad de la información, incluyendo la protección de datos personales.
b) El proceso de Gestión de Talento Humano deberá incluir dentro del Plan Institucional de Capacitación, temáticas asociadas a la seguridad y privacidad de la información, que incluyan las políticas, roles, responsabilidades y obligaciones relacionada con el Modelo de Seguridad y Privacidad de la Información de la UAESP.
c) Es responsabilidad de todos los servidores (as) públicos (as) y contratistas conocer y cumplir las políticas de seguridad y privacidad de la información, asistir a charlas, capacitaciones o sensibilizaciones en la materia y uso correcto de los sistemas de información de la Entidad.

d) Es obligación de todos los servidores (as) públicos (as) y contratistas reportar las vulnerabilidades o incidentes de seguridad de la información cumpliendo con la Política 9.16 Gestión de Incidentes de Seguridad y Privacidad de la información.
e) Está prohibido la realización de pruebas para detectar y explotar una vulnerabilidad o falla de seguridad como: actividades de rastreo, denegación de servicio, difusión de virus, spyware, entre otros y el uso de programas no autorizados, salvo las personas (naturales o jurídicas) autorizadas por la Oficina TIC en el cumplimiento de sus funciones u obligaciones contractuales.
f) La solicitud de acceso a los servicios de información y las herramientas colaborativas de la Entidad seguirán los lineamientos dispuestos por la Oficina TIC conforme a la Política 9.6 Control de acceso, numeral 9.6.2.
g) No se debe almacenar información personal en los equipos de cómputo o dispositivos móviles de la Entidad y sitios de almacenamiento corporativos en la nube. La Entidad no se hace responsable por la pérdida de información que no corresponda con las actividades propias del cargo u obligaciones contractuales y de acuerdo con los lineamientos de la Oficina TIC para el respaldo de información.
h) Cualquier acción u omisión que atente contra la seguridad y privacidad de la información o explotación de vulnerabilidades de los sistemas internos o externos, realizada por los servidores (as) públicos (as) o contratistas será considerado como una falta al Manual y a la Política de General de Seguridad y Privacidad de la Información y se adelantaran las acciones del proceso disciplinario correspondiente.

9.4.3. Finalización de la prestación del servicio o del empleo.

Directrices:

a) El proceso de Gestión de Talento Humano deberá informar de forma oportuna a la Oficina TIC, a través de la herramienta colaborativa de trabajo, la Mesa de servicios o la herramienta que la OTIC disponga, las situaciones administrativas del servidor (a) público (a), que lo separen del cargo, para proceder a suspender, cancelar o remover el acceso a los sistemas de información y demás servicios o recursos tecnológicos de la Entidad.

b) Los supervisores de contrato deberán informar de forma Oportuna a la Oficina TIC, a través de la herramienta colaborativa de trabajo, la Mesa de servicios o la herramienta que disponga la OTIC, cesión o terminación del vínculo contractual del contratista para proceder a suspender, cancelar o remover el acceso a los sistemas de información y demás servicios o recursos tecnológicos de la Entidad.

c) En los casos en que los accesos a los sistemas de información o herramientas tecnológicas de la Entidad deban mantenerse, luego de finalizada la vinculación del contratista con la Entidad o las situaciones administrativas que separen a un servidor (a) público (a) de su cargo, se deberá solicitar a la Oficina TIC, de forma oportuna, la ampliación del tiempo de acceso. Esta solicitud, solo podrá ser autorizada por los supervisores de contratos, subdirectores, jefes de Oficina o Director(a), quienes asumirán la responsabilidad por los riesgos asociados a las acciones del usuario. En todo caso, este tiempo no puede ser ilimitado y deberá determinarse en la solicitud.

d) La Oficina de Tecnologías de la Información y Comunicaciones deberá implementar controles para la desactivación de los usuarios en los sistemas de información, y en aquellos que no se autentican con el directorio activo se deberá hacer de forma manual.

e) Los servidores (as) públicos (as) o contratistas en el momento de su desvinculación laboral o terminación de contrato deberán devolver su carné y los activos de información que estén en su custodia o responsabilidad siguiendo los lineamientos vigentes.

9.5. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

9.5.1. Responsabilidad y Clasificación de Activos de Información

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones definirá y documentará el método de reporte, identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades,

manteniendo mecanismos acordes para el control de riesgos de la información y alineados al Programa de Gestión Documental.

b) La Oficina de Tecnologías de la Información y Comunicaciones debe identificar y comunicar a las partes interesadas la infraestructura critica cibernética de acuerdo con la normatividad vigente aplicable.
c) Cada proceso de la Entidad debe contar con el inventario actualizado de sus activos de información a través del instrumento dispuesto para ello y reportarlos a la Oficina TIC.
d) Cada activo de información de la Entidad debe tener un propietario y custodio, quienes deben clasificarlos y reportarlos en el instrumento establecido para ello, de acuerdo con la metodología de identificación y clasificación definida por la Oficina TIC.
e) Los custodios de los activos de información deben operar y proponer mejoras a los controles definidos con el fin de asegurar un apropiado nivel de protección de estos, basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados o requerimientos legales.
f) La Subdirección Administrativa y Financiera, junto con el Apoyo de la Oficina TIC, debe implementar los mecanismos necesarios y acordes para el rotulado de la información física y digital de acuerdo con lo establecido en la Entidad y alineado a la normatividad sobre información pública y protección de datos personales.
g) La Oficina de Tecnologías de la Información y Comunicaciones debe consolidar los inventarios reportados por los diferentes procesos en una herramienta única que contenga todos los activos de información de la Entidad, con el objetivo de publicarlos en cumplimiento de la normativa vigente.
h) Los servidores(as) públicos(as), contratistas o terceros deben hacer la devolución de los activos de información asignados a su cargo, a su jefe inmediato, supervisor de contrato o el que haga sus veces, una vez finalice la vinculación, relación contractual o cualquier situación administrativa que lo desvincule funcionalmente con la Entidad más de 15 días hábiles.

i) Para la disposición final de los activos de información de tipo “información” se deberá seguir lo dispuesto por el proceso de Gestión Documental.

j) En caso de presentarse un incidente de seguridad de la información se deberá reportar inmediatamente a través de los canales dispuesto para ello de acuerdo con la Política 9.16 Gestión de incidentes de seguridad y privacidad de la información.

9.5.2. Medios Removibles

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe proveer a los usuarios de la UAESP los métodos de cifrado de la información, así como las herramientas adecuadas para tal fin, de acuerdo con la Política 9.9 Controles Criptográficos.

b) Es responsabilidad de todos, tomar las medidas necesarias para la protección de la información sensible que se encuentre en medios removibles bajo su custodia (Discos Duros Externos, Memorias USB, MicroSD, SD, entre otros) para evitar accesos no autorizados, daños, perdida o fugas de información. Dentro de las medidas recomendadas se encuentra el cifrado de información y respaldos o backups, de acuerdo con los lineamientos de las políticas 9.9 Controles criptográficos y 9.11 Backups.

c) Es responsabilidad de todos, escanear todo medio removible con el software antivirus en concordancia con el numeral 9.10.2 Lineamientos – Contra Código Malicioso.

d) Está prohibido el uso de medios removibles que contengan información sensible, información pública clasificada o reservada en los dispositivos que tenga acceso el público. De igual manera, se prohíbe el préstamo o uso de los medios que contengan información sensible a personal no autorizado o externo de la Entidad.

e) Ningún medio de almacenamiento removible debe ser usado como medio de respaldo, para esta tarea la Oficina TIC dispondrá los lineamientos, las herramientas, medios y canales adecuados de acuerdo con la política 9.11 Backups.

f) Todo medio removible que deba ser retirado de las instalaciones propias de la Entidad, deberá ser informado por su custodio al jefe inmediato o líder del proceso para su respectiva autorización. En caso de que estos medios contengan información sensible, clasificada o reservada, deberán implementarse controles de seguridad como el cifrado del dispositivo o de información, de acuerdo con la política 9.9 Controles Criptográficos.

g) La información sensible (información pública clasificada o reservada) que deba ser eliminada de medios removibles, por reúso o eliminación de este, deberá emplear métodos de borrado seguro, para lo cual, la Oficina TIC dispondrá de las herramientas y métodos apropiados de acuerdo con el numeral 9.2 literal q.

h) Para la transferencia de medios de almacenamiento removibles a otras Entidades se deberán seguir los lineamientos del numeral 9.7.2 – Seguridad de equipos tecnológicos literal o.

i) En caso de pérdida o robo de un medio removible propiedad de la Entidad deberá notificarse al jefe inmediato y reportar como un incidente de seguridad de la información en la brevedad posible. Si el medio removible relacionado con el caso no era propiedad de la Entidad, pero contenía información sensible, deberá igualmente notificarse como un caso de incidente de seguridad de la información a través de los canales dispuesto en el procedimiento para el reporte y gestión de incidentes de seguridad de la información definidos por la Oficina TIC.

j) Se prohíbe el uso de medios removibles de la Entidad para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionados con el cumplimiento de la funciones u obligaciones contractuales.

9.6. POLÍTICA DE CONTROL DE ACCESO

9.6.1. Requisitos para el Control de Acceso

Directrices:

a) Los custodios de los activos de información deberán establecer las medidas de control de acceso adecuadas con el fin de mitigar riesgos asociados al acceso a la información y recursos de infraestructura de la Entidad.

b) La Oficina de Tecnologías de la Información y Comunicaciones debe suministrar las credenciales para acceder a los sistemas de información y demás servicios de red que tenga la Entidad a los que haya sido autorizado de acuerdo con su rol o deberes.
c) La asignación de los privilegios de acceso de todos los usuarios en los sistemas información y servicios de red de la UAESP debe regirse de acuerdo solo con las actividades que el usuario vaya a realizar.
d) Las cuentas de usuario de los sistemas de información y demás servicios de red otorgados a los servidores (as) públicos (as), contratistas o terceros constituyen un activo de la Entidad que permite identificar de manera única e irrepetible a cada usuario. En ninguna circunstancia las cuentas de usuario deberán ser compartidas, transferidas, reasignadas y su contraseña revelada.
e) Las solicitudes para conexión remota a la red de la Entidad deberán ser realizadas por los líderes de procesos, supervisores de contrato o quienes hagan sus veces y serán aprobadas y registradas por la Oficina TIC.
f) Los(as) líderes de proceso, Supervisores(as) de Contrato o quienes hagan sus veces son los únicos autorizados para solicitar el acceso a los servicios de información, sistemas y recursos tecnológicos de la Entidad, especificando los privilegios que debe tener el usuario. Esta solicitud está sujeta aprobación por la Oficina TIC.
g) La Oficina de Tecnologías de la Información y Comunicaciones debe monitorear el uso de los servicios de red a través de las diferentes herramientas tecnológicas con las que cuente la Oficina TIC para este fin.

9.6.2. Gestión de Acceso de Usuarios

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe definir y documentar un procedimiento para la creación, modificación y cancelación de usuarios y privilegios, teniendo en cuenta que las credenciales deben ser únicas.
b) La creación de las cuentas de usuario en los sistemas de información de la Unidad Administrativa Especial de Servicios Públicos está sujeta al estándar de

identificadores de usuario que establezca la Oficina TIC, salvo que existan impedimentos técnicos justificables que dificulten la adopción de dicho estándar.

c) La Oficina de Tecnologías de la Información y Comunicaciones deberá deshabilitar las credenciales de usuarios tan pronto se haya informado de la finalización del vínculo laboral, contractual u otra situación administrativa que amerite la acción, de acuerdo con la Política 9.4 Seguridad de la información para el recurso humano, numeral 9.4.3 Lineamientos – Finalización de la prestación del servicio o del empleo, por parte de las personas responsables para esto, siguiendo el procedimiento establecido por la Oficina TIC para la gestión de usuarios.

d) La Oficina de Tecnologías de la Información y Comunicaciones deberá realizar revisiones periódicas con el fin de:

   i. Inhabilitar cuentas de usuarios redundantes.

   ii. Inhabilitar cuentas que no presenten actividad por más de 60 días, de acuerdo con los sistemas de información, aplicativos y las condiciones de trabajo remoto a los que estén expuestos los servidores (as) públicos (as), contratistas y terceros.

e) La creación de cuentas genéricas, deben contar con la aprobación de la Oficina TIC y estas deberán registrarse y ser asignadas a una sola persona responsable de su utilización, quien será la encargada de notificar las novedades correspondientes de la cuenta.

f) Las cuentas por defecto asociadas a los dispositivos que conforman la infraestructura tecnológica de la Entidad, los sistemas operativos, sistemas de información, bases de datos o aplicativos deben ser deshabilitadas y su contraseña cambiada, siempre que no sea de uso obligatorio para el funcionamiento del servicio. En caso contrario deberán ser asignadas, autorizadas y controladas por la Oficina TIC.

g) La Oficina de Tecnologías de la Información y Comunicaciones podrá permitir conexiones remotas seguras para la administración de la plataforma tecnológica únicamente a las personas que cumplan con esta labor y estén autorizados por el jefe de la Oficina TIC o quien haga sus veces. En caso de tener que adelantar

accesos por otro tipo de conexión, deberá ser aprobada y controlada por la Oficina TIC.

h) La Oficina de Tecnologías de la Información y Comunicaciones deberá suministrar las claves de acceso a los servidores (as) públicos (as), contratistas o terceros, cuando aplique, y solicitar el cambio inmediato de la misma al ingresar por primera vez.

i) La Oficina de Tecnologías de la Información y Comunicaciones debe procurar que exista interoperabilidad entre los sistemas de información, servicio de correo electrónico y herramientas colaborativas con el directorio activo.

j) Las cuentas con roles administrativos sobre los sistemas de información, sistemas operativos, base de datos, aplicaciones e infraestructura tecnológica deben limitarse a aquellas personas que están encargadas o asignadas de la administración, mantenimiento o seguridad de los sistemas.

k) La Oficina de Tecnologías de la Información y Comunicaciones debe mantener un registro actualizado con las cuentas de usuario con privilegios administrativos y deben estar dentro de un inventario de cuentas, especificando su relación con cada uno de los sistemas de información, a nivel de sistema operativo, base de datos, aplicaciones e infraestructura tecnológica, especificando la siguiente información:

   i. Nombre de la Cuenta y propietario o Responsable de la cuenta
   ii. Ubicación de la cuenta (servidor, sistema o aplicativo)
   iii. Ambiente al que pertenece la cuenta (Producción, Desarrollo, entre otros.)
   iv. Servicio o aplicativo al que pertenece.
   v. Tipo de Cuenta (Genérica o de Conexión).
   vi. Descripción general de la cuenta (que hace la cuenta y para que se usa).
   vii. Vigencia de la contraseña de la cuenta (Cada cuanto debe cambiarse).

l) La Oficina de Tecnologías de la Información y Comunicaciones será la encargada de aprobar la asignación de acceso privilegiado a usuarios a los sistemas de información y aplicativos, teniendo en cuenta los siguientes lineamientos:

i. Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
ii. Asignar los privilegios a servidores (as) públicos (as) y contratistas sobre el principio del mínimo privilegio, es decir, el requerimiento mínimo para su rol funcional.
iii. Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
iv. Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

m) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar mecanismos que permitan verificar la identidad de un usuario antes de reemplazar la información secreta para la autenticación o proporcionar una nueva o temporal.
n) Las contraseñas para autenticación se deben suministrar de manera segura y los sistemas deben solicitar el cambio inmediato de la misma al ingresar.
o) Las contraseñas por defecto, presentes en los diferentes dispositivos adquiridos por la entidad, deben ser cambiadas de manera inmediata y previa a su conexión a la red por contraseñas seguras, siguiendo los lineamientos del numeral 9.6.3.

9.6.3. Responsabilidades de los Usuarios para el Uso de Contraseñas.

a) Todas las personas a quienes se les ha otorgado una cuenta de usuario deberán cambiar la contraseña temporal asignada por la Oficina TIC para el acceso a los sistemas de información y demás servicios de red cuando ingresan por primera vez.
b) Para el cambio de contraseña, se debe seguir las siguientes recomendaciones:
i. Contener mínimo 8 caracteres alfanuméricos, incluyendo minúsculas, mayúsculas y caracteres especiales.
ii. No contener datos personales o de identificación que puedan ser obtenidos por otra persona, como nombres, números de cedula, pasaporte, fechas de cumpleaños, números de teléfono, fechas de nacimiento, entre otros.

iii. Ser diferente a las ultimas 5 suministradas al directorio activo o ultimas 5 empleadas.
iv. Deben cambiarse al menos cada 180 días.
v. Debe cambiarse inmediatamente cuando se detecte una anomalía en la cuenta y notificar a la Mesa de servicios, siguiendo los lineamientos de la política 9.16 Gestión de incidentes de seguridad y privacidad de la información.
vi. Mantener las contraseñas en secreto y no compartir con otras personas.
vii. No se debe almacenar contraseñas en los procesos de inicio de sesión.

c) Se debe evitar almacenar las contraseñas en un papel, archivo de texto plano u otro medio que pueda ser accedido por otra persona, a menos que se pueda almacenar en forma segura como un gestor de contraseñas o cifrando el archivo.

9.6.4. Acceso a Sistemas y Aplicaciones.

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar mecanismos de identificación de usuarios para el acceso a los sistemas de información, dispositivos de móviles y sistemas de comunicación.
b) Si otra Entidad, empresa o personal externo requiere acceso a información sensible o crítica, La UAESP debe implementar los controles necesarios y suscribir acuerdos de confidencialidad o de no divulgación, cuando sea necesario, para salvaguardar la información y cumplir con la normatividad vigente asociada.
c) La Oficina de Tecnologías de la Información y Comunicaciones deberá implementar los controles que permitan:
   i. Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación.
   ii. Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
   iii. Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.

iv. Limitar la información contenida en los elementos de salida.
v. Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

d) La Oficina de Tecnologías de la Información y Comunicaciones debe configurar el directorio activo para que se bloquee el acceso cuando se ingrese cinco veces seguidas la contraseña de forma errónea. Cuando la contraseña no pueda ser cambiada por el mismo titular de la cuenta, este deberá reportar y solicitar el cambio por medio de la Mesa de servicios y está validará la identificación del solicitante por medio de los mecanismos necesarios para ello.

e) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar los mecanismos necesarios que permitan:

i. Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.
ii. Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder al servicio o al servidor.
iii. Evitar dar mensajes de servicios que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
iv. Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
v. Limitar el número de intentos de conexión no exitosos permitidos.
vi. Registrar los intentos no exitosos.
vii. Impedir otros intentos de identificación, una vez superado el límite permitido.
viii. Desconectar conexiones de comunicaciones de datos.
ix. Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.

f) Los registros de auditoría o logs de los sistemas y aplicaciones deberán incluir:

i. Identificación del usuario.
ii. Fecha y hora de inicio y terminación.
iii. Identidad de la terminal (por dirección IP pública).

iv. Registros de intentos exitosos y fallidos de acceso al sistema.
v. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.
vi. Cambios en las configuraciones de los sistemas y aplicativos más importantes.
vii. Cambios de privilegios de acceso.
viii. Aproximación a los límites de uso de los recursos físicos de hardware cuando sea necesario.
ix. Los logs o registros de eventos deben almacenarse y ser incluidos en la política de back ups de la entidad para poderla recuperar en caso de pérdida.
x. Cualquier otro que se considere pertinente

g) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar mecanismos que permitan a los sistemas de administración de contraseñas:
i. El uso individual de contraseñas.
ii. Permitir al usuario el cambio de su contraseña.
iii. Exigir contraseñas de seguridad.
iv. Para cuentas administrativas incluir mínimo 13 caracteres y doble factor de autenticación en los sistemas que lo permitan.
v. Exigir el cambio de contraseña cuando se ingresa por primera vez.
vi. Impedir el reúso de contraseñas de acuerdo con los lineamientos 9.6.3 Responsabilidades de los Usuarios.
vii. Implementar mecanismos de captcha en los sistemas o aplicaciones que lo permitan.

h) Se prohíbe el uso o instalación de programas utilitarios privilegiados capaces de invalidar o evadir los controles de los sistemas y aplicaciones, excepto los aprobados por la Oficina TIC

i) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar los mecanismos necesarios para controlar los utilitarios capaces de invalidar o evadir los controles de los sistemas y aplicaciones, que incluyan:
i. Utilizar procedimientos de autenticación para utilitarios del sistema.
ii. Separar entre utilitarios del sistema y software de aplicaciones.

iii. Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.

iv. Evitar que personas ajenas a la UAESP tomen conocimiento de la existencia y modo de uso de los utilitarios empleados.

v. Mantener un registro actualizado de los programas utilitarios privilegiados autorizados para su uso.

vi. Definir los niveles de autorización para utilitarios del sistema.

vii. Remover todo el software basado en utilitarios y software de sistema no autorizados.

j) El acceso al código fuente de los programas de la Entidad debe estar limitado solamente a los desarrolladores y personal de soporte autorizados por la Oficina TIC.

k) La Oficina de Tecnologías de la Información y Comunicaciones debe establecer un procedimiento y controles de acceso a los ambientes de desarrollo y producción; así mismo, debe limitar y controlar el acceso a datos o información que se encuentre en los ambientes de producción.

l) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar controles para asegurar que:

i. Las librerías de fuentes de programas no se deben mantener en los sistemas operativos.

ii. Gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos;

iii. La actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada.

iv. Establecer que los listados de programas y códigos fuente se deben mantener en un entorno seguro.

v. Conservar un registro de auditoría de todos los accesos a las librerías y códigos fuentes de programas.

vi. Mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.

vii. Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la UAESP.

9.7. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

9.7.1. Áreas Seguras

Directrices:

a) La Subdirección Administrativa y Financiera de la Unidad Administrativa Especial de Servicios Públicos, deberá establecer perímetros de seguridad para controlar el acceso físico a las instalaciones de la Entidad, Data Center, suministro de energía y otras áreas seguras, si las hubiere, teniendo en cuenta las normas de seguridad y salud en el trabajo.

b) La Entidad deberá implementar los sistemas de monitoreo y vigilancia que considere pertinentes, para el ingreso a las instalaciones y áreas seguras de la Unidad.

c) El emplazamiento y fortaleza de cada perímetro o control será definido por la Subdirección Administrativa y Financiera junto con el responsable del activo de información y el asesoramiento del Oficial de seguridad de la información, o el que haga sus veces, de acuerdo con una evaluación de riesgos.

d) La Subdirección Administrativa y Financiera deberá garantizar que todos los puntos de acceso o entradas a la Entidad, en todas sus sedes, cuenten con vigilancia o controles que permitan el acceso físico únicamente a personal autorizado.

e) La Subdirección Administrativa y Financiera junto con el Oficial de seguridad de la información, o quien haga sus veces, deben establecer controles de acceso físico como el registro, incluyendo fecha y hora, de ingreso y salida de todo visitante, y establecerá los mecanismos necesarios para inspeccionar y examinar los bolsos, bolsas, morrales, cajas y otros paquetes que ingresen a la Entidad. El registro de ingreso y salida deberá atender los lineamientos normativos en tratamiento y protección de datos personales.

f) Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyendo al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
g) La Subdirección Administrativa y Financiera deberá establecer el protocolo o procedimiento para las autorizaciones de ingreso a las instalaciones de la Entidad.
h) La Subdirección Administrativa y Financiera junto con los responsables de los activos de información definirán la necesidad de llevar un registro de ingreso en las áreas seguras respectivas.
i) Todo material que ingrese a las instalaciones de la Entidad debe ser inspeccionado para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga.
j) Siempre que sea posible, las áreas para despacho y recepción de material deben estar físicamente separadas.
k) Se debe inspeccionar todo material que ingrese para determinar evidencia de manipulación. En caso de manipulación, informar al personal de seguridad, proveedor, o a quien corresponda.
l) Las instalaciones de procesamiento de información, como el Data Center y otras áreas seguras, deben estar separadas físicamente del acceso por parte de la ciudadanía y de las gestionadas por personal externo a la Entidad, si las hubiera.
m) La Subdirección Administrativa y Financiera asegurará que toda instalación de procesamiento debe ser físicamente segura realizando las adecuaciones necesarias para ello, evitando una irrupción o situación de riesgo de factor ambiental.
n) Cuando sea necesario, el acceso al Data Center por parte de un tercero solo podrá ser autorizado por el jefe de la Oficina TIC, o a quien este delegue, y deberá contar con acompañamiento durante el tiempo que permanezca en las instalaciones.
o) El personal de aseo y mantenimiento en el Data Center debe contar con el acompañamiento del personal designado o autorizado de la Oficina TIC.
p) La Subdirección Administrativa y Financiera deberá mantener en buen estado la infraestructura física del Data Center y centros de cableado, como puertas, ventanas, paredes, techos, pisos, entre otros.

q) Los sitios donde se realicen actividades de procesamiento de información deberán ser discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

r) Todo el personal que transite dentro de las instalaciones de la entidad, en cualquiera de sus sedes, deberán portar el carné que lo identifica como servidor (a) público (a) o contratista de la Entidad. Los(as) visitantes deberán portar la identificación asignada en un lugar visible o estar acompañados por una persona del proceso que autorice su ingreso.

s) Se debe evitar realizar trabajos, por parte de terceros o proveedores, en áreas seguras sin supervisión o sin ser monitoreados por razones de seguridad. En caso de ser monitoreados por medio de circuitos cerrados de televisión o CCTV, las cámaras no deberán apuntar directamente a la captura de información de estas áreas.

t) Las puertas y ventanas de áreas seguras permanecerán cerradas cuando no haya supervisión o vigilancia.

u) Se debe evitar que las actividades o la información confidencial sea visible o audible desde el exterior.

v) Cuando sea necesario el almacenamiento de materiales y residuos peligrosos debe realizarse a una distancia prudencial de las áreas seguras de la Entidad.

w) No se permite tomar fotos o videos dentro de las instalaciones en áreas seguras sin la debida autorización por parte del líder de proceso, a excepción de las funciones propias del cargo u obligaciones contractuales.

x) Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados. Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

   i. Limitar el acceso a las áreas de almacén, desde el exterior de la sede a la Entidad, sólo al personal previamente identificado y autorizado.

   ii. Establecer controles que permitan que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

iii. Las personas encargadas de recibir el material deben inspeccionarlo para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

iv. Registrar el material entrante en el aplicativo correspondiente.

9.7.2. Seguridad de Equipos Tecnológicos

Directrices:

a) La Subdirección Administrativa y Financiera con el apoyo del Oficial de seguridad de la información o la Oficina TIC propenderán por ubicar los equipos de cómputo e impresoras en sitios que reduzcan el riesgo contra amenazas ambientales, accesos no autorizados y visualizaciones de la información durante su uso.

b) La Subdirección Administrativa y Financiera con el apoyo del Oficial de seguridad de la información o la Oficina TIC implementaran los controles que permitan:

i. Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

ii. Minimizar el riesgo de amenazas físicas y ambientales como: Hurto, incendio, explosivos, humo, inundaciones, filtraciones de agua, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión), entre otros.

iii. Revisar regularmente los sistemas de monitoreo de condiciones ambientales (temperatura y humedad) de las áreas seguras para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento la información.

iv. Proteger contra descargas eléctricas atmosféricas.

c) Está prohibido el consumo de alimentos, bebidas o fumar en las áreas seguras o en instalaciones de procesamiento de información de la Entidad.

d) La Subdirección Administrativa y Financiera junto con la Oficina TIC deben implementar y mantener mecanismos, como el uso de planta eléctrica y sistemas de alimentación ininterrumpida (UPS), para regular el flujo de energía eléctrica en caso

de fallas en el suministro del servició público y propender por la continuidad del servicio y las operaciones.

e) La Subdirección Administrativa y Financiera con el apoyo de los procesos que correspondan, deberán asegurar el suministro de servicios de energía eléctrica, agua, gas, alcantarillado, ventilación, aire acondicionado, entre otros, de forma que cumplan con las disposiciones legales aplicables y requerimientos de la Entidad.
f) La Subdirección Administrativa y Financiera junto con la Oficina TIC deberán asegurar la protección del cableado eléctrico y de telecomunicaciones contra interceptaciones, interferencias o cualquier tipo de daño dentro de las instalaciones de la Entidad, adicional:
   i. Usar piso ducto o cableado embutido en la pared, siempre que sea posible cuando corresponda a las instalaciones de procesamiento de información.
   ii. Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.
   iii. Evitar trayectos que atraviesen áreas públicas.
g) Se debe procurar separar el cableado eléctrico y el de comunicaciones para evitar interferencias.
h) Para la instalación o modificaciones al cableado eléctrico se deberá tener en cuenta las consideraciones técnicas de las normas vigentes y el Reglamento Técnico de Instalaciones Eléctricas RETIE. En su última versión vigente o disponible.
i) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar mecanismos de soporte y mantenimiento de equipos de cómputo y demás elementos de la infraestructura tecnológica que lo requieran. De igual forma, deberá llevar registro de todas las fallas y acciones realizadas de los mantenimientos.
j) Solo el personal autorizado por la Oficina TIC puede llevar a cabo los mantenimientos y reparaciones a la infraestructura tecnológica de la Entidad.
k) Cuando un equipo de cómputo o dispositivo móvil deba ser retirado de la Entidad para realizar un mantenimiento, reparación, cambios por garantía u otros, el custodio o la Oficina TIC deberá verificar que estos elementos no contengan información pública clasificada o reservada, en caso de contener este tipo de

información se deberá realizar respaldo y un borrado seguro para evitar fugas de información.

l) Para el uso de equipos de cómputo o dispositivos móviles de la UAESP por fuera de sus instalaciones, se deben implementar los mecanismos de seguridad equivalente a la suministrada dentro de las instalaciones de la Entidad.

m) Para el uso de equipos de cómputo o dispositivos móviles de la UAESP se respetarán permanentemente las instrucciones del fabricante respecto del cuidado de los equipos. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera de las instalaciones de la UAESP, cuando sea pertinente.

n) Cuando un equipo de cómputo o dispositivo móvil sea reutilizado, la Oficina TIC debe implementar mecanismos de borrado seguro, incluyendo la destrucción física cuando sea dado de baja y así lo amerite, cumpliendo los lineamientos de la Subdirección Administrativa y Financiera para la disposición final de residuos de aparatos eléctricos y electrónicos – RAEE.

o) Cuando haya traslado, intercambio o movimientos de dispositivos móviles o medios removibles a otras entidades o terceros, se deben establecer controles para condiciones seguras de traslados y acuerdos enfocados a la transferencia segura de información entre las partes. Se debe tener en cuenta el registro de contenido, la protección aplicada y los responsables durante el transporte.

p) Es deber de todos (as) cerrar las sesiones activas al finalizar la jornada laboral y apagar el dispositivo o bloquear las sesiones al levantarse del puesto de trabajo. De igual manera se deben cerrar o salir de las aplicaciones o sistemas de información cuando no se necesiten.

q) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar mecanismos para proteger los equipos de cómputo o dispositivos móviles contra uso no autorizado, como el bloqueo de la sesión luego de cinco minutos de inactividad, monitoreo y sistemas de acceso por contraseña cuando no se encuentran en uso.

9.8. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Directrices:

a) Está prohibido guardar información en el escritorio del equipo de cómputo, para prevenir el acceso no autorizado. La ubicación para guardar la información dentro de los equipos de cómputo es la carpeta “Mis Documentos” o en la nube, de acuerdo con el proveedor de la herramienta autorizada por la Oficina TIC, cuando estén por fuera del dominio o de la Entidad.
b) Se debe almacenar bajo llave los documentos en papel y los medios de almacenamiento externos o extraíbles en gabinetes u otro tipo de mobiliario seguro, cuando contengan información sensible y no estén siendo utilizados, especialmente fuera del horario de trabajo.
c) Se prohíbe el uso de fotocopiadoras o escáneres no autorizados por la Entidad.
d) Se deben retirar inmediatamente los documentos que contengan información pública clasificada o pública reservada, una vez impresos.

9.9. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe establecer y documentar el proceso y controles criptográficos a implementar en los servicios que lo requieran.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe establecer e implementar herramientas y algoritmos de cifrado que se encuentren vigentes, de carácter abierto o legalmente adquiridos.
c) Mediante la evaluación de riesgos se identificará el nivel de protección requerido, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.
d) Al implementar la Política de la UAESP en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica.
e) Con base en el análisis de riesgos, los discos duros externos, memorias USB u otros dispositivos de almacenamiento removible asignados por la Entidad y que contengan información sensible, deben estar cifrados.

f) La Oficina de Tecnologías de la Información y Comunicaciones apoyará la transmisión de información a otra Entidad o tercero usando controles criptográficos a fin de garantizar la seguridad de la información cuando sea pertinente.

g) La Entidad asegura el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información. Por lo cual establece técnicas criptográficas y cifrado como son: Cifrado de la información cuando se requiere trasferir o almacenar información sensible y uso de protocolos seguros para comunicaciones y redes Wifi actualizados.

h) La Oficina de Tecnologías de la Información y Comunicaciones deberá aplicar controles criptográficos para la protección de claves de acceso a sistemas de información.

i) Los servidores(as) públicos(as) y contratistas a los que la Entidad les haya asignado una firma digital o token deben hacer buen uso de estos.

j) En caso de presentarse un incidente de seguridad de la información, como perdida, robo u otra afectación relacionada con el uso de las firmas digitales o tokens, se debe reportar inmediatamente por medio de la herramienta mesa de servicios y al jefe inmediato respectivo o el que haga sus veces.

k) El certificado asignado es personal e intransferible, por lo cual, es responsabilidad del servidor(a) público(a) o contratista los documentos que firme. Así mismo, el servidor(a) público(a) o contratistas son responsables de salvaguardar los certificados, claves y tokens asignados.

l) La Oficina de Tecnologías de la Información y Comunicaciones definirá y documentará los lineamientos para la generación de claves criptográficas que incluya:

i. Generar claves robustas para sistemas criptográficos y aplicaciones.
ii. Generar y obtener certificados de clave pública de manera segura.
iii. Distribuir claves de forma segura a los usuarios que corresponda, incluyendo Información sobre cómo deben activarse cuando se reciban.
iv. Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.

v. Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse.

vi. Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo, cuando las claves están comprometidas o cuando un usuario se desvincula de la Unidad.

vii. Reponer claves pérdidas o alteradas como parte de la administración de la Continuidad de Operaciones de la UAESP, por ejemplo, para la recuperación de la información cifrada.

viii. Designar un responsable encargado de archivar, respaldar y destruir claves.

ix. Registrar y auditar las actividades relativas a la gestión de claves.

9.10. SEGURIDAD EN LAS OPERACIONES

9.10.1. Procedimientos y Responsabilidades Operacionales.

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones es la encargada de la operación y administración de los recursos tecnológicos que soportan la operación de la Entidad, por ello, deberá documentar y mantener actualizados los procedimientos operacionales a nivel de Tecnologías de la Información (TI) para reducir riesgos asociados a la seguridad de la información y ponerlos a disposición de toda la Entidad.

b) La Oficina de Tecnologías de la Información y Comunicaciones debe establecer, documentar y mantener actualizado un procedimiento para la gestión de cambios significativos a nivel de infraestructura, sistemas de información y otros servicios tecnológicos, que permitan gestionarlos de forma oportuna, adecuada y evaluando los posibles impactos o riesgos en seguridad de la información. El procedimiento debe incluir la recuperación de cambios no exitosos y eventos fallidos.

c) La infraestructura tecnológica de la Entidad deberá estar configurada de acuerdo con los estándares y buenas prácticas de seguridad establecidas (Hardening o Endurecimiento).

d) La Oficina de Tecnologías de la Información y Comunicaciones debe revisar que los equipos personales de los servidores (as) públicos (as) o contratistas que se conecten a la red interna de la Entidad cumplan con todos los requerimientos y controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.

e) El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones o a quien él designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la Unidad para el período estipulado de vida útil de cada componente.

f) Los ambientes de desarrollo, prueba y producción, siempre que sea posible estarán separados y se definirán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo. Para ello, se tendrán en cuenta los siguientes controles:

   i. Ejecutar el software de desarrollo, de pruebas y de producción, en diferentes ambientes de operaciones, equipos, o directorios.

   ii. Separar las actividades de desarrollo, prueba y producción en entornos diferentes.

   iii. Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento de este.

   iv. Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

   v. Definir propietarios de la información para cada uno de los ambientes de procesamientos existentes.

g) El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.
h) Los cambios realizados sobre los sistemas de información deben ser probados en un ambiente diferente al de producción, garantizando la seguridad de la información y que se mantiene operativo el sistema.
i) No se debe copiar datos sensibles en el ambiente del sistema de desarrollo o pruebas, a menos que se suministren controles para asegurar la seguridad y privacidad de los datos.

9.10.2. Directrices Contra Código Malicioso.

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar soluciones que consideren necesarias que aseguren la protección de la información de posibles ataques internos y externos.
b) La Oficina de Tecnologías de la Información y Comunicaciones implementará las configuraciones necesarias para el escaneo y protección contra virus o programa maligno (malware) de toda la información procesada, almacenada y transmitida en estaciones de trabajo o equipos de cómputo portátil y servidores físicos o virtuales.
c) La Oficina de Tecnologías de la Información y Comunicaciones documentará el procedimiento para la gestión de antivirus con el fin de proteger la red y estaciones de trabajo contra virus o cualquier código malicioso.
d) Está prohibido el evadir, modificar, desactivar o eliminar los elementos de seguridad instalados o configurados en los equipos o sistemas de información asignados para el cumplimiento de sus funciones u obligaciones contractuales que estén bajo su custodia, sin autorización o conocimiento de la Oficina TIC.
e) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar controles que permitan estar al día con las ultimas actualizaciones de seguridad disponibles correspondientes del software antivirus y demás herramientas o

sistemas de información con el fin de proteger los equipos de la Entidad contra código malicioso y posibles ataques cibernéticos.

f) Es responsabilidad de todos, escanear todo medio removible de almacenamiento cada vez que se conecte a un equipo de la Entidad, con las herramientas antivirus o antimalware licenciadas y suministradas por la Oficina TIC.

9.10.3. Registros y Supervisión.

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe sincronizar los relojes de los servidores con una única fuente de referencia de tiempo, con el fin de garantizar la exactitud de los registros de auditoría.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe disponer herramientas para generar, resguardar y revisar registros de auditoria o eventos relacionados con la seguridad en los sistemas de información críticos, elementos de red y aquellos que considere la Oficina TIC necesarios, que permitan identificar errores, intentos de acceso exitosos o fallidos, cambios realizados, uso de privilegios, direcciones, alarmas, otros indicadores para la gestión de incidentes y medidas correctivas a las que haya lugar.
c) Las auditorías a sistemas de información críticos de la entidad se deberán realizar limitando el acceso a estos y a los datos de solo lectura. En caso de requerir acceso diferente al de solo lectura se deberá acordar previamente con las personas quienes realicen la labor de auditoría e implementar controles como el borrado de datos o información una vez finalizada la auditoria para evitar fugas de información.
d) La Oficina de Tecnologías de la Información y Comunicaciones debe asegurar la protección de los registros de auditorías de sistemas de información y eventos ante cambios no autorizados y la capacidad de almacenamiento de estos. El tiempo de retención de los registros serán, al menos, de un año.

9.10.4. Control de Software.

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones es la única autorizada para la instalación o actualización de software, sistemas operativos y otros, asegurando que esta tarea se lleve a cabo por personal autorizado y capacitado.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe conservar la última versión estable del software como estrategia de contingencia ante la necesidad de un retroceso o rollback.
c) La Oficina de Tecnologías de la Información debe implementar controles para:
   i. Proteger todo el software y la documentación del sistema.
   ii. Guardar sólo los archivos de ejecución de los aplicativos en el ambiente de producción.
   iii. Llevar un registro de auditoría de las actualizaciones realizadas.

9.10.5. Gestión de Vulnerabilidades.

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones de realizar mínimo una vez al año una evaluación de vulnerabilidades a los sistemas de información críticos y misionales.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe restringir la instalación de software o aplicativos por parte de los usuarios finales.
c) La Oficina de Tecnologías de la Información y Comunicaciones debe probar los parches y valorar los riesgos asociados a su aplicación.
d) La Oficina de Tecnologías de la Información y Comunicaciones debe documentar y corregir las vulnerabilidades encontradas, aplicando las acciones correctivas necesarias para mitigar los hallazgos.
e) Solo está permitido el uso de software licenciado o libre que sea autorizado por la Oficina TIC.
f) Todo software o aplicaciones desarrolladas o adquiridas por la Entidad deben ser reportadas a la Oficina TIC para evaluar su compatibilidad técnica y análisis de posibles riesgos o vulnerabilidades que surjan de su uso.

g) La Oficina de Tecnologías de la Información y Comunicaciones debe recoger y analizar información sobre amenazas, bien sea de carácter estratégico u operacional, de fuentes internas o externas confiables que permitan identificar patrones o tendencias relevantes para la Entidad y ayuden a prevenir eventos no deseados.
h) La entidad debe promover el intercambio seguro y efectivo de información de inteligencia de amenazas con otras organizaciones y partes interesadas. Lo anterior, implica participar en foros de seguridad o grupos de inteligencia o de seguridad para intercambio de información y ayudar a crear una red de colaboración más completa del panorama de amenazas

9.10.6. Auditoria de Sistemas de Información.

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe definir, realizar y documentar auditorías a los sistemas de información críticos o misionales, contemplando su alcance y controlando las herramientas a utilizar, teniendo en cuenta el acceso a sistemas y datos.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe custodiar documentos, dispositivos y medios usados en las auditorias para protegerlos de accesos no autorizados y asegurar su disposición final.
c) Se debe procurar el desarrollo de auditorías en horario no laboral o aquel que no interfiera en la operación normal de la Entidad.

9.11. POLÍTICA DE BACKUPS

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar herramientas y mecanismos para la gestión de respaldos de la información de la Entidad.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe documentar e implementar los procedimientos y controles necesarios para el respaldo y

restauración de información de los equipos de cómputo, servidores, aplicaciones, bases de datos, sistemas de información o cualquier elemento de la infraestructura tecnológica que sea requerido por el responsable o custodio de la información.

c) La Oficina de Tecnologías de la Información y Comunicaciones debe almacenar los respaldos de información crítica en una ubicación remota, bien sea física o lógica, que permita minimizar el riesgo de pérdida de información por afectaciones a la ubicación del Data Center principal.

d) La Oficina de Tecnologías de la Información y Comunicaciones definirá los lineamientos para la frecuencia y cobertura de los respaldos de acuerdo con la criticidad de la información y análisis de riesgo.

e) La retención de los respaldos será, al menos, de 10 años para cuentas de Directivos (Director(a), Subdirectores, jefes de Oficina y asesores de Dirección) y 5 años para el resto de los usuarios, contados a partir de la fecha de su desvinculación con la Entidad.

f) La Oficina de Tecnologías de la Información y Comunicaciones asignará a la información de resguardo (Backups) un nivel de protección física y ambiental adecuado cuando el almacenamiento sea en la infraestructura propia de la Entidad. Se deben aplicar los mismos niveles de protección en las ubicaciones de respaldo alternas bajo las mismas condiciones del sitio principal.

g) La Oficina de Tecnologías de la Información y Comunicaciones debe realizar pruebas periódicas de restauración de forma que permita asegurar la disponibilidad e integridad de la información respaldada, al igual que probar la eficacia de los medios de resguardo.

h) Ningún servidor (a) público (a), contratista o tercero debe realizar copias de seguridad o respaldo en dispositivos de almacenamiento removibles u otros espacios de almacenamiento para evitar fugas de información, excepto en los casos autorizados por los líderes de proceso o jefe inmediato y para el cumplimiento propio de las funciones u obligaciones contractuales.

i) Se deberán utilizar los medios que la Oficina TIC disponga para realizar las copias de respaldos.

j) Los servidores (as) públicos (as) y contratistas son responsables de la información que reside en el equipo o dispositivo asignado y no deberá mantenerse información personal o fuera del ámbito laboral o contractual para respaldarse.

9.12. POLÍTICA DEL BUEN USO DEL INTERNET Y HERRAMIENTAS COLABORATIVAS

9.12.1. Buen Uso del Internet.

Directrices:

a) El uso del Internet estará limitado por la necesidad de acceso que se requiera en el desarrollo de las funciones u obligaciones contractuales.
b) El acceso a Internet será sólo de índole laboral y no personal, por lo cual está prohibido acceder a páginas web de entretenimiento para adultos (Páginas pornográficas) y cualquier otra a las cuales no haya sido autorizado.
c) Los equipos de cómputo de los visitantes podrán tener acceso a internet mediante conexión limitada o restringida a los sistemas de información, atendiendo las medidas o controles de seguridad establecidos por la Oficina TIC.
d) Los dispositivos móviles propios de servidores (as) públicos (as), contratistas y terceros podrán tener acceso a internet mediante conexión limitada o restringida a los sistemas de información, atendiendo las medidas o controles de seguridad establecidos por la Oficina TIC.
e) No se debe descargar o bajar ningún software y ejecutarlo, sin la debida autorización por parte de la Oficina TIC, ya que algunos pueden no tener licencia para su uso o pueden ocasionar daños a los sistemas o activos de información alojados en los equipos de cómputo o dispositivos móviles.
f) No se debe descargar archivos multimedia (audio, video e imágenes) o documentos de los cuales no se tengan licencias, con el fin de cumplir con disposiciones normativas en materia de derechos de autor, derechos conexos y reducir el riesgo por amenazas como virus o malware.
g) Solo podrá realizarse llamadas por Internet en cumplimiento de las funciones u obligaciones contractuales con la entidad.

h) Está prohibido realizar configuraciones o instalaciones de aplicativos o herramientas cuyo propósito sean saltar las medidas de seguridad dispuestas por la Entidad o puedan abrir puertas traseras (backdoor).
i) No se debe realizar compras a través de Internet, a no ser que este autorizado para ello en cumplimiento de sus funciones u obligaciones contractuales.
j) Todo equipo institucional con conexión a internet puede ser sometido a auditoria, por personal autorizado por la Entidad o en los casos que autorice la ley, con el fin de verificar el buen uso de este.
k) Toda actividad en línea de los usuarios (as) puede ser sometida a auditoría o revisión por la Oficina TIC, para asegurar que los servicios están siendo utilizados adecuadamente.
l) Es deber de todos, reportar cualquier uso indebido del internet a través de la mesa de servicios.
m) Todos los servicios de internet deben ser configurados para evitar que aplicaciones, protocolos o utilitarios no deseados estén siendo habilitados o redireccionados, en este sentido, la Oficina TIC es la encargada de administrar puertos y definir los servicios a los que se pueden acceder.
n) Si alguna dependencia, área, oficina o proceso, servidor (a) público (a) o contratista en ocasión de sus funciones u obligaciones contractuales necesita exponer servicios a internet, sobre redes públicas, o que se consuma algún tipo de servicio de la web se debe solicitar permiso ante la Oficina TIC por medio de la mesa de servicios.

9.12.2. Buen Uso del Correo electrónico y Herramientas Colaborativas.

Directrices:

a) El servicio de correo electrónico de la Entidad debe usarse única y exclusivamente para actividades relacionadas directamente con las funciones propias del cargo o ejecución de las obligaciones contractuales. Por lo anterior, el único correo electrónico autorizado para la transmisión de información institucional es el que cuenta con el dominio @uaesp.gov.co.

b) Toda la información almacenada, procesada o transmitida por correo electrónico y las herramientas colaborativas de la Entidad está sujeta a auditoría.
c) Los usuarios de correo electrónico no están autorizados a enviar información en forma masiva a múltiples direcciones de correo electrónico, ya que dicho comportamiento podría ser interpretado como correo “spam” y acarrear que terceros bloqueen el servicio de correo electrónico de la UAESP, salvo la Oficina de Comunicaciones y Relaciones Interinstitucionales y los casos autorizados en cumplimiento de las funciones u obligaciones contractuales. Cuando se requiera el envío de correo masivo se recomienda enviar con copia oculta a los destinatarios.
d) Ningún usuario (a) de correo electrónico debe modificar, falsificar o eliminar cualquier información que aparezca en cualquier lugar de un mensaje de correo electrónico, incluyendo el cuerpo del mensaje o encabezado.
e) Las comunicaciones oficiales solo están autorizadas por las herramientas de mensajería y colaborativas que disponga la Entidad para ello.
f) Salvo que exista una autorización de la Oficina TIC, ningún servidor (a) público (a) o contratista está autorizado para interceptar, revelar o contribuir en la intercepción de mensajes de correo electrónico a través de herramientas de escaneo.
g) Los usuarios del servicio del correo electrónico de la UAESP no deben abrir, responder o reenviar mensajes SPAM, con el fin de reducir el riesgo de materialización de una amenaza.
h) En caso de recibir correos sospechosos o de dudosa procedencia, deben abstenerse de abrirlos, descargarlos, reenviarlos y reportar inmediatamente a la Oficina TIC por medio de la herramienta mesa de servicios.
i) Está prohibido el uso del correo electrónico institucional o herramientas colaborativas para el envío de mensajes con contenido político, noticias falsas, cadenas de mensajería, mensajes con fines comerciales o mensajes vulgares u obscenos.
j) Es responsabilidad de todos, el adecuado manejo de las herramientas colaborativas asignadas, incluyendo los permisos y la información compartida con otras personas.

k) Todo e-mail saliente se le debe asociar un aviso o advertencia en términos de seguridad de la información y atendiendo la normatividad vigente.

9.13. POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES

9.13.1. Gestión de Seguridad en las Redes

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar y mantener una plataforma tecnológica que soporte los sistemas de información y servicios de red de la Entidad.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe establecer controles para el acceso a los servicios de red, tales como autenticación, encriptación y controles de conexión de red.
c) La Oficina de Tecnologías de la Información y Comunicaciones debe definir los lineamientos que considere necesarios para la utilización de los servicios de red.
d) La Oficina de Tecnologías de la Información debe definir controles para la transferencia de información a través de las aplicaciones de la UAESP que pasan sobre redes públicas, como el uso de firewall, IDS, IPS y cualquier otro que ayude a prevenir actividades fraudulentas, divulgación o modificaciones no autorizadas.
e) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar las conexiones remotas a la red de la Entidad mediante conexión VPN, mientras los recursos técnicos lo permitan, registrándola y monitoreándola.
f) La Oficina de Tecnologías de la Información y Comunicaciones debe segregar o segmentar las redes WIFI, de forma lógica o física, para asegurar los activos de información mediante la implementación de perímetros de seguridad acordes con la infraestructura tecnológica de la Entidad.
g) La Oficina de Tecnologías de la Información y Comunicaciones debe bloquear el acceso a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional mediante el uso de servidor proxy, firewall o la herramienta que mejor se ajuste a la necesidad.

h) El Oficial de Seguridad de la información o quien haga sus veces definirá y hará seguimiento a los controles necesarios para preservar la seguridad de los datos y los servicios conectados en las redes de la Entidad, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:
   i. Establecer los documentos para la administración de los equipos servidores, incluyendo los equipos en las áreas usuarias.
   ii. Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de Internet, y para proteger los sistemas conectados.
   iii. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
   iv. Asegurar mediante actividades de monitoreo o supervisión, que los controles se aplican en toda la infraestructura tecnológica.
i) La Oficina de Tecnologías de la Información y Comunicaciones debe restringir y monitorear los puertos físicos y lógicos de las plataformas que soporten los sistemas de información y de las redes de datos, a excepción de los estrictamente necesarios para su funcionamiento, con el fin de prevenir accesos no autorizados.
j) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar y actualizar la infraestructura tecnológica, incluyendo los protocolos de comunicaciones y cualquier medida de seguridad en concordancia a las buenas prácticas y lineamientos normativos para la gestión de las comunicaciones y la información.
k) Está prohibido la instalación de dispositivos de red que brinden acceso o conectividad a la red de datos y comunicaciones de la Entidad sin la debida autorización de la Oficina TIC.

9.13.2. Intercambio de Información

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones deberá brindar servicios o herramientas de intercambio de información seguras, como el correo

electrónico, mensajería electrónica o herramientas colaborativas, las cuales deben cumplir con requerimientos técnicos, legales y de seguridad para evitar accesos no autorizados, ataques informáticos y de códigos maliciosos. Así mismo, deberá implementar controles, como el cifrado de información, que permita proteger la información contra divulgación o modificaciones no autorizadas.

b) La Oficina de Tecnologías de la Información y Comunicaciones debe definir los lineamientos y controles que consideren necesarios para el uso adecuado de las instalaciones de comunicaciones.
c) La Oficina de Tecnologías de la Información y Comunicaciones debe asegurar el direccionamiento y transporte correcto de los mensajes, disponibilidad y no repudio en los servicios o herramientas de intercambio de información.
d) La Oficina de Tecnologías de la Información y Comunicaciones debe definir niveles de autenticación fuertes para el control de acceso desde redes públicas.
e) La subdirección Administrativa y Financiera - Gestión documental, debe definir directrices sobre la retención, disposición y transferencia de la información física de la Entidad, de acuerdo con las tablas de retención documental, TRD.
f) Se deben implementar controles criptográficos para la transferencia de información electrónica protegiendo la confidencialidad, integridad y disponibilidad de la información. Lo anterior se realizará con la observancia de la normatividad vigente en materia de protección de datos personales y Ley de Habeas Data.
g) Está prohibida la divulgación no autorizada de la información propiedad de la Unidad Administrativa Especial de Servicios Públicos.
h) Cuando se establezcan proyectos de interoperabilidad o intercambio de información con entes externos, se deberá suscribir acuerdos de confidencialidad o no divulgación con el fin de proteger los activos de información para la Entidad. Estos acuerdos de confidencialidad deberán contemplar lo siguiente:
    i. Responsabilidades de las partes para evitar la divulgación no autorizada de la información y el uso de esta.
    ii. Mantener la confidencialidad de los activos de información aun después de finalizado los acuerdos de interoperabilidad o intercambio de información.

iii. Establecer las actividades requeridas cuando termina el acuerdo.

iv. Propiedad de los activos de información, propiedad intelectual y términos y condiciones de la licencia bajo la cual se suministra el software, cuando sea necesario.

v. Actividades de auditoría.

vi. Proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial.

vii. Tiempos para la devolución de los activos o destrucción de estos, cuando aplique.

viii. Responsabilidades y obligaciones en caso de incumplimiento del acuerdo.

9.14. POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

9.14.1. Requisitos de Seguridad de los Sistemas de Información.

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe definir y documentar el proceso para la solicitud de nuevos sistemas de información y modificaciones a los existentes, donde se contemple los requisitos, análisis e implementación de criterios de seguridad de la información, tales como:

   i. Suministrar el acceso y autorización para usuarios de la Entidad, usuarios con privilegios o administradores funcionales.

   ii. Informar a los usuarios y operadores sobre sus deberes y responsabilidades.

   iii. Exigir otros controles de seguridad, como, registro de transacciones, seguimiento, protección de la confidencialidad, integridad, disponibilidad, no repudio y otros que apliquen en materia de seguridad de la información.

b) La Oficina de Tecnologías de la Información debe definir controles de acceso y autenticación para la transferencia de información a través de redes públicas para las aplicaciones de la Entidad

c) La Oficina de Tecnologías de la Información debe realizar y documentar análisis de amenazas y vulnerabilidades de los sistemas de información de la Entidad.

d) La Oficina de Tecnologías de la Información debe establecer controles para realizar transferencias completas, sin alteraciones, visualizaciones no autorizadas de la información en los servicios o aplicativos de la Entidad que contemplen:
   i. Mantener la privacidad asociada a las partes involucradas.
   ii. Cifrar las comunicaciones cuando sea necesario, usando protocolos seguros, en conformidad con la Política 9.13 Seguridad en las comunicaciones.
   iii. Asegurar el almacenamiento de los detalles de transacción de información o auditorias estén fuera de cualquier entorno accesible públicamente.
e) Cuando una aplicación tenga previsto el envío de mensajes que contengan información Pública Clasificada o Reservada, se implementarán los controles determinados en el punto “Controles Criptográficos”.

9.14.2. Seguridad en el desarrollo y soporte de sistemas de información

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe asegurar que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos de seguridad que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo se identifican y gestionan los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe definir mecanismos para asegurar:
   i. Solicitudes por parte de usuarios autorizados.
   ii. Niveles de autorización de cambios.
   iii. Presentación de los cambios a los usuarios autorizados.
   iv. Revisar la integridad de los cambios.
   v. Aceptación de los cambios por parte de los usuarios autorizados.
   vi. Control de versiones y resguardo de estas.
   vii. Documentar los cambios y mantenimientos posteriores.

viii. Implementar los cambios aprobados en momentos adecuados y que no afecten los procesos de la Entidad.

c) La Oficina de Tecnologías de la Información y Comunicaciones debe resguardar en un repositorio las versiones de todos los sistemas de información.

d) La Oficina de Tecnologías de la Información y Comunicaciones debe exigir la documentación relacionada con el código fuente para los desarrollos propios y para los casos en que la Entidad adquiera el sistema de información a un proveedor externo, según las obligaciones del contrato.

e) En caso de considerarlo necesario, la modificación de paquetes de software suministrados por proveedores, y previa autorización del responsable de la Oficina de Tecnologías de la Información y las Comunicaciones, se deberá:

i. Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

ii. Realizar el análisis del riesgo e impacto frente a la modificación.

iii. Consentimiento del proveedor en los casos que sea necesario.

iv. Determinar la conveniencia de que la modificación sea efectuada por la Entidad, por el proveedor o por un tercero.

v. Evaluar el impacto que se produce si la UAESP se hace cargo del mantenimiento.

vi. Resguardar el paquete de software original realizando los cambios sobre una copia perfectamente identificada.

f) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar ambientes de desarrollo seguro, teniendo en cuenta:

i. El carácter de datos sensibles que el sistema va a procesar.

ii. Requerimientos externos e internos como normativas, buenas prácticas o políticas

iii. Controles de seguridad definidos en la Entidad.

iv. Separación y control de acceso a los ambientes de desarrollo

v. Seguimiento de los cambios en el ambiente y los códigos almacenados allí.

vi. Control sobre el movimiento de datos desde y hacia el ambiente.

g) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar controles para el desarrollo externo de sistemas de información o aplicativos, que contemplen:
   i. Acuerdos de licencias, propiedad de código fuente y derechos conferidos (Derechos de Propiedad Intelectual).
   ii. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
   iii. Documentos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorias, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, cumplimiento de tratamiento de datos personales, entre otros.
   iv. Verificación del cumplimiento de las condiciones de seguridad contempladas en el numeral 7.9.2, cuando aplique.
   v. Acuerdos de custodia de las fuentes del software, y cualquier otra información requerida, en caso de considerarse necesario.

h) La Oficina de Tecnologías de la Información y Comunicaciones debe realizar pruebas funcionales y de seguridad, a todos los sistemas de información actualizados, modificados y desarrollados interna o externamente, simulando condiciones reales de operación y buscando la aceptación del usuario antes de lanzarlo al entorno operativo.

i) Los cambios realizados sobre los sistemas de información deben ser probados en un ambiente separado, garantizando la seguridad de la información y que se mantiene operativo el sistema.

j) El grupo de desarrollo debe solicitar autorización al grupo de gestión de cambios de la Oficina TIC, al jefe de la Oficina TIC o quienes hagan sus veces, para realizar los despliegues en los ambientes de producción.

k) Los administradores funcionales de los aplicativos deben validar periódicamente la autorización de usuarios en los aplicativos y se asegure que los privilegios no han sido modificados.

l) La Oficina de Tecnologías de la Información y Comunicaciones debe definir lineamientos para bloquear cuentas luego de 5 intentos fallidos de acceso.

m) La Oficina de Tecnologías de la Información y Comunicaciones debe definir lineamientos basados en la criticidad de los sistemas de información para cerrar sesiones cuando se detecte tiempos de inactividad.

9.14.3. Datos de Prueba

Directrices:

a) Los desarrolladores y la Oficina de TIC deben evitar usar datos que contengan información personal o sensible durante la ejecución de pruebas. En caso de requerir copia de la base operativa que contiene información sensible se debe:

i. Solicitar autorización formal por parte del custodio del activo de información, a través de correo electrónico, especificando el tiempo aproximado de las pruebas y su finalidad.

ii. El custodio del activo de información solicita, a través del correo electrónico, el visto bueno del Oficial de Datos Personales para el acceso a la base de datos que contiene información sensible.

iii. El custodio del activo de información dará la respuesta negativa o positiva al solicitante, especificando los controles de acceso o de seguridad que se deberán mantener para evitar fugas de información o violación a la Política de Tratamiento de Datos Personales de acuerdo con la clasificación del activo, de igual manera, se deberá solicitar borrar o eliminar la copia de base de datos suministrada una vez finalizada las pruebas respectivas.

iv. Suministrar la copia de las bases de datos por los medios apropiados de acuerdo con su clasificación.

v. El solicitante o desarrollador debe borrar del ambiente de pruebas la copia de la base de datos o información operacional que se haya usado e informar al custodio del activo de información.

vi. El custodio del activo de información informará mediante correo electrónico al Oficial de Datos Personales la finalización de las pruebas y controles aplicados.

b) La Oficina de Tecnologías de la Información y Comunicaciones debe establecer controles de acceso a los ambientes de desarrollo, pruebas y producción.

9.15. POLÍTICA DE RELACIÓN CON PROVEEDORES

Directrices:

a) La Subdirección de Asuntos Legales deberá verificar la inclusión en las obligaciones contractuales o en el mecanismo que consideren necesario, con terceros o proveedores, el cumplimiento de las obligaciones contractuales relacionadas con seguridad y privacidad de la información, entre las cuales se debe contemplar:
   i. Cumplimiento de la normatividad vigente en relación con seguridad de la información y protección de datos personales.
   ii. Atender las auditarías programadas por la entidad con la finalidad de verificar el cumplimiento de los requisitos vigentes referentes a la seguridad y privacidad de la información.
   iii. Realizar transferencia de conocimiento sobre la administración y uso de los bienes o servicios adquiridos, donde se incluya la entrega de la documentación soporte, manuales y relación de links para descarga de la información pertinente.
   iv. Identificar, notificar, investigar y presentar informes al supervisor del contrato cuando se presenten incidentes de seguridad de la información en el menor tiempo posible, cuando sean de su responsabilidad.
   v. Realizar el análisis o evaluación de riesgos asociados a la cadena de suministros.
   vi. Verificación periódica del cumplimiento de los acuerdos de nivel de servicio (ANS-SLA) relacionados con la seguridad y privacidad de la información.
   vii. Los proveedores críticos de tecnología deben contar con planes de continuidad de negocio y recuperación de desastres definidos e implementados, para responder ante eventuales escenarios que afecten los activos de información de la Entidad.
c) En ningún caso se debe otorgar acceso a proveedores o terceros a la información, las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto

se hayan implementado los controles apropiados y se establezcan los acuerdos que definan las condiciones para la conexión o el acceso.

d) La Oficina de Tecnologías de la Información y Comunicaciones junto con el propietario del activo de información deben implementar controles y permisos cuando un proveedor o tercero requiera tener acceso a la información por medio de la infraestructura tecnológica de la Entidad, teniendo en cuenta:
   i. Acceso requerido (Físico / Lógico).
   ii. Permisos mínimos necesarios.
   iii. Tiempos de acceso para revocación de permisos, en concordancia con los lineamientos de la Política 7.6 Control de acceso.
   iv. Motivo del acceso.
   v. Valor o Criticidad de la información.
   vi. Controles empleados por el proveedor o tercero.
   vii. Riesgos del acceso a la seguridad y privacidad de la información de la Entidad.
   viii. Protección contra software malicioso
   ix. El cumplimiento de la protección especial e integra establecida en la ley de datos personales vigente.
   x. Los cambios realizados por proveedores de servicios críticos de TI deben realizarse mediante un procedimiento formal de gestión de cambios establecido por la Entidad.

9.16. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones deberá documentar e implementar un procedimiento de gestión de incidentes de seguridad de la información, en el cual se contemple el reporte, la identificación, análisis, valoración, tratamiento y comunicación.
b) La Oficina de Tecnologías de la Información y Comunicaciones debe comunicar todos los reportes de incidentes de seguridad de la información al Oficial de

seguridad de la información para iniciar las acciones de tratamiento, investigación y monitoreo.

c) Es deber de todos los servidores (as) públicos (as), contratistas o terceros, reportar cualquier posible incidente, violaciones de acceso o acceso no autorizado y mal funcionamiento en el software o hardware del que se tenga conocimiento o experiencia directa, a través de la mesa de servicios.

d) Está prohibido la realización de pruebas y el uso de herramientas, tales como sniffers, analizadores de protocolos y puertos, entre otros, para detectar, verificar, explorar, validar o confirmar cualquier posible vulnerabilidad o falla de seguridad sin la debida autorización por parte del Oficial de Seguridad de la Información o el Jefe de la Oficina TIC.

e) La Oficina de Tecnologías de la Información y Comunicaciones debe reportar a las autoridades competentes los incidentes de seguridad de información graves o los que afecten a la infraestructura de la Entidad, a través de los canales de gestión apropiados.

f) La Oficina de Tecnologías de la Información y Comunicaciones debe documentar y comunicar, por los medios que considere necesario, las lecciones aprendidas de incidentes de seguridad de la información, con el fin de evitar recurrencias y usar la información para reforzar las capacitaciones y sensibilizaciones en relación con la seguridad y privacidad de la información.

g) La Oficina de Tecnologías de la Información y Comunicaciones, el Oficial de Seguridad de la Información o el que haga sus veces, deberá evaluar y actualizar los planes de tratamiento de incidentes de acuerdo con las lecciones aprendidas.

h) La Oficina de Tecnologías de la Información y Comunicaciones y el Oficial de seguridad de la información son los encargados para la recolección de evidencias de los incidentes de seguridad de información con el fin de presentar a las autoridades competentes en las investigaciones que sean necesarias.

i) La Oficina de Tecnologías de la Información y Comunicaciones, el Oficial de seguridad de la información o el que haga sus veces, deberá registrar y dar cierre

formal a los incidentes de seguridad, una vez gestionados, por el mismo medio en que fue reportado.

j) La Oficina de Tecnologías de la Información y Comunicaciones deberá monitorear e investigar las alertas y notificaciones de los sistemas de información e infraestructura tecnológica.

k) La Oficina de Tecnologías de la Información y Comunicaciones deberá poner en conocimiento a los responsables de los activos de información cuando se detecten irregularidades, incidentes o prácticas que atente contra la seguridad y privacidad de la información.

l) El Oficial de seguridad de la información deberá presentar un informe periódico sobre la gestión de incidentes a la mesa técnica de seguridad digital, o quien haga sus veces, para ser presentado al Comité institucional de gestión y Desempeño.

m) Los resultados de las investigaciones que involucren posible intencionalidad de servidores públicos, contratistas o terceros, deberán ser informados a las autoridades competentes.

n) La Oficina de Tecnologías de la Información y Comunicaciones podrá revocar o deshabilitar permisos de acceso a sistemas de información, a la infraestructura tecnológica de la Entidad o interrumpir los servicios de forma temporal, en respuesta a incidentes de seguridad graves, sin previo aviso.

o) La Oficina de Tecnologías de la Información y Comunicaciones establecerá un plan de continuidad de los servicios críticos de TI, para gestionar los incidentes durante o después de la materialización de un incidente de seguridad de la información.

9.17. POLÍTICA DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

9.17.1. Cumplimiento de Requisitos legales y Contractuales

Directrices:

a) La Oficina Asesora de Planeación, con el apoyo del responsable de seguridad de la información y los líderes de procesos, deberán diseñar y actualizar una metodología para la identificación de riesgos de seguridad y privacidad de la información para la

continuidad de la operación de los servicios de la Unidad Administrativa Especial de Servicios Públicos. – UAESP.

b) La Oficina Asesora de Planeación, con el apoyo del Oficial de seguridad de la información y los líderes de procesos, deberá identificar y priorizar los servicios críticos de la Entidad.
c) La Oficina Asesora de Planeación, con el apoyo del Oficial de seguridad de la información y los líderes de procesos, debe diseñar las estrategias y tiempos definidos para la recuperación de la operación de los servicios críticos de la Entidad.
d) La Oficina Asesora de Planeación, con el apoyo del Oficial de seguridad de la información y los líderes de procesos, deberá elaborar el plan de continuidad del negocio, incluyendo la definición de roles, responsabilidades y un plan de pruebas del mencionado plan.
e) La Oficina Asesora de Planeación debe presentar el plan de continuidad del negocio, y el plan de pruebas del plan de continuidad del negocio al comité institucional de gestión de desempeño para su aprobación.
f) La Oficina de Tecnologías de la Información y Comunicaciones debe establecer un plan de continuidad de servicios críticos de TI de la Entidad, que permita retornar a la operación normal ante un evento no deseado.
g) La Oficina Asesora de Planeación debe asegurar la integración de los planes de emergencia, contingencia y de continuidad de los servicios tecnológicos con el plan de contingencia y continuidad del negocio.
h) Las pólizas de seguros podrían formar parte del proceso de continuidad de operaciones de la UAESP de acuerdo con los servicios críticos de la Entidad.
i) La Oficina Asesora de Planeación debe comunicar el plan de continuidad del negocio al interior de la Entidad.
j) La Oficina Asesora de Planeación junto con el apoyo de los procesos de la Entidad deberán documentar las pruebas al plan de continuidad del negocio y generar reportes o informes para ser presentados al Comité Institucional de Gestión y Desempeño y realizar los ajustes o mejoras al plan de contingencia y continuidad del negocio, o el que haga sus veces.

9.17.2. Disponibilidad de Instalaciones de procesamiento de información

Directrices:

a) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar redundancia en la arquitectura tecnológica critica.
b) La Oficina de Tecnologías de la Información y Comunicaciones deben poner a prueba los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla los componentes funcionen adecuadamente e informar los resultados a la Oficina Asesora de Planeación.

9.18. POLÍTICA DE CUMPLIMIENTO DE REQUISITOS LEGALES

9.18.1. Cumplimiento de Requisitos Legales.

Directrices:

a) Todos los procesos de la Entidad deben identificar la normativa referente a seguridad y privacidad de la información que les competa, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, y remitirla a la Subdirección de Asuntos Legales con el objeto de consolidar y actualizar la información suministrada en la herramienta de verificación de requisitos legales.
b) La Subdirección de Asuntos Legales deberá definir y establecer un procedimiento y una herramienta de verificación de requisitos legales donde se contemple la normativa aplicable en materia de seguridad y privacidad de la información.
c) Todos los procesos de la Entidad deben identificar la normativa referente a seguridad y privacidad de la información que les competa, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, y remitirla a la Subdirección de Asuntos Legales con el objeto de consolidar y actualizar la información suministrada en la herramienta de verificación de requisitos legales.
d) Los supervisores de contrato junto con la Oficina de Tecnologías de la Información y Comunicaciones, implementará los mecanismos apropiados para asegurar el

cumplimiento de los requisitos normativos y contractuales que puedan afectar los sistemas de información o aplicativos de la Entidad.

e) La Oficina de Tecnologías de la Información y Comunicaciones establecerá los mecanismos que permitan proteger la propiedad intelectual de la Entidad, como los derechos de autor de software, licencias y códigos fuentes, con el apoyo de la Subdirección de Asuntos Legales, de considerarse necesario.

f) La Oficina de Tecnologías de la Información y Comunicaciones debe establecer lineamientos para evitar que los servidores (as) públicos (as) y contratistas realicen las acciones como; copiar, descargar, almacenar, transferir, reproducir o emplear material que no sea propiedad de la Entidad o aquel con el que no se cuente autorización de su propietario o autor. Entiéndase por material el software, imágenes, videos, audios, documentos, y cualquier otro elemento susceptible de estar patentado o registrado con derechos de autor.

g) Cuando se celebren contratos con personas naturales o jurídicas se debe establecer una cláusula donde se especifiquen que todos los productos, desarrollos, trabajos, investigaciones, entre otros, serán propiedad de la Entidad de acuerdo con el artículo 20 de la ley 23 de 1982, Modificado por el artículo 28, Ley 1450 de 2011.

h) La Oficina de Tecnologías de la Información y Comunicaciones debe implementar controles que permitan verificar que solo se instalen productos licenciados, revisando su vigencia y evitando exceder el número máximo de licencias adquiridas.

i) Ningún servidor (a) público (a), contratista o tercero está autorizado para instalar software sin licencias y distintos a los aprobados por la Oficina TIC en los dispositivos móviles y equipos de escritorio propiedad de la Entidad.

j) La Subdirección Administrativa y Financiera, junto con la Subdirección de Asuntos Legales y la Oficina TIC, debe establecer lineamientos para proteger los registros contra pérdida, destrucción y falsificación de información física y digital en cumplimiento con la normatividad legal vigente.

k) La Subdirección de Administrativa y Financiera, la Subdirección de Asuntos Legales, la Oficina TIC y con el apoyo Oficial de datos personales deben definir o actualizar,

cuando sea necesario, la política de tratamiento de datos personales en cumplimiento de las disposiciones normativas en la materia.

l) Los activos de información de la UAESP deberán ser utilizados de acuerdo con las funciones u obligaciones contractuales para los cuales fueron asignados. Toda utilización de estos activos por fuera de su alcance será considerada como un uso indebido o incumplimiento a las políticas descritas en el documento.

9.18.2. Revisión de Seguridad de la Información.

Directrices:

a) Los líderes de procesos deben velar por la correcta implementación y cumplimiento de las políticas, lineamientos, normas y procedimientos de seguridad y privacidad de la información dentro de sus respectivos procesos.
b) La Oficina de Tecnologías de la Información y Comunicaciones y el Oficial de Seguridad de la información realizarán revisiones necesarias de las áreas de la Entidad a efectos de verificar el cumplimiento de la política, normas y procedimientos de seguridad y privacidad de la información. Las revisiones pueden incluir:
   i. Equipos de cómputo.
   ii. Proveedores de servicios tecnológicos.
   iii. Propietarios de información.
   iv. Usuarios.
c) La Oficina de Tecnologías de la Información y Comunicaciones debe comprobar periódicamente que los sistemas de información cumplen con las normatividad vigente y buenas prácticas de seguridad y privacidad de la información. Se deberán realizar auditorías periódicas con servicios de herramientas automatizadas o con el apoyo de personal especializado y se deberán generar informes técnicos.
d) La Entidad deberá recolectar y resguardar las evidencias necesarias cuando sea requerida la judicialización o la aplicación de una ley, tanto civil como penal, para realizar la investigación respectiva, atendiendo las buenas prácticas de informática vigencia.

10. OBLIGACIONES

Los servidores (as) públicos (as), contratistas y terceros que accedan a los activos de información de la Unidad Administrativa Especial de Servicios públicos – UAESP, son responsables del manejo adecuado de la información utilizada en el desarrollo de sus actividades u obligaciones contractuales.

Los sujetos de aplicabilidad de esta política deberán cumplir con los lineamientos, requisitos y buenas prácticas legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad y privacidad de la información que adopte la entidad y que se encuentran en el Manual de Políticas de Seguridad y Privacidad de la Información, en su última versión, previniendo, detectando y reportando cualquier incidente, contravención u omisión de la política aquí descrita.

11. REVISIÓN

La Políticas de Seguridad y Privacidad de la Información serán revisada anualmente, o cuando se requieran, para mantenerlas oportunas, suficientes y eficaces.

El proceso de revisión será liderado por el Oficial de Seguridad de la Información, el Oficial de Protección de Datos Personales, la Oficina de Tecnologías de la Información y las Comunicaciones, de igual forma, la política será revisada y aprobada por el Comité Institucional de Gestión y Desempeño.

12. COMUNICACIÓN

La Unidad Administrativa Especial de Servicios Públicos UAESP establecerá los canales necesarios y accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI).

Algunos canales para la comunicación son: Correo Electrónico, intranet, comunicación impresa, charlas, sensibilizaciones y los demás que considere la Entidad para permitir la divulgación y acceso a la información relacionada con seguridad de la información.

13. ROLES Y RESPONSABILIDADES

13.1. ROLES

Para llevar a buen término el cumplimiento de las políticas y gestión de la seguridad y privacidad de la información, la Unidad Administrativa Especial de Servicios Públicos ha definido los siguientes roles:

Comité Institucional de Gestión y Desempeño – CIGD:

1. Orientar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:
    - Aprobación y seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información.
    - Promover la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.
2. Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

Jefe Oficina de Tecnologías de la Información y las Comunicaciones:

1. Asesorar a la Dirección General y dependencias de la Unidad en materia de Seguridad y privacidad de la Información.
2. Planear y administrar los recursos informáticos y de telecomunicaciones para satisfacer las necesidades y requerimientos de los usuarios de la UAESP, de conformidad con las políticas, metodologías y normatividad vigente.
3. Adoptar e implementar buenas prácticas o estándares informáticos, de calidad y de seguridad y privacidad de la información.
4. Apoyar y aprobar estudios, investigación y análisis de tendencias tecnológicas para su posible aplicación en la Entidad.
5. Apoyar en la formulación del plan de capacitación en relación con seguridad y privacidad de la información.

6. Asumir el rol del Oficial de Seguridad de la Información, en ausencia de la persona designada en la Entidad para este fin.

Oficial de Seguridad de la Información:

1. Apoyar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información de conformidad con la regulación vigente.
2. Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad.
3. Realizar la planificación y cronograma de la implementación del MSPI.
4. Proponer, definir, elaborar o acompañar en la implementación las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.
5. Brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
6. Liderar la implementación del procedimiento de Gestión de Incidentes de seguridad de la información en la entidad.
7. Verificar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a la alta dirección.
8. Convocar la participación de los servidores (as) públicos (as), contratistas o terceros cuando el incidente lo amerite.
9. Verificar el cumplimiento de los procedimientos y buenas prácticas en gestión de incidentes y recomendar, si lo amerita, la aplicación de planes de contingencia o continuidad.
10. Indagar todos los incidentes de seguridad de la información y apoyar el análisis forense, cuando se requiera.

Oficial de Datos Personales:

1. Consolidar y reportar la información de Base de datos personales que maneja o tiene la Entidad en conformidad con la normatividad vigente.

2. Fomentar la cultura de la protección y privacidad de datos personales que tiene a cargo la entidad y el cumplimiento de la normatividad aplicable.
3. Apoyar en la definición, implementación y seguimiento de los controles para el tratamiento de datos personales y privacidad de la información de acuerdo con la normatividad vigente.
4. Apoyar en la elaboración, comunicación y aplicación de la política de datos personales, con los criterios de calidad y oportunidad.
5. Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la SIC o entes externos en temas de su competencia.

Líderes de Proceso:

1. Velar por el cumplimiento de las políticas de seguridad y privacidad en temas de su competencia, en sus equipos de trabajos o personal a cargo.
2. Identificar e inventariar los nuevos activos de información y los riesgos de seguridad y privacidad de la información asociados.
3. Apoyar la gestión de riesgos de seguridad digital o de la información conforme a la Política de Administración de Riesgos o la que haga sus veces.
4. Reportar cualquier evento o riesgo materializado, por medio de los canales dispuesto para ello.

Usuarios:

1. Conocer y cumplir las Políticas de Seguridad y Privacidad de la Información y la normatividad vigente relacionada en el desarrollo de sus funciones u obligaciones contractuales.
2. Reportar cualquier evento de seguridad que atenten contra la confidencialidad, disponibilidad o integridad de la información o cuando se evidencie un incumplimiento de las Políticas de Seguridad y Privacidad de la Información.
3. Participar en las campañas de sensibilización del MSPI.
4. Participar de las actividades para la identificación de activos de información y riesgos de seguridad y privacidad de la información.
5. Colaborar en el desarrollo de las auditorías internas y externas al MSPI.

13.2. PERFILES

La designación del Oficial de Seguridad de la información y el Oficial de Datos Personales será a discreción de la Dirección, tomando en consideración los siguientes perfiles:

Tabla 1 Perfiles de los Oficiales

ROL	PERFIL
Oficial de Seguridad de la Información	Núcleos Básicos del Conocimiento (NBC): Ingeniería de Sistemas, informática, telemática, Ingeniería Electrónica, telecomunicaciones, Ingeniería Industrial, afines o cualquiera pertinente a la naturaleza de las responsabilidades descritas en el numeral 12.1. Conocimientos: Implementación y mantenimiento del estándar ISO 27001:2013 o versiones posteriores, si existieran, conocimientos en ISO 27032 o prácticas de seguridad del Instituto Nacional de Estándares y Tecnologías -NIST-, riesgos de seguridad de la información o seguridad digital, arquitecturas de seguridad informática, gestión de incidentes de seguridad de la información y capacidad para desarrollar políticas y procesos de Seguridad y Ciberseguridad. Deseable: • Postgrados en seguridad informática, seguridad de la información, ciberseguridad o afines. • Certificación en ISO 27001:2013 o posteriores. • Certificaciones en CISM, CISSP, CSX o GRISC.
Oficial de Datos Personales	Núcleos Básicos del Conocimiento (NBC): Cualquiera pertinente a la naturaleza de las responsabilidades descritas en el numeral 12.1.

ROL	PERFIL
	Conocimientos: Legislación y buenas prácticas en materia de protección de datos personales, funcionamiento de la Entidad junto con sus normas y procedimientos administrativos.

Fuente: UAESP 2023

14. INCUMPLIMIENTO

Cualquier contravención u omisión de las políticas aquí descritas, traerá consigo, las consecuencias legales que apliquen a la normatividad vigente y se sancionará por parte de la autoridad competente.

15. CONTROL DE CAMBIOS

Tabla 2 Control de Cambios

Versión	Fecha	Descripción de la modificación
01	15/10/2019	Se adopta la Política de Seguridad de la Información mediante resolución interna 0589 de 2019
02	28/09/2021	Se actualiza la normativa legal vigente aplicable en relación con la seguridad de la información. Se ajustan los objetivos y se definen objetivos específicos de acuerdo con los requerimientos de la ISO 27001, el MSPI y la Política del Sistema integrado de Gestión. Se elimina las menciones al Modelo de Transformación Organizacional – MTO. Se ajustan los principios básicos y se define de forma explícita el compromiso por la dirección. Se definen y ajustan la matriz de roles y responsabilidades en materia de seguridad de la información de acuerdo con la implementación del MSPI.
03	21/06/2022	Se actualiza y ajusta de conformidad al Decreto 767 de 2022, Por el cual se establecen los lineamientos generales

Versión	Fecha	Descripción de la modificación
		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. Se adiciona el principio de confianza, el numeral 10 especificando la revisión de la política y responsables. Se ajustan los roles y responsabilidades para la implementación del MSPI, al igual que sus nombres, y se adiciona el perfil mínimo, para los Oficiales de Seguridad de la Información y el de Protección de Dato Personales y se especifica el incumplimiento a la política.
04	22/03/2024	Se unifica la Política General de Seguridad y Privacidad de la Información con el Manual de Políticas de Seguridad y Privacidad de la Información y se actualizan los lineamientos para dispositivos móviles y BYOD.

Fuente: UAESP 2023

16. AUTORIZACIONES

Tabla 3 Revisión y Aprobación de las Políticas

	NOMBRE	CARGO	FIRMA
Elaboró	Juan Sebastián Perdomo Méndez	Profesional Universitario – Oficina TIC	
Revisó	Cesar Mauricio Beltrán López	Jefe Oficina TIC	
Aprobó	Comité Institucional de Gestión y Desempeño		Acta No 2 del 22/03/2024